

Exercising the CCPA Opt-out Right on Android: Legally Mandated but Practically Challenging

Sebastian Zimmeck
Wesleyan University
Middletown, Connecticut, USA
szimmeck@wesleyan.edu

Nishant Aggarwal
Wesleyan University
Middletown, Connecticut, USA
naggarwal@wesleyan.edu

Zachary Liu
Wesleyan University
Middletown, Connecticut, USA
zliu01@wesleyan.edu

Sage Altman
Wesleyan University
Middletown, Connecticut, USA
jaltman01@wesleyan.edu

Konrad Kollnig
Maastricht University
Maastricht, Netherlands
konrad.kollnig@maastrichtuniversity.nl

Abstract

Many mobile apps' business model is based on sharing user data with ad networks to deliver personalized ads. The California Consumer Privacy Act (CCPA) gives California residents a right to opt out. In two experiments we evaluate to which extent popular Android apps enable California residents to exercise their right. In our first experiment—manually exercising the right via app-level UIs—we find that only 48 out of 100 apps implement a respective setting, which suggests that CCPA opt-out right compliance on the Android platform is generally low. In our second experiment—automatically exercising the opt-out right by sending Global Privacy Control (GPC) signals—we find for an app dataset of 1,811 apps that GPC is largely ineffective. While we estimate with 95% confidence that 62%–81% of apps in our app dataset must respect the CCPA opt-out right, many apps do not do so. Our evaluation of disabling apps' access to the AdID—which is technically not intended for exercising the CCPA opt-out right but could be practically effective—does not change our conclusion. For example, when sending GPC signals and disabling apps' access to the AdID, 338 apps still had the ccpa status of the ad network Vungle set to `opted_in` while only 26 had set it to `opted_out`. Overall, our results suggest a compliance gap as California residents have no effective way of exercising their CCPA opt-out right on the Android platform; neither at the app nor at the platform-level. We think that re-purposing the Android AdID setting as an opt-out right setting with legal meaning under the CCPA and other laws could close this gap and improve users' privacy on the platform significantly.

Keywords

global privacy control, gpc, opt-out, app privacy, online privacy

1 Introduction

The business model of many mobile apps is based on advertising. Many apps rely on personalized advertising and share personal information with third-party ad networks, data brokers, and other

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license visit <https://creativecommons.org/licenses/by/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.

Proceedings on Privacy Enhancing Technologies YYYY(X), 1–18
© YYYY Copyright held by the owner/author(s).
<https://doi.org/XXXXXXX.XXXXXXX>

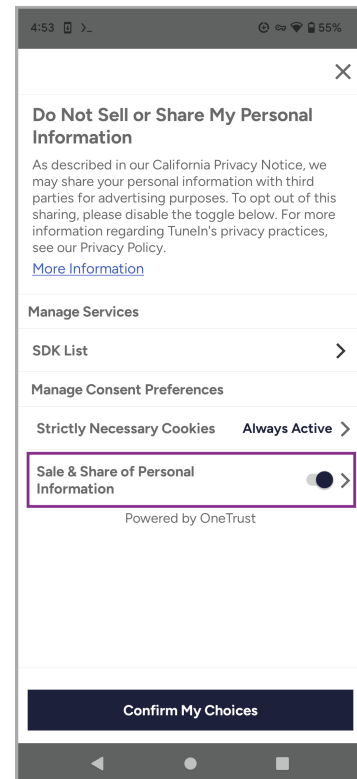


Figure 1: The *TuneIn Radio: Music & Sports* app [37] allows California residents to opt out of the selling and sharing of personal information per the CCPA.

companies in the online ad industry. However, such *cross-context behavioral advertising* is often not transparent and exposes users to privacy risks without control over the sharing of their data [86]. The California Consumer Privacy Act (CCPA) gives California residents a right to opt out of the selling and sharing of their personal information, including cross-context behavioral advertising. Mobile apps that are subject to the CCPA opt-out right are required to provide California residents functionality to exercise their right. Figure 1 shows an opt-out screen for one such app. In this study we evaluate to which extent popular apps on the Android platform

enable California residents to exercise their CCPA opt-out right, how they can do so, and which effect, if any, exercising the right has. We focus on the Android platform as its apps have been shown to share personal information more broadly than their counterparts on the iOS platform [54].

