December 11, 2023

Colorado Department of Law
Ralph L. Carr Colorado Judicial Center
1300 Broadway, 10th Floor
Denver, Colorado 80203

RE: Joint Ad Trade Letter – Comments on OptOutCode Application

Dear Colorado Department of Law:

On behalf of the advertising industry, we provide this set of comments on OptOutCode's application to become a recognized universal opt-out mechanism ("UOOM"). As explained below, OptOutCode does not meet requirements established by the Colorado Privacy Act ("CPA") and its implementing regulations. Our comments also highlight several other critical factors the Colorado Department of Law ("Department") should consider that weigh against naming OptOutCode as a recognized UOOM.

As the nation's leading advertising and marketing trade associations, we collectively represent thousands of companies across the country. These companies range from small businesses to household brands, long-standing and emerging publishers, advertising agencies, and technology providers. Our combined membership includes more than 2,500 companies that power the commercial Internet, which accounted for 12 percent of total U.S. gross domestic product ("GDP") in 2020.[1] By one estimate, over 150,000 jobs in Colorado are related to the ad-subsidized Internet.[2] We welcome the opportunity to engage with you further on the non-exhaustive list of issues with the OptOutCode UOOM application that we outline here.

I. OptOutCode should not be recognized as a UOOM because it does not meet the technical specifications set forth in the CPA and Rule 5.06 of the CPA implementing regulations.

The Department should not include OptOutCode on the list of required UOOMs because OptOutCode fails to meet certain technical specifications established by the CPA and its implementing regulations. Under the CPA, controllers are required to process opt-out requests that consumers submit via UOOMs only when those mechanisms "meet the technical specifications established by the Attorney General pursuant to section 6-1-1313."[3] OptOutCode does not meet multiple technical specifications established by the CPA and its implementing rules and should accordingly be excluded from the list of UOOMs controllers must honor.

---

[1] John Deighton and Leora Kornfeld, *The Economic Impact of the Market-Making Internet*, INTERACTIVE ADVERTISING BUREAU, 15 (Oct. 18, 2021), located here.
[2] *Id*. at 123.
[3] Colo. Rev. Stat. § 6-1-1306(a)(IV)(B).

a. OptOutCode does not communicate consumers' opt-out choices in a format that is commonly used and recognized, nor does it describe safeguards or protections it employs to refrain from becoming a default mechanism, as required by Rules 5.04 and 5.06(A)(1).

The Department should not approve OptOutCode for the UOOM list because the proposed mechanism (1) relies on a device field that is not commonly accessed or recognized by controllers, and (2) does not provide sufficient assurances it will not be set by default in contravention of the CPA and implementing regulations.

The CPA's technical specification requires that an eligible UOOM signal "must be in a format commonly used and recognized by Controllers."[4] According to the application, controllers would need to "read the name of the device using established IT protocols, determine if the name starts with '0$S' and, if so, consider it an opt-out."[5] The application asserts that implementing the infrastructure to recognize OptOutCode is "available and free" because it requires controllers to "leverag[e] existing protocols to read the names of devices."[6] Contrary to the application's assertions, many controllers that do not collect device name information or interact with connected devices would now be required to build out infrastructure to access a device name field. Thus, most controllers would need to design and implement new system infrastructure rather than one that is commonly used and recognized in the market.

The signal's lack of recognition by entities that are unable to capture device names is likely to raise a host of costly implementation issues that are addressed nowhere in the OptOutCode application. For example, websites operating on a browser typically do not have permission or the ability to access the device field. Additionally, consumers may configure their device settings so that a business does not have permission to access the device field; however, the application provides no guidance as to how a business should navigate a situation in which it is unable to access the required field. In such a scenario, a consumer is likely to believe he or she has successfully opted out when in reality the business is blocked from accessing the field name needed to ingest the opt-out request. Even if a business is able to access the device name and recognize the prefix as an opt-out, the application provides no details as to how the business should process that request without additional information. As described further in Section II, this proposed mechanism would require consumers to provide additional personal information in this device field in order for a controller to action the request. In other words, this prefix alone – "0$S Joe's Phone" – is insufficient to convey a meaningful signal.

Furthermore, according to the CPA itself and its implementing regulations, consumers must be allowed to make an informed decision about their opt-out rights, and no UOOM mechanism may transmit an "opt-out" signal for the user by default.[7] OptOutCode's application could enable default opt-out settings, in contravention of the CPA. For example, device sellers could name the device with OptOutCode's prefix without informing the consumer or asking the consumer to first make an affirmative choice to opt out. OptOutCode's UOOM application does not describe how it

---

[4] 4 C.C.R. 903-4, Rule 5.06(A)(1).
[5] OptOutCode Application, Colo. Dept. of Law, at 6, available at https://coag.gov/app/uploads/2023/11/OptOutCode-Application.pdf [*hereinafter* "Application"].
[6] *Id.* at 12.
[7] Colo. Rev. Stat. §§ 6-1-1313(2)(b), (c); 4 C.C.R. 903-4, Rule 5.04.

will prevent such a scenario, nor does it make any commitments to abide by the CPA's requirements that an UOOM may not operate as a default setting. OptOutCode could consequently enable an entity to make an opt-out choice *for* the consumer rather than ensuring the choice is one that is made *by* the consumer. This result would undermine the consumer's rights under the statute. UOOM candidates should be required to clarify how they will protect against opt-out mechanisms being set by default to conform with the CPA's requirements for user transparency and control related to opt-out requests.

b. OptOutCode hinders a controller's ability to verify the legitimacy of a request in violation of § 6-1-1313 and Rule 5.06(D).

