OptOutCode

A Privacy4Cars® Universal Opt-Out Concept

December 11th, 2023

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

Re: OptOutCode's Comments on its Colorado UOOM Application

Dear Office of the Attorney General:

We thank the Attorney General Weiser and the Colorado Department of Law (the "Department") for shortlisting OptOutCode on November 20th, 2023. As you seek input from stakeholders, we appreciate the opportunity to submit our own comments.

We are grateful for you reviewing our application filed on November 6th, 2023. Since then, we have had discussions with various stakeholders and made technical progress, and we want to update you in four areas:

1. We want to make sure we are **clarifying that OptOutCode is compatible with Global Privacy Control** ("GPC"): in fact, it is complementary and expands privacy protections for GPC users;

2. We have **made OptOutCode even easier for consumers and businesses to adopt** as an effective opt-out mechanism by (a) creating a **"banner"** that all websites can easily add to raise awareness among Colorado Consumers and encourage them to turn on UOOMs, (b) developing **tutorials** for consumers, and (c) publishing an OptOutCode **app for Android and iOS** platforms;

3. We want to point out to policy – not technical – **changes that Google and Apple have been making** to their app stores which could be improved to make it easier for consumers and companies to use OptOutCode in some specific scenarios; and

4. In light of the legal actions the Office of the Colorado Attorney General is taking (with other states) against certain social media platforms, we want to stress out that **approving OptOutCode as a valid UOOM in Colorado would be an effective mechanism for reducing the financial incentive many tech companies have to monitor, target, and influence Colorado residents, including some of the most vulnerable: children and teens**. It would

also efficiently protect the resources the State has while casting a wider protection net.

1. OptOutCode is compatible with GPC and actually expands the privacy protections for GPC users

OptOutCode does not conflict with Global Privacy Control, which is an established and not surprisingly also shortlisted opt-out mechanism.[1] Currently, businesses subject to California Consumer Privacy Act ("CCPA") are required to detect and honor GPC signals as legally binding opt-out requests for California consumers.[2] We deemed it important to explicitly address the question of potential conflicts, hence we performed an analysis to demonstrate the complementary and compatible relationship between OptOutCode and GPC. OptOutCode is consistent with GPC for two main reasons:

a. **Complementary.** GPC is a browser-level privacy signal designed to allow website visitors to notify businesses of their preference to not have their data sold or shared, or used for cross-context behavioral advertising. Whereas, OptOutCode is compatible with smartphones, laptops, tablets, routers, apps, and IoTs. The average American spends 6 hours and 58 minutes online daily. Browsing social media accounts and streaming videos accounts for more than five hours of that time. It is common for companies with online services to encourage and nudge consumers to stop consuming content through their browsers (where GPC could offer protections) and instead do so through their apps (particularly on smartphones) or their IoTs (e.g. "connected"/"smart" TVs, speakers, watches, vehicles, etc.), for which no UOOM was effective prior to OptOutCode. Consequently, current GPC users can easily expand the level of protection to their personal data by also adopting OptOutCode; for individuals who have not used a UOOM before and adopt OptOutCode, GPC adoption would also be encouraged.

b. **Compatibility.** Individuals can activate GPC by toggling a browser privacy setting or installing an extension for their browser. The browser or extension will automatically send a signal to each website the user visits broadcasting that individual's preference not to have their data sold or shared, or used for targeted advertising. OptOutCode does not interfere and in facts promotes adoption of private browsing (possibly with GPC).

As we outlined in our original Colorado UOOM submission, since consumers have the right to freely give or revoke consent, the last signal and preference expressed by a consumer is the one that governs and directs businesses to opt a consumer out - or not. Specifically, there are four possible scenarios depending on whether a user sets GPC and/or OptOutCode on or off. The matrix below illustrates how those four scenarios should be interpreted:

---

[1] Colorado Privacy Act 6-1-1313(2)(e) ("Adopt a mechanism that is as consistent as possible with any other similar mechanism required by law or regulation in the United States").
[2] CCPA § 1798.140(d)(1).