While app-level opt-out UIs, as shown in Figure 1, are one way to exercise the opt-out right, they are not the only way. The Office of the California Attorney General is also enforcing the opt-out right as expressed via Global Privacy Control (GPC) [81, 83], a technical specification for opting out [91]. Per the CCPA, a “business shall treat [...] opt-out preference signal[s] as a valid request to opt-out of [the] sale/sharing [...] for [a] browser or device. [12]”¹ Compliance with GPC is required in California since January 2021 [6]. However, achieving compliance is challenging for app operators since Android currently does not have a platform-level GPC setting.² Thus, the effectiveness of GPC on Android is unclear and has not been studied in previous research. We see our study as a GPC requirement evaluation of the Android platform: without platform-level GPC support, to which extent do Android apps respect California residents’ opt-out rights under the CCPA?

Despite the lack of platform-level GPC support, there is already an opt-out setting on Android. While not intended for exercising legal opt-out rights, if a user has opted out using the AdID setting, Google prohibits app operators to use the AdID for creating user profiles for advertising purposes or for targeting users with personalized advertising [30]. Google requires that all apps uploaded or published to the Google Play store must generally use the AdID in lieu of any other device identifier for any advertising purposes [26]. Thus, as part of our evaluation we also study the effect of disabling the AdID. We explore whether opting out using the AdID setting effectively results in exercising the CCPA opt-out right.

We evaluate the effectiveness of opting out on Android per the CCPA with two experiments and address the following research questions:

RQ1. UI Opt-out Evaluation: For a set of 100 popular Android apps, do those apps enable California residents to opt out per the CCPA, how can they do so, and which effect, if any, does exercising the opt-out right have? (Section 5)

RQ2. GPC Opt-out Evaluation: For a set of 1,811 popular Android apps, what effect does sending GPC signals have for opting out per the CCPA? What effect does disabling the AdID have? (Section 6)

By addressing these questions, we aim to advance legally mandated opt-out rights on mobile platforms. More broadly, we view our study as a contribution towards giving users more control over the sharing of their data on mobile platforms. The Android and iOS platforms are currently in a transitional phase. Mobile app operators are required to respect users’ GPC signals as valid means of exercising opt-out rights in jurisdictions in which GPC is in effect. However, they lack platform-level support in form of native Android and iOS GPC settings and respective APIs. To that end, we propose to re-purpose the current Android AdID setting as a platform-level opt-out setting with legal meaning (Section 7).

¹CCPA Regulations §7025(c)(1).

²The same is true for iOS, other mobile platforms, IoT platforms, and, broadly, any other platform beyond the web.

Addressing our research questions requires a combination of legal and technical analysis. In the following, we will discuss related work (Section 2), provide a brief background discussion on the application of the CCPA opt-out right on mobile platforms (Section 3), and describe our methodology for detecting apps that are non-compliant with the right (Section 4). Based on this groundwork we will then address our research questions and discuss the practical implications of our findings for the Android platform.

2 Related Work

Our work builds on previous studies on the dynamic analysis of mobile apps’ data practices and privacy compliance (Section 2.1), opting out of ad tracking in mobile apps (Section 2.2), and privacy preference signals (Section 2.3).

2.1 Dynamic Analysis of Mobile Apps’ Data Practices and Privacy Compliance

Our study makes use of dynamic analysis of mobile apps for purposes of privacy compliance analysis. Early studies in this research area focused on modifying mobile operating systems to observe personal data traversing through the systems. Enck et al.’s TaintDroid [22] falls in this category for Android as does Agarwal’s and Hall’s ProtectMyPrivacy [1] for iOS. While this operating system-focused approach can give highly accurate insights into apps’ data flows, the growing complexity of mobile operating systems makes it increasingly challenging. Thus, more recent studies tend to focus on the capture and analysis of apps’ network traffic [58, 75, 76, 80], which is also our approach. In the closest work to ours, Kollnig et al. performed a dynamic analysis of the network traffic of 1,297 Android apps and found that while most engaged in third-party tracking, only few obtained user consent before doing so [52]. While they selected their apps from the Google Play store randomly, we selected apps based on Google’s lists of popular apps as those are most likely to rely on an ad-based business model that implies selling of personal information or sharing such with third parties (Section 3.1). Nguyen et al. [64, 65] extended the work of Kollnig et al. and found that 24,838/86,163 (29%) apps sent personal data to data controllers without the user’s prior explicit consent. While previous studies focused on EU law, we focus on the CCPA.