OptOutCode does not provide for sufficient identity authentication mechanisms to allow a controller to authenticate a consumer as a Colorado resident or verify the legitimacy of a request. Under the CPA, controllers are not required to comply with an opt-out request unless that request can be authenticated.[8] Including a proposed UOOM that does not sufficiently allow for authentication on the list of required UOOMs would read out of the text of the CPA important provisions related to controller authentication of consumer requests. The regime contemplated by OptOutCode would force controllers to honor opt-out requests they otherwise would not without first obtaining important authenticating information from the consumer. In this way, OptOutCode's proposal conflicts with the authentication provisions in the statutory text of the CPA. Thus, rather than requiring controllers to honor all OptOutCode opt-out requests, the Department should allow controllers to choose whether to honor an OptOutCode opt-out request if the controller is unable to authenticate the request.

The CPA requires that a recognized 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."[9] OptOutCode is designed so that consumers can opt-out "from most if not all" selling or sharing for targeted advertising by "renaming three devices: their smartphone, their personal computer, and their home router."[10] OptOutCode does not permit a controller to authenticate a consumer's residency as required by the CPA and its implementing rules. Although a UOOM provider does not itself have to authenticate that a consumer is a Colorado resident, the UOOM is still required to permit a controller to do so.[11]

OptOutCode's application suggests that controllers can adequately authenticate a request based on a user's IP address. However, an IP address does not equate to residency. For example, consumers from any state could access a Colorado IP address via a VPN. At best, IP address provides a guess as to where a consumer may reside. Such a standard is not sufficient when an opt-out request could have far-reaching impacts on consumer privacy and choice. Controllers should have the option to honor UOOMs that do not permit controllers to authenticate residency, as the controller otherwise would under the CPA.

---

[8] Colo. Rev. Stat. § 6-1-1306(2)(d).
[9] Colo. Rev. Stat. § 6-1-1313(2)(f); 4 C.C.R. 903-4, Rule 5.06(D).
[10] Application, at 3.
[11] *Compare* 4 C.C.R. 903-4, Rule 5.03(C) (stating UOOM providers are not obligated to authenticate that a user is a Colorado resident), *with* Colo. Rev. Stat. § 6-1-1313(2)(f) (requiring the UOOM permit the controller to accurately authenticate the user as a Colorado resident).

OptOutCode's design also presumes that an individual consumer is always accessing and connecting to their personal devices, but consumers often connect to other devices, such as public networks or a friend's systems. OptOutCode provides no guidance for how controllers should treat opt-out signals that a consumer may have set up on a registered device when a guest connects their own device to the consumer's network via their home router. The device owner and their guest may have two different opt-out preferences, yet businesses do not have a way to verify which signals from the connected devices reflect the legitimate request of the consumer who wishes to opt out. This problem is exacerbated if a consumer joins a public network that has been named with an opt-out code. In this case, the individual that established the network may be opting out other individuals who join the network without providing any opportunity for those consumers to express their individual privacy preferences. Such a system would prevent a controller from verifying a consumer request is legitimate because the controller would have no reliable way to match a particular device to a consumer who has actually decided to opt out. Thus, OptOutCode violates the CPA's technical specifications and should not be included on the Department's list of approved UOOMs, or, at the very least, should be made optional if a controller us unable to authenticate a request sent through the mechanism.

II. The Department should consider the consumer privacy concerns raised, high anticipated implementation costs, and lack of commercial adoption of the proposed UOOM as additional factors that weigh against required recognition of OptOutCode.

In addition to OptOutCode's failure to adhere to the CPA and its implementing regulations' explicit technical specifications, the Department may consider several additional critical factors that weigh against OptOutCode's inclusion on the list of recognized UOOMs.[12] These optional factors permit the Department to consider the proposed mechanism's likely impact on consumers, controllers, and the market as a whole. The consumer privacy concerns, anticipated implementation costs, and lack of commercial adoption of OptOutCode are likely to negatively impact consumers, controllers, and the market alike. The Department should exclude the OptOutCode from the approved UOOM list accordingly.

a. OptOutCode raises several consumer privacy concerns because the proposed mechanism would require many controllers to collect and share more consumer data than they otherwise would.

The Department should not approve a proposed UOOM that creates new privacy concerns for consumers. CPA implementing regulations allow the Department to look at the "ease and cost of use, implementation, and detection by Consumers" when evaluating proposed UOOMs.[13] Additionally, the regulations explicitly prohibit controllers from "require[ing] the collection of additional Personal Data beyond that which is strictly necessary" for several enumerated purposes.[14] OptOutCode requires that controllers collect a new data field that is not regularly collected, and most likely will necessitate a request for additional information to authenticate the consumer. The collection of device name and the very likely need to request or provide additional data with the

[12] 4 C.C.R. 903-4, Rule 5.07(D).
[13] *Id.*, Rule 5.07(D)(2).
[14] *Id.*, Rule 5.05.