	Global Privacy Control OFF	**Global Privacy Control ON**
OptOutCode OFF	[1] Consumer is not expressing an opt out automatically. This is equivalent to the scenario that exists today for consumers who do not use GPC. Consumers who wish to opt out must do so manually on each website they visit, for every IoT they purchase, every service they use, etc.	[2] This is equivalent to the scenario that exists today for current users of GPC. There is no conflict when users browse the web as the GPC signal is read by websites who respect their opt-out wish. Outside of web properties, consumers would not have a UOOM in place that protects them.
OptOutCode ON	[3] Upon launching the web browser on a device that has OptOutCode on (e.g. on a consumer's smartphone), the OS or the browser app can detect the name of the device, parse the first three letters, and determine that OptOutCode is on. That opt-out signal must now be relayed from the browser to the websites the consumer visits. This could be done in two main ways: 1. If the browser is compatible with GPC but GPC is turned off or a necessary plugin is not installed, it should turn on GPC or prompt the user to download one or a choice of plugins that would activate GPC. If the consumer refuses, when prompted, to turn on GPC, it should be interpreted as an active choice of that consumer wanting to be tracked, hence setting the OptOutCode default off, until the next browser session or forever if the consumer asserts that unequivocal choice with a clear opt-in message. 2. If the browser is not compatible with GPC, the developer of the browser should either make the browser compatible with GPC or develop an alternative mechanism to ensure that the consumer's desire to opt-out is respected by the online properties visited while using the browser.	[4] Consumers have set both UOOMs on. There is no conflict as the consumer is consistently expressing their desire to opt out from certain data processing. Web browsers, and all the websites a consumer visits, would be aware of the consumer's desire to opt-out and respect that choice accordingly.

It is obvious from scenario [3] (GPC off, OptOutCode on) that OptOutCode, if approved by Colorado and other states that allow for Universal Opt-Out Mechanisms, may make it easier for consumers to set and turn on GPC on their browsers, hence resulting in a greater adoption of GPC.

Scenario [2] (GPC on, OptOutCode off) suggests that there is also an opportunity, for the many consumers who elected to use GPC already, to greatly expand the protections available to them by learning about and starting to use OptOutCode.

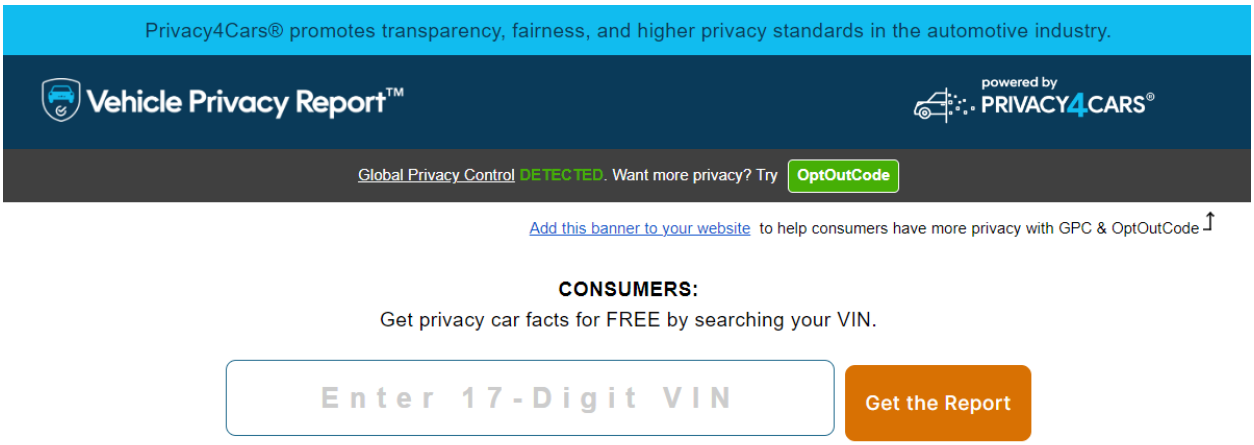
Lastly, scenario [1] (both GPC and OptOutCode are off) is an important reminder that educating the public that greater privacy is possible and requires only small, simple, fast actions, is critical to raise the privacy bar for Colorado residents.

2. OptOutCode is now even easier for consumers and businesses to adopt as an effective opt-out mechanism

Since the date of our submission, we developed three tools to facilitate the adoptions of UOOMs: (a) we created a website "banner" that online publishers can easily add to raise awareness among Colorado consumers and encourage them to turn on UOOMs, (b) we started developing "how-to" tutorials for consumers, and (c) we submitted to Apple's App Store and Google's GooglePlay store an "OptOutCode" app to make it easier for consumers to check and turn on the opt-out signal as well as to demonstrate how easily companies can listen to the OptOutCode on smartphones (and trigger opt-outs for the IoTs they connect to and the apps that run on them).