2.2 Opting Out of Ad Tracking in Mobile Apps

In many cases, the lack of consent is the result of a coordination failure. Specifically, most third parties rely on app operators to obtain consent on their behalf but in many cases fail to put in place robust measures to ensure operators can actually do so [52]. Consent Management Platforms (CMPs), such as OneTrust [70], provide software integrations to assist operators in obtaining consent. For Apple devices, the platform itself includes a consent setting. With iOS 14.5 Apple introduced mandatory choice prompts. In doing so, Apple deviated from its earlier implementation of the ad tracking setting as an opt-out mechanism similar to that implemented on Android since 2013. However, Apple is facing challenges to enforce its App Tracking Transparency framework [55]. Across platforms, there are also usability challenges. Examining 100,000 Android apps, Chen et al. found that 36.3% of privacy settings identified in these apps are hard to find due to unclear user interface designs, which

impact users’ privacy because 82.2% of the observed settings are set to disclose data by default [13].

Users often do not know which data is collected from them and by whom [89]. Industry concentration has significantly increased the breadth and depth of data accessible to individual companies engaging in data collection [8]. For a long time mobile platforms have had dedicated identifiers to enable third-party tracking. On iOS, Apple rolled out the Identifier for Advertisers, alongside an opt-out setting from ad tracking, in 2012 [84]. Google quickly followed suit for Android by rolling out a similar mechanism in 2013 [84]. These initiatives had the goal of moving away from using permanent device identifiers, such as the Unique Device Identifier on iOS or the Android_ID on Android, for advertising purposes. Permanent identifiers cannot be reset by users and, thus, entail identification risk. In the wake of these developments, various self-help tools for blocking ad tracking have emerged [40, 53, 58].

To exercise their legal opt-out rights for various US jurisdictions, users can use Consumer Reports’ Permission Slip app, which has a human in the loop for performing some opt-out tasks [15]. Further, OptOutCode is a platform-agnostic proposal to automate opting out based on users’ prefixing the names of their devices with “0\$” for “do not (0) sell (\$) or share (S)” personal information [74].³ The Digital Advertising Alliance, an ad industry association, provides the AppChoices app [20]. However, despite these tools, privacy choices have historically been more limited on mobile platforms compared to the web. This development is the result of the lag of privacy mechanism implementations on mobile platforms.

2.3 Privacy Preference Signals

Recently, privacy preference signals have re-emerged and present an increasingly viable opt-out method [43]. However, various legal, technical, usability, and accountability challenges persist [44]. Automating privacy choices via privacy preference signals has been tried before. The Platform for Privacy Preferences Project (P3P) was an early signal to help people understand data practices and automate opt-outs and other privacy choices based on machine-readable privacy policies [16, 17]. Advanced Data Protection Control (ADPC) follows in P3P’s footsteps and is developed for EU law [45]. Perhaps, the most well-known signal, Do Not Track (DNT) [23], was developed from 2009 as a binary signal for users to express their opt-out of tracking towards websites and other online services [9]. However, DNT, just as the other signals, was never broadly adopted because no law mandates compliance. Recently, a decision of the Landgericht Berlin [57]—requiring LinkedIn to respect DNT signals—revitalized DNT. However, so far the decision remains an outlier. As a successor to DNT, GPC [91] is currently emerging as the standard for exercising opt-out rights. Thus, in our study we focus on GPC.

GPC is a binary signal with which users can express their Do Not Sell Or Share preference [91]. Most importantly, compliance with this preference is required under the CCPA and has been enforced by the Office of the California Attorney General [81, 83]. Our GPC analysis is based on the methodology developed by Zimmeck et

al. for the web [92], which we adapt for use on the Android platform. The basic idea is to inject GPC headers into all apps’ outgoing HTTP requests to detect changes in app behavior that could indicate whether the opt-out via GPC is respected or not. For example, we evaluate whether GPC signals are propagated to third parties by measuring respective changes in their US Privacy Strings [49]. If apps do not notify ad networks and other third parties of California residents’ opt-out preferences by setting privacy flags, such omission indicates a CCPA violation [92]. In addition to measuring the effect of sending GPC signals, we also measure the effect of disabling the AdID.

