December 11, 2023

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

Re: Universal Opt-Out Shortlist

Dear Colorado Department of Law:

On behalf of the Computer & Communications Industry Association (CCIA), I write to respectfully express several concerns about the shortlist of potential Universal Opt-Out Mechanisms (UOOM) for consideration.

CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms.[1] CCIA and its members commend the Department for its efforts to implement the requirements under the Colorado Privacy Act swiftly and transparently. However, CCIA is concerned about the list of UOOMs for consideration, especially given the operational difficulties and implementation challenges presented by each UOOM. As discussed below, the application does not satisfy all the requirements of the CPA and the Final Rules and as such, CCIA recommends the Department to require further disclosures before approval.

1. "Global Privacy Control" Application

The Global Privacy Control (GPC) application describes how it grants a user the ability at the browser level to notify websites of their opt-out preferences. However, several concerns remain regarding how the GPC adheres to the statutory requirements under Colorado law. Until further clarification is provided, CCIA recommends that the GPC application should not be included in the final list.

Statutory Requirements. Several unresolved questions remain regarding how the GPC qualifies as a UOOM, especially given that it is more of a framework that can be interpreted and implemented differently.

First, under Colorado law, only a "platform, developer, or provider" can offer a UOOM. Yet, it is not clear that this protocol meets any of these definitions. Second, a valid UOOM needs a consistent mechanism that provides sufficient notice and disclosure to inform a consumer's choice to opt-out. The UOOM needs to ensure that the user interface clearly indicates to the consumer which opt-out choices they are making. However, the GPC application does not address how these requirements would be met. Rather, the application indicates that the opt-out for targeted advertising would be bundled with other opt-outs such as "sale". It is not clear that the GPC can satisfy these requirements due to the lack of a user interface and its technical nature as a protocol. Lastly, the lack of consistent implementation of the GPC creates compatibility and compliance issues. For instance, it is unclear if each entity that offers an opt-out using the GPC specifications needs to apply individually to be listed, or can simply use this open source tool. Additionally, the lack of consistent implementation of the GPC has seen some user-agents turn the UOOM signal on by

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

default. It seems counterintuitive to grant a blanket approval of this UOOM if it cannot meaningfully inform a user of what they are consenting to.

2. “Opt-OutCode” Application

The Opt-outCode (OOC) application describes how it will be compatible with all online services, including devices and apps. This UOOM would require device owners to modify the name of a device by adding the following prefix: “0$S”. To recognize this signal, companies would need to develop a means to collect and read the name of the device, and where the prefix is present, convert it into an opt-out request. While this application promises a universal solution that is simple, CCIA urges against its inclusion in the final list and requests further analysis over its technical feasibility and risks to consumers.

Timing. It is too early to mandate the adoption of the OOC as per the application, the technical documentation is still in progress. The application proposes a novel mechanism that ostensibly works on a variety of devices, but the viability of the solution for the various device types has not yet been tested at any kind of scale, and it is not clear to what extent it has been reviewed by any industry organizations. Further, on page 5, the application provides only one context of a controller honoring opt-out signals – WiFi routers. The Department should not approve the application until further testing and after technical specifications are finalized and published.

Technical Feasibility. On page 5 of the application, it argues that with companies having already adopted opt-out infrastructure, “the marginal cost companies would face to roll-out those code and process changes should be zero or negligible.” This claim is misguided and fails to recognize the resources required to implement any such additions.

For an impacted service like an app, website, or device to respect the “0$S” opt-out, it would need access to the Device Name field. The application does not provide sufficient guidance on what an affected service is required to do in situations where it does not have native permissions to access this field. Services that do not currently reference Device Name would have to start scanning this field, which means mandating the collection of more data points about the customer than the business otherwise would – undermining organizations’ efforts and progress to adhere to data minimization principles.

The application also provides insufficient specifics on the obligations that operating systems, browsers, devices, and apps have to pass on the opt-out to their upstream services. The application only references translating the “0$S” opt-out into a GPC opt-out but does not provide any concrete requirements.

Additionally, the technical documentation on the expectations of browsers and the websites accessed via those browsers is overly vague. While a myriad of devices may have default permission to access the device name, websites operating on a browser should not. For instance on page 4, the documentation provides little guidance that browsers may look at the device name and if the “0$S” signal is present, set a default GPC opt-out signal. However, this procedure does not address the timing considerations nor the follow-on expectations for sites that receive this second-hand GPC signal. Under this scheme, when a user opt-outs through the OOC, the customer is then opted-out of GPC, and then opted-out of the company website. It is not clear if the customer will be able to opt back into GPC or the company website.

The OOC also raises identity-matching concerns. For example, a consumer that owns a registered device like a smart TV may prefer not to opt-out of targeted ads, but it is unclear how the device interprets a signal from a guest's connected device – such as from their smartphone.

Consumer Concerns. If approved, the OOC will require companies to collect more personal data about consumers. Currently, many devices, apps, browsers, and websites do not collect device names, this is typically limited to bluetooth and the internet-of-things (IoT) context. The OOC would require companies to pull the Device Name field, which may include information that directly identifies the consumer – ex: "123 Center Street Tablet." Compliance with this mandate would force companies to continuously ping devices for this information in order to detect whether the "0$S" prefix has been added.