(a) The OptOutCode website banner:

Awareness of Colorado residents is critical for the successful widespread adoption of UOOMs. For the above reasons, Privacy4Cars developed a "banner" feature that is very easy for webmasters to add to their websites and makes it easy to educate and encourage website visitors to turn on GPC and OptOutCode. We already implemented this banner on https://optoutcode.com, https://privacy4cars.com, and https://vehicleprivacyreport.com (see example below).

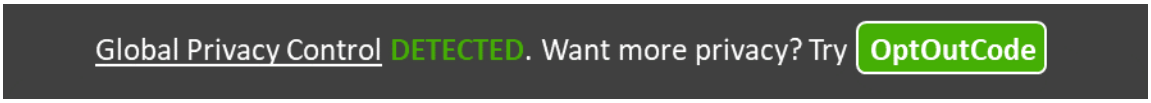


Example of OptOutCode's banner used in a third-party website (GPC is on)

The banner works as follows:

1. If a user's browser does not have GPC enabled, a website using this banner would encourage users to learn about and turn on GPC so they can enjoy a more private browsing experience (the button takes users to https://globalprivacycontrol.org/).

2. If a user's browser already has GPC turned on, a website using our banner acknowledge their GPC privacy choices and encourage them to expand protections by learning about and turning OptOutCode, resulting in casting a wider privacy safety net beyond browsing online (the "Global Privacy Control" points to https://globalprivacycontrol.org/and the button takes website visitors to https://optoutcode.com/).



Webmasters wishing to advocate for consumer privacy can easily implement this banner in a few minutes by following these steps:

a) Add the following line of code[3] inside your website's <head> tag and make sure to allow any external scripting permissions that might be required on your website to allow the above line of code to work:

```
<script
src="https://storage.googleapis.com/privacy4cars/static/script/gpc/optoutcode
-banner.js"></script>
```

b) Add the following line of code in your website's <body> or <main> tag where you want the banner to appear and do not place the line of code as/in any nested elements to ensure proper visibility:

```
<div class="optoutcode-banner-container"></div>
```

c) Only the two snippets of code above need to be added to a website to add the OptOutCode banner. For illustrative purposes, we are copying the code that powers this feature at this time of submitting this comment. Webmasters should be using the link in the footnote to use the latest version of the code:

[3] Code is publicly available at https://storage.googleapis.com/privacy4cars/static/script/gpc/optoutcode-banner.js

```
//This script is an initiative by OptOutCode. Learn more at:
https://optoutcode.com/
//A Privacy4Cars Universal Opt Out Mechanism. Learn more about Privacy4Cars
at: https://privacy4cars.com/
let gpcBannerContainer;

let gpcEnabledBanner = `<!-- This script is an initiative by OptOutCode.
Learn more at: https://optoutcode.com/ -->
<!-- A Privacy4Cars Universal Opt Out Mechanism. Learn more about
Privacy4Cars at: https://privacy4cars.com/ -->

<div id='gpc-enabled-banner' class='gpc-banner'><span>Good job! GPC Detected.
Want more privacy? Try</span><a href='https://optoutcode.com/'
target='_blank'>OptOutCode</a></div>`;<div id='gpc-enabled-banner'
class='gpc-banner'><span><a id="gpc-link-text"
href='https://globalprivacycontrol.org/' target='_blank'>Global Privacy
Control</a> <a id="detected-text">detected</a>. Want more privacy?
Try</span><a class="button-link" href='https://optoutcode.com/'
target='_blank'>OptOutCode</a></div>`;

let gpcDisabledBanner = `<!-- This script is an initiative by OptOutCode.
Learn more at: https://optoutcode.com/ -->
<!-- A Privacy4Cars Universal Opt Out Mechanism. Learn more about
Privacy4Cars at: https://privacy4cars.com/ -->
<div id='gpc-disabled-banner'class='gpc-banner'><div class="psa-block"><svg
xmlns="http://www.w3.org/2000/svg" width="20" height="20" viewBox="0 0 20 30"
fill="none"><path d="M11.3986 0.21875H8.69564C6.00327 0.21875 3.80713 2.40433
3.80713 5.10726V6.68046H8.8329C9.04292 6.68046 9.24434 6.76389 9.39284
6.91239C9.54135 7.0609 9.62478 7.26232 9.62478 7.47233C9.62478 7.68235
9.54135 7.88377 9.39284 8.03228C9.24434 8.18078 9.04292 8.26421 8.8329
8.26421H3.80713V10.0486H8.8329C9.27635 10.0486 9.62478 10.397 9.62478
10.8404C9.62478 11.2733 9.27635 11.6323 8.8329
11.6323H3.80713V13.4061H8.8329C9.04292 13.4061 9.24434 13.4896 9.39284
13.6381C9.54135 13.7866 9.62478 13.988 9.62478 14.198C9.62478 14.408 9.54135
14.6094 9.39284 14.7579C9.24434 14.9064 9.04292 14.9899 8.8329
14.9899H3.80713V16.4469C3.80713 19.1499 5.99271 21.3354 8.69564
21.3354H11.3986C14.1015 21.3354 16.2871 19.1499 16.2871
16.4469V5.10726C16.2871 2.40433 14.091 0.21875 11.3986 0.21875ZM16.2871
6.68046V8.26421H11.2613C11.0513 8.26421 10.8499 8.18078 10.7014
8.03228C10.5529 7.88377 10.4694 7.68235 10.4694 7.47233C10.4694 7.26232
10.5529 7.0609 10.7014 6.91239C10.8499 6.76389 11.0513 6.68046 11.2613
6.68046H16.2871ZM11.2613 10.0486H16.2871V11.6323H11.2613C10.8179 11.6323
10.4694 11.2733 10.4694 10.8404C10.4694 10.397 10.8179 10.0486 11.2613
10.0486ZM16.2871 13.4061V14.9899H11.2613C11.0513 14.9899 10.8499 14.9064
10.7014 14.7579C10.5529 14.6094 10.4694 14.408 10.4694 14.198C10.4694 13.988
10.5529 13.7866 10.7014 13.6381C10.8499 13.4896 11.0513 13.4061 11.2613
13.4061H16.2871Z" fill="#DD9200"/>

<path d="M18.3991 11.7031C18.6791 11.7031 18.9477 11.8144 19.1457
12.0124C19.3437 12.2104 19.4549 12.4789 19.4549 12.759V17.2885C19.4549
19.2009 18.6953 21.035 17.3431 22.3873C15.991 23.7397 14.157 24.4996 12.2446
24.4998L7.74572 24.5104C3.77155 24.5104 0.544922 21.2806 0.544922
17.299V12.7695C0.544922 12.4895 0.656161 12.2209 0.854169 12.0229C1.05218
11.8249 1.32073 11.7137 1.60076 11.7137C1.88078 11.7137 2.14934 11.8249
```

```
2.34734 12.0229C2.54535 12.2209 2.65659 12.4895 2.65659
12.7695V17.299C2.65603 18.6497 3.19154 19.9454 4.14553 20.9016C5.09951
21.8577 6.39398 22.3962 7.74466 22.3987L12.2425 22.3882C13.595 22.3882