3 Legal Background

Over the past few years many countries and various states in the US have adopted new privacy laws. In our study we focus on California’s CCPA and its implementation via the CCPA Regulations.

3.1 The CCPA Opt-out Right

The CCPA gives consumers, i.e., California residents,⁴ a right to opt out.⁵ The right does not apply to residents of other states or countries. Specifically, a consumer has the right “at any time, to direct a *business* that *sells or shares personal information* about the consumer to third parties not to sell or share the consumer’s personal information.”⁶ Whether an app operator is running a “business” depends on annually buying, selling, or sharing the personal information of 100,000 or more consumers or households.⁷ For this determination Samarin et al. used the number of app installs [77]. We rely on app operators’ self-declaration of CCPA applicability in their privacy policies (Sections 4.3 and 4.4), which represents a lower bound since there may be additional apps that are subject to the CCPA but whose operators do not declare so. This approach also has the advantage of identifying a business across apps. For example, an operator may have multiple apps, each of which does not reach the threshold for CCPA applicability on its own.

For the opt-out right to be applicable, the app operator must also “sell” or “share” personal information. “Selling” means to communicate a consumer’s personal information to a third party for monetary or other valuable consideration.⁸ “Sharing” means to communicate a consumer’s personal information to a third party for cross-context behavioral advertising.⁹ The concept of “sharing” was introduced to the CCPA by the California Privacy Rights Act, an amendment to the CCPA, to remove any doubt that the CCPA applies to cross-context behavioral advertising [85]. Evidence for selling or sharing can consist of dedicated CCPA opt-out of sale or share links, respective opt-out implementations, or statements of applicability of the CCPA opt-out right in privacy policies [67]. As the enforcement actions of the Office of the California Attorney General show [83], the integration of third-party libraries for ads personalization falls squarely under the definitions of selling and

⁴CCPA §1798.140(i).

⁵CCPA §1798.120.

⁶CCPA §1798.120(a) (emphasis added).

⁷Alternatively, thresholds of annual gross revenues in excess of 25 million dollars or deriving 50% or more of annual revenues from selling or sharing consumers’ personal information can be used to determine whether an entity qualifies as a “business” per CCPA §1798.140(d)(1).

⁸CCPA §1798.140(ad)(1).

⁹CCPA §1798.140(ah)(1).

³This idea is similar to Google’s opt-out solution for Google Location services access points [34]: “To opt out, change the SSID (name) of your Wi-Fi access point (your wireless network name) so that it ends with ‘_nomap.’ For example, if your SSID is ‘12345,’ you would change it to ‘12345_nomap.’”

sharing. Thus, for our GPC opt-out evaluation we rely on an app’s integration of an ad network that discloses in its privacy policy that it is “buying” or “collecting” personal information or “selling” or “sharing” such (Section 4.4).

3.2 Methods for Opting Out

The CCPA Regulations outline several methods through which businesses must allow consumers to exercise their opt-out right.¹⁰ As a general guideline, they require businesses to consider the methods by which they interact with consumers, the manner in which they collect the personal information that they make available to third parties, available technology, and ease of use by the consumer when determining which methods consumers may use to submit requests to opt out of selling and sharing with at least one method reflecting the manner in which the business primarily interacts with the consumer.

For websites the CCPA requires businesses to provide a “clear and conspicuous link on the business’ internet homepages, titled ‘Do Not Sell or Share My Personal Information,’ to an internet web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale or sharing of the consumer’s personal information.”¹¹ In this regard, cookie banners or cookie controls, by themselves, are insufficient because selling and sharing practices are not identical to cookie practices.¹² While there may be some overlap—for example, disabling targeting cookies may also reduce selling and sharing of personal information—the CCPA requires a dedicated method for submitting requests to opt out of the selling and sharing of personal information.