OptOutCode device name prefix is unnecessary when other market opt-out options exist that do not require the same additional data collection.

The data collection that would be required under OptOutCode is particularly problematic because it would require businesses to continuously collect device name information and run queries to determine whether the prefix that did not appear before has been added to the device when a user returns. Additionally, the prefix alone is meaningless unless the consumer provides additional information for authentication in the device field or the business begins maintaining additional data about a device in order to recognize requests. For example, a business could not connect the prefix "0$S – Joe's Phone" to the relevant Joe in their system without additional information about Joe. The Department should reject adding OptOutCode to the approved UOOM list due to the avoidable privacy risks created by its extraneous data collection and sharing requirements.

b. OptOutCode is likely to impose heavy design, implementation, and testing costs on many controllers who do not already integrate device name collection in their existing infrastructure.

OptOutCode's proposed additions to businesses' opt-out infrastructure is likely to be resource intensive and impose significant costs on controllers. CPA implementing regulations allow the Department to consider the "ease and cost of use, implementation, and detection by . . . Controllers" when evaluating a proposed UOOM.[15] As discussed in Section I.a, contrary to the application's assertions, businesses do not widely recognize or have access to device field name or have infrastructure in place to easily do so. Failure to recognize this signal is likely to result in partial opt-out coverage. Many businesses therefore would need to undergo significant design, implementation, and testing efforts to integrate an additional field code into their existing infrastructure. Such infrastructure updates are often resource-intensive and impose heavy costs on businesses. Additional costs are especially likely in a situation like the one here where the market has not in fact widely adopted a particular mechanism and numerous implementation questions are likely to arise. Small businesses and startups, which often do not have the dedicated infrastructure resources or scalable testing processes of their larger counterparts, are especially likely to face significant cost burdens. The Department should consider the anticipated integration costs to controllers as a factor weighing against inclusion of OptOutCode on the approved UOOM list.

c. OptOutCode is premature and should not be approved until it has been more widely adopted and undergone additional testing.

OptOutCode is still in early development stages, and at a minimum, the Department should delay inclusion of the proposed mechanism on the approved UOOM list until after OptOutCode has undergone more rigorous testing and development. CPA implementing regulations allow the Department to consider both the proposed mechanism's "commercial adoption by Consumers or Controllers" and "whether the [UOOM] has been approved by a widely recognized, legitimate standards body after broad multistakeholder participation in the standards-making process."[16] Neither factor weighs in favor of including OptOutCode as described in the application materials.

---

[15] *Id.*, Rule 5.07(D)(2).
[16] *Id.*, Rule 5.07(D)(1), (3).

The application materials clearly demonstrate that OptOutCode, as applied to most consumer devices, is still in its infancy. The introduction explicitly states the developers considered applying OptOutCode to traditional consumer devices a mere three weeks before submitting the application.[17] The technical specification is incomplete and conditions the development of a consumer app through which consumers can easily turn OptOutCode "on" or "off" on the Department's inclusion of OptOutCode on the UOOM shortlist.[18] Although the application indicates developers have "been testing OptOutCode for the past two years," the application materials do not provide the results of these tests.[19] Instead, the application points to an example of one controller successfully applying this mechanism in a single context.[20] The viability of OptOutCode as a solution for various device types has not yet been tested at any kind of scale.

The application illustrates OptOutCode clearly has not yet been commercially adopted by consumers or the industry and that testing by stakeholders is still ongoing.[21] Inclusion of OptOutCode on the Department's approved UOOM list at this time would be premature, and the Department should require further technical analysis to assess feasibility and risk to consumer privacy before approving the proposed UOOM.

* * *

Thank you for the opportunity to submit comments on this important topic. Please do not hesitate to contact us with questions regarding this submission.

Sincerely,

Christopher Oswald
EVP for Law, Ethics & Govt. Relations
Association of National Advertisers
202-296-1883

Alison Pepper
Executive Vice President, Government Relations
American Association of Advertising Agencies, 4A's
202-355-4564

Lartease Tiffith
Executive Vice President for Public Policy
Interactive Advertising Bureau
212-380-4700

Clark Rector
Executive VP-Government Affairs
American Advertising Federation
202-898-0089

Lou Mastria, CIPP, CISSP
Executive Director
Digital Advertising Alliance
347-770-0322

CC: Mike Signorelli, Venable LLP
Allie Monticollo, Venable LLP

---

[17] Application, at 2 ("As of 3 weeks ago it dawned on us that OptOutCode could be successfully used as a UOOM also on traditional computing devices (laptops, desktops, tablets, terminals) and all the programs that run them.")
[18] *Id.* at 6-7.
[19] *Id.* at 17.
[20] *Id.* at 3, 12, 14.
[21] *See id.* at 14 (listing OptOutCode's recognition by the Department and consumer awareness as "two hurdles to the adoption of OptOutCode as a broadly accepted UOOM standard").