14.8922 21.8509 15.8485 20.8945C16.8049 19.9381 17.3422 18.641 17.3422
17.2885V12.759C17.3422 12.4789 17.4534 12.2104 17.6514 12.0124C17.8495
11.8144 18.1191 11.7031 18.3991 11.7031ZM5.06389
25.5557H7.73516V24.5104H12.3703V25.5557H15.031C16.0129 25.5557 16.9104
26.0942 17.3644 26.9494L18.4096 28.871C18.6314 29.2828 18.3357 29.779 17.8712
29.779H2.21314C1.74857 29.779 1.45294 29.2828 1.67467 28.871L2.71994
26.9494C3.18451 26.0942 4.09253 25.5557 5.06389 25.5557Z"
fill="#DD9200"/></svg><div class="psa-text-block"><span>Public
Service</span><span>Announcement</span></div></div> Turn on<a class="button-
link" href='https://globalprivacycontrol.org/' target='_blank'>Global Privacy
Control</a> for better privacy online</div>`;


let bannerCTA = `<a href='https://optoutcode.com/optoutcode-does-not-
conflict-with-gpc/' target='_blank'>Add this banner to your website</a>  
to help consumers have more privacy with GPC & OptOutCode <svg
xmlns="http://www.w3.org/2000/svg" width="12" height="30" viewBox="0 0 12 19"
fill="none"><path d="M8 18.5V19H8.5V18.5H8ZM8.35355 0.646446C8.15829 0.451185
7.84171 0.451185 7.64645 0.646446L4.46447 3.82843C4.2692 4.02369 4.2692
4.34027 4.46447 4.53553C4.65973 4.7308 4.97631 4.7308 5.17157 4.53553L8
1.70711L10.8284 4.53553C11.0237 4.7308 11.3403 4.7308 11.5355 4.53553C11.7308
4.34027 11.7308 4.02369 11.5355 3.82843L8.35355 0.646446ZM8.5 18.5L8.5
1H7.5L7.5 18.5H8.5ZM8 18H0.5L0.5 19H8V18Z" fill="black"/></svg>`;

let gpcEnabled = navigator.globalPrivacyControl;
let stylesheetHref =
'https://storage.googleapis.com/privacy4cars/static/script/gpc/optoutcode-
banner.css'
const observer = new MutationObserver(handleMutations);
document.addEventListener("DOMContentLoaded", function () {
      addStylesheet();
});
function addStylesheet() {
  let head = document.head;
  new Promise((resolve, reject) => {
  let link = document.createElement("link");
  link.type = "text/css";
  link.rel = "stylesheet";
  link.href = stylesheetHref;
  link.onload = () => { resolve() };
  link.onerror = () => { reject() };
  head.appendChild(link);

}).then(() => {

    addBanners();

  }).catch(() => {

    console.error("Error loading GPC Banner Stylesheet");

  });
```

```
}

function addBanners() {

  gpcBannerContainer = document.querySelector('.optoutcode-banner-
container');

  if (gpcBannerContainer) {
    gpcBanner();
  } else {
    observer.observe(document.documentElement, { childList: true, subtree:
true });
  }

}

function handleMutations(mutationsList, observer) {
  mutationsList.forEach(mutation => {
    const nodes = mutation.addedNodes;
    handleNewNodes(nodes);
  });
}
function handleNewNodes(nodes) {
  nodes.forEach(node => {
    if (node.classList && node.classList.contains('optoutcode-banner-
container')) {
      gpcBannerContainer = node;
      gpcBanner();
    } else if (node.querySelectorAll) {
      const targetNodes = node.querySelectorAll('.optoutcode-banner-
container');
      targetNodes.forEach(targetNode => {
        gpcBannerContainer = targetNode;
        gpcBanner();
      });
    }
  });
}
function gpcBanner() {
  if (!gpcEnabled) {
    gpcBannerContainer.innerHTML = gpcDisabledBanner;
  } else {
    gpcBannerContainer.innerHTML = gpcEnabledBanner;
  }
  if (gpcBannerContainer.dataset.bannerCta == 'true') {
    addBannerCTA()
  }
}
function addBannerCTA() {
  const bannerCtaFloat = document.createElement("div");
  bannerCtaFloat.classList.add('banner-cta');
  bannerCtaFloat.innerHTML = bannerCTA;
  gpcBannerContainer.appendChild(bannerCtaFloat);
}
```