Mandating the OOC will also require devices to share personal data about their consumers with third parties. If a business normally restricts access to device names to protect end users' privacy, it may now be forced to make the field available to upstream services – a smartphone would need to share with third-party apps, and a browser with all visited websites. The OOC also invites consumer confusion as it may trigger opt-out requests that extend beyond the scope of what consumers want to opt-out of. The application indicates that companies should also read the name of the Wi-Fi router and various IoT devices, and if the prefix is present, then opt-out the consumer. But if the consumer connects to a Wi-Fi network or IoT device controlled by others, including in public settings, then this may unintentionally communicate an opt-out signal. This is also inconsistent with the purpose of the UOOM requirement, which is to empower individuals to manage how their data is collected and used.

Importantly, the OOC does not allow a user to specify what they are opting-out of. This hardline approach raises concerns about interoperability as various jurisdictions introduce additional types of opt-outs. The application notes that such a development may potentially be available in the future, but makes no commitments about it.

3. "Opt-Out Machine" Application

CCIA is concerned that the Opt-Out Machine (OOM) seems to operate more as an authorized agent rather than a UOOM, along with failing to provide a consumer the ability to select different opt-out. A consumer would sign up for a service with OOM, which would then send an email to companies that "likely" hold that consumer's data. Further, the OOM also appears to still be in development and its approval might be premature. The application notes that the scope of the requests is still being developed and the results from expert testing and reviews has not been publicly shared. CCIA recommends that the Department does not include the OOM application in the final list.

Statutory Requirements. As described in the application, the OOM exceeds the permitted scope for UOOMs. The Colorado Privacy Act and implementing rules limit UOOMs to the opt-outs of targeted advertising and the sale of personal data.[2] Importantly, the consumer needs the ability to choose which opt-out they prefer. Here, the OOM fails to provide users the ability to express their opt-out choice and extends beyond the legal requirements in CPA to other customer rights such as data access and deletion. ***Specifically, an unintended signal may cause serious harm to customers, ranging from permanently deleting their accounts across services to potentially making account information available to bad actors***.

[2] Colorado Privacy Act, Rule 5.02(A).

The OOM also does not limit its signal to those controllers with whom the consumer interacts with after activating the UOOM.[3] Rather, similar to an authorized agent, the OOM decides which controllers to interact with and the application contains no information or clarity on how it selects these controllers. The inconsistent signaling would likely result in an unfair disadvantage to certain controllers that are always included in the communications, while others are excluded.[4] The OOM impermissible extends to individuals who are not "consumers" as defined under the CPA, because it also applies to individuals acting in a commercial context – employees signing up on behalf of a company.

This appears to be an application to recognize OOM as an authorized agent. However, the CPA does not permit the Colorado Attorney General to mandate that controllers honor requests from certain agents. Nonetheless, the 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.[5] The application references that in only "some cases" will it ask consumers for proof of identity.

Verification. Under the CPA, a UOOM must "permit the controller to accurately authenticate the consumer" as a resident of the state and "determine that the mechanism represents a legitimate request" to opt-out of processing for targeted advertising and sale.[6] The application describes 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. As stated, the OOM would not sufficiently allow for a controller to accurately confirm the identity and residency of the consumer. Further, the application does not address:

- How the OOM would determine which third parties it will email on behalf of consumers;
- Whether consumers can indicate a preference as to which third parties they wish to exercise their right against; or
- Whether the OOM can automatically update consumer preferences across websites.

Consequently, it would be difficult for a controller to determine that the opt-out request is legitimate.

Consumer Concerns. The application states that the OOM collects significant personal data including physical address and sometimes proof of identity but provides no details on how this information will be secured or used. This is an undue burden on the consumer, especially considering that alternative UOOMs do not require such information. Under Rule 4.02, controllers are required to use reasonable data security measures when exchanging information in furtherance of data rights requests. The application's described method of email transmission fails to constitute reasonable data security measures as emails are not a sufficiently secure mechanism to transmit personal data. In addition, the OOM application contains no discussion of what security measures such as access controls or use of encryption the OOM employs to protect the personal data it collects, stores, or transmits, from security threats.

Lastly, despite the availability of low to no cost alternatives like the GPC, the OOM is expensive. The price ranges from a "$30 do-it-yourself service" to $150. The OOM is not a viable UOOM option for consumers and should not be included in the final list.

[3] Rule 5.02(B).
[4] Rule 5.06(E).
[5] Rule 4.03(C).
[6] Colo. Rev. Stat. § 6-1-1313(2)(f).

*   *   *   *   *

CCIA shares the urgency of the Department to implement the requirements under the Act, providing consumers and businesses with much-needed clarity. However, for the aforementioned reasons, we urge the Department to not include these UOOMs in the final list. We appreciate the Department's consideration of these comments and stand ready to provide additional information as the list is finalized.

Respectfully submitted,

Alvaro Marañon
Privacy Policy Counsel
Computer & Communications Industry Association

December 11, 2023