We ask the Office of Attorney General and the Colorado Department of Law to reach out to and encourage all Colorado state and local entities with consumer-facing websites to add the OptOutCode banner and, by doing so, show Colorado residents the good work their government is doing to protect their privacy and teach them how to take small but effective actions to do the same. It is our hope that other non-profit and for-profit organizations will follow that example, adopt the OptOutCode banner, and contribute to driving awareness, promoting adoption of UOOMs, and improving privacy protections for all.

(b) OptOutCode "how-to" tutorials:

In our original submission we stated that changing the device name to add "0$S" as its first three letters can be performed manually in a short amount of time.

We have now published two tutorials demonstrating how anyone can do this in less than 30 seconds:

- Android smartphone and tablet tutorial: https://youtu.be/dFizYVCvxtI
- Apple iOS iPhone and iPad tutorial: https://youtu.be/d7ju7b-2JTo

We will in the future develop additional tutorials.

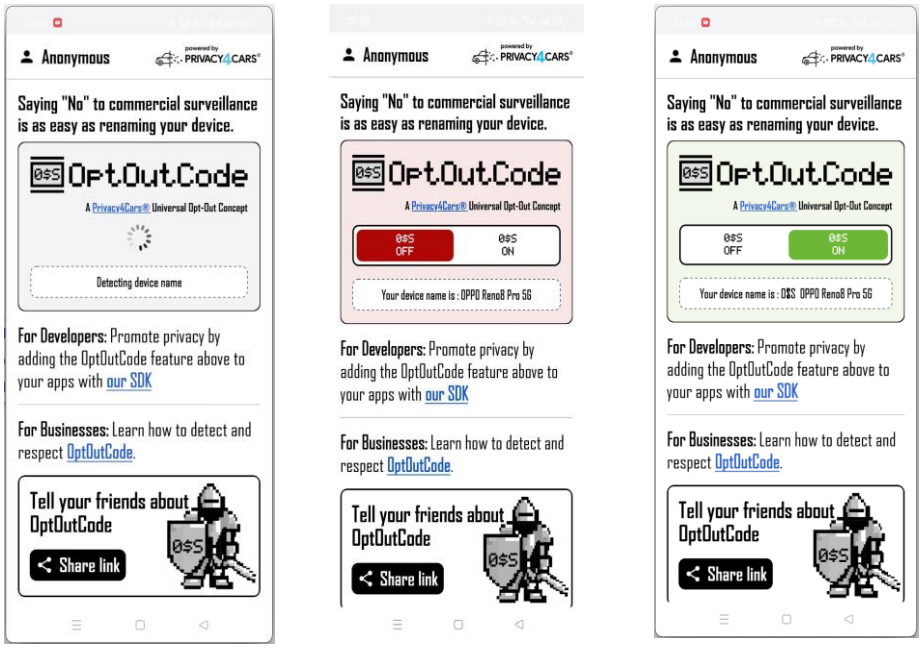
(c) The OptOutCode app and SDK:

We decided to develop an app even though it takes less than 30 seconds to turn on OptOutCode on a smartphone or tablet manually. The app gives users another option - to automatically turn on OpOutCode in just a few seconds.

The OptOutCode app for GooglePlay was published on December 9th, 2023 and is at https://play.google.com/store/apps/details?id=com.privacy4cars.optoutcode. Readers are encouraged to try it (the app does not collect data) readers if they have an Android smartphone or tablet. The iOS version was been submitted for publication on Apple's App Store on December 5th, 2023 and is currently under review. A demo video of the OptOutCode app is publicly available on the Privacy4Cars YouTube channel at: https://youtube.com/shorts/ZmVz2gBgHxo?feature=share

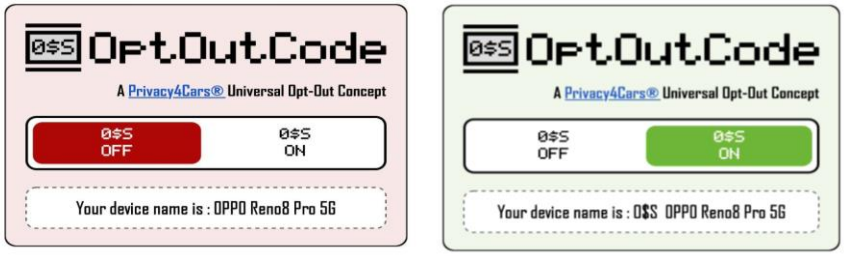
The OptOutCode app does three things:

A. **The OptOutCode app detects the name of the device it is installed on.** As stated in the original submission, this can be done automatically by any app who cares to attempt to listen to OptOutCode. For most consumers, all that is required is for Bluetooth to be on, as is common with consumers (the app checks, and gives users the option to turn Bluetooth on if it is off).



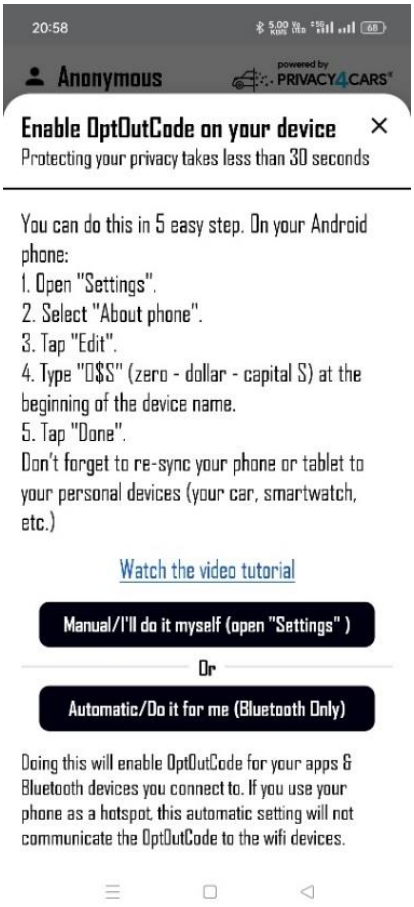
Upon launching, the OptOutCode app reads the device name and gives feedback

B. The OptOutCode app parses the first three letters of the device name and determines if OptOutCode is on or off. This information is visualized with a very clear red (off) or green (on) switch. The name of the device (including the "o$S" prefix, if present) is clearly displayed. The app clearly demonstrates that any app publisher could make the same determination and consequently opt-out the user from certain data processing.



The OptOutCode switch and device name feedback feature is available as an SDK so any app can add this functionality. Developers can inquire at https://optoutcode.com

C. If the OptOutCode signal is off, the OptOutCode app automatically or semi-automatically turns on OptOutCode by modifying the name of the device by adding the "o$S" prefix. The way this is accomplished varies slightly between Apple and Android users, and versions of Android. We also help users turn off OptOutCode if they no longer wish to have the UOOM signal broadcast for their device.



App publishers can easily take this feature (detect and switch on/off OptOutCode) and add it to their own apps with a Software Development Kit ("SDK"). They can request the code and the technical documentation on the https://optoutcode.com website.

3. Suggestions on how Google and Apple can improve on their recent policy changes to make it easier for consumers and companies to use OptOutCode in specific scenarios

Adoption of Universal Opt-Out Mechanisms can face friction and limitations not because of technical challenges, but because of policies of large tech players. An analysis on which browsers support Global Privacy Control recently highlighted how this can be the case[4] (California started to take steps to mandate major browsers to support GPC[5]). Similarly for OptOutCode, Apple and Google could very easily restore, improve, or harmonize recent policy changes to their stores and mobile Operating Systems so that both

[4] *See also*, Aaron Massey and Keir Lamont, *Survey of Current Universal Opt-Out Mechanisms*, Future of Privacy Forum, Oct. 12, 2023, available at: https://fpf.org/blog/survey-of-current-universal-opt-out-mechanisms/#:~:text=Google%20Chrome%2C%20Microsoft%20Edge%2C%20and,that%20natively%20support%20the%20GPC ("Google Chrome, Microsoft Edge, and Safari do not natively support the GPC signal").

[5] Maureen Mahoney, *CPPA Agenda Item 5 – Legislation Update & Agency Proposals*, Nov. 27, 2023, available at: https://cppa.ca.gov/meetings/materials/20231208_agenda_item5.pdf.

consumers and companies can adopt OptOutCode as a UOOM with the same ease they used to have prior to those policy modifications.

Mobile phone with OptOutCode on, synched with a vehicle and expressing an opt-out preference. Google and Apple OS policy changes do not affect Bluetooth or WiFi protocols hence do not affect OptOutCode's opt-out requests for IoTs

Android: starting in version v.12, if Bluetooth is off on a smartphone/tablet, and an app wants to read the name of that device to determine if OptOutCode is on or off, Google added an authorization request.[6] Some consumers may be shown a notification warning them that the app they are using wants to be able to "find, connect to, and determine the relative position of nearby devices". If all an app is trying to do is to read the name of the device, and not access the Bluetooth features, this new message may unreasonably deter privacy-conscious consumers from using OptOutCode.

We recommend that, whenever an Android app is only trying to read the name of a device (e.g. to detect OptOutCode) and not access the full Bluetooth capabilities, Google rolls back this notification (as is the case with many devices in circulation). Google could further improve by adopting a generic name for a device that includes the OptOutCode prefix (as we are suggesting for Apple). Either change would be very easy to carry out.

Android devices v.12 and above display a misleading message that may scare consumers away from using OptOutCode for their mobile apps and connected IoTs. OptOutCode only reads the name of a device, and does not finds, connects to, or determines the relative position of nearby devices.

[6] Android Developers, *Bluetooth permissions*, Nov. 30, 2023, available at https://developer.android.com/develop/connectivity/bluetooth/bt-permissions

Mobile iOS: Starting with iOS 16, if an app asks for the *user-assigned device name*, instead of the actual name of the device (e.g. "0$S Ravi's iPhone 13 Pro", which would include the prefix "0$S" if OptOutCode was turned on), Apple returns a generic device name instead by default (e.g., "iPhone"). Apple makes it still possible for an app to read the actual device name (inclusive of the OptOutCode prefix) if apps request it through a specific app submission process – proving this is an artificial constraint driven entirely by policy. Apple could easily preserve its intent to limit access to the real name of a device, yet pass along the OptOutCode information (i.e. if the real device name is "0$S Ravi's iPhone 13 Pro", Apple could tell apps its generic name is "0$S iPhone"). This change would be very easy to carry out.

Arguably, since both Google and Apple can determine if a device on their platform contains the "0$S" prefix or not, they can consequently determine if a consumer is expressing a request to universally opt-out, which may become a legally binding request if OptOutCode is approved in Colorado or other jurisdictions. Consequently, Apple and Google may feel compelled to seamlessly pass that signal along to publishers, which as illustrated above is a matter of policy and is straightforward to implement.

4. Approving OptOutCode as a valid UOOM in Colorado would be an effective mechanism for reducing the financial incentive many tech companies have to monitor, target, and influence Colorado residents, including some of the most vulnerable: children and teens.

The Colorado Attorney General's Office is currently part of a bipartisan group of state AGs suing Meta in the U.S. District Court for the Northern District of California for privacy violations and to prioritize the protection of kids' safety, mental health, and data online. It is our understanding that the complaint includes allegations that Meta deliberately deployed highly manipulative algorithms and technological tools to attract and sustain engagement of young users on Facebook and Instagram. These actions were allegedly taken with the intent to collect personal information from its users, including children without parental consent, for advertisers.

We believe it is important to point out that, regardless of the outcome of the legal proceedings, should Colorado confirm OptOutCode as a valid opt-out mechanism, OptOutCode may become the most effective tool Colorado residents have to protect themselves and their family members from the mass data collection, targeting, and influencing tech companies currently perform. Being a Universal opt-out mechanism, Colorado would not have to invest precious resources into suing a small subset of specific tech companies and hope that the rest of the AdTech ecosystem "gets the message". OptOutCode would make it easy for Colorado residents to say "no" to essentially all companies, all platforms, all apps, and all IoTs regardless of whether they are a very large, well known tech company (e.g. social media, search, mapping, shopping, etc.) or a less known entity (e.g. gaming, edu-tech, data brokers, etc.) for which it would be very difficult

for Colorado residents to be aware that their data or the data of their children is being harvested and monetized.

If all Colorado residents had to do was to rename their own and the devices of their children to opt out of certain data processing, sharing, and selling, this would accomplish two things:

1. It would take away the financial incentive companies currently have to nudge users into "consenting" by default (e.g. by downloading an app or purchasing a vehicle), and proceed to spy on them for their economic advantage; and
2. It would require those same companies to convince users to either turn off OptOutCode or to override the OptOutCode signal, which would require a prominent opt-in (i.e. the default becomes not collecting, instead of collecting data) and to invest in providing consumers, and particularly children, safer experiences online, on their apps, and with their devices.

As the dad of two young girls who face increasing pressure to be on social media, our CEO cannot imagine why any Colorado parent would not want to take a few seconds to activate OptOutCode on their own and their children's devices.

Conclusions

To summarize our comments, we want to emphasize that (1) OptOutCode is complementary to GPC, (2) there are now more OptOutCode tools available for consumers and businesses to adopt it as their opt-out mechanism, and (3) Small changes by the part of Google and Apple could facilitate the adoption of OptOutCode for apps, and (4) OptOutCode can be an effective way to take incentives away from tech companies to commercially surveil Colorado residents, including children and teens.

Thank you again for shortlisting OptOutCode and for the opportunity to submit our public comments.