In addition to links, the CCPA Regulations mandate that businesses respect opt-out preference signals: “A business that collects personal information from consumers online shall, at a minimum, allow consumers to submit requests to opt-out of sale/sharing through an opt-out preference signal and at least one of the following methods: an interactive form accessible via the ‘Do Not Sell or Share My Personal Information’ link, the Alternative Opt-out Link, or the business’s privacy policy if the business processes an opt-out preference signal in a frictionless manner.”¹³ The idea is that businesses should (1) prominently notify consumers of the selling and sharing of personal information and how they can opt out and (2) process their opt-out preferences via automated opt-out preference signals. If a business processes opt-out preference signals in a frictionless manner, it is not required to provide any opt-out links.¹⁴ Businesses are required to treat opt-out preference signals as a valid request to opt out of the sale or sharing of personal information for a browser or device and any consumer profile associated with that browser or device, including pseudonymous profiles.¹⁵

¹⁰CCPA Regulations §7026(a).

¹¹CCPA §1798.135(a)(1).

¹²CCPA Regulations §7026(a)(4).

¹³CCPA Regulations §7026(a)(1). The “Alternative Opt-out Link” means a link combining the two separate “Do Not Sell or Share My Personal Information” and “Limit the Use of My Sensitive Personal Information” links into one “Your Privacy Choices,” or, “Your California Privacy Choices” link per CCPA Regulations §7001(b) and §7015.

¹⁴CCPA Regulations §7025(e).

¹⁵CCPA Regulations §7025(c)(1).

3.3 Opting Out via GPC

The most important privacy preference signal for purposes of the CCPA is GPC, which is a draft standard at the W3C [91]. GPC signals are transmitted from users’ clients to servers via request headers. Servers can also query a user agent’s GPC status via the GPC DOM property. GPC can be set to 1 (header) or true (DOM property) to express a user’s opt-out as defined by applicable law in the user’s jurisdiction. Thus, GPC can be used in multiple jurisdiction and will have the meaning that a particular law or regulation attaches to it. GPC aims to enable users to exercise their opt-out rights beyond individual websites and apps for sets of sites or apps.

Recent studies evaluating the usability of GPC suggest that most users understand its purpose and that they would turn it on if it were more broadly available [90, 92]. Its rate of adoption by website operators appears to increase slowly and steadily estimated at a few percentage points per year [42]. Compliance with GPC is required in California (since January 2021) [6], Colorado (since July 2024) [14], Connecticut [68] (since January 2025), and New Jersey [63] (since July 2025). Notably, in these jurisdictions the opt-out right and GPC are not limited in their applicability to websites but apply to mobile apps as well.

3.4 Opting Out via GPC on Mobile Apps

The Office of the California Attorney General brought various enforcement actions against mobile app operators for not respecting consumers’ opt-out right [81–83]. Consumers have a right to opt out on every “device,” which the CCPA defines as “any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.”¹⁶ Thus, the International Association of Privacy Professionals, a nonprofit and non-advocacy membership association of privacy professionals, recommends for mobile apps that “[a]t a minimum, mobile apps should [...] include a functional ‘Do Not Sell or Share My Personal Information’ link in the app [...]” [19]. However, opting out via GPC on mobile devices presents a challenge.

The core problem is the lack of a native and platform-level GPC setting on Android.¹⁷ This technical gap is in conflict with the CCPA Regulations, which mandate that “[t]hrough an opt-out preference signal, a consumer can opt-out of sale and sharing of their personal information with all businesses they interact with online *without having to make individualized requests with each business*.”¹⁸ This discrepancy between the law and the technical reality raises crucial questions: How are app operators expected to facilitate GPC opt-out signals without platform-level support. Do they even anticipate receiving such signals? On a fundamental level, as mobile apps are using the web for their client–server communication, including for ad-serving, they can generally process GPC signals in the same way as websites. Thus, our study investigates to which extent this is actually the case.

4 Methodology

We study the effectiveness of exercising the CCPA out right via Android apps’ user interfaces and sending GPC headers.

¹⁶CCPA §1798.140(o).

¹⁷For that matter, such settings are lacking on any platform but the web.

¹⁸CCPA Regulations §7025(a) (emphasis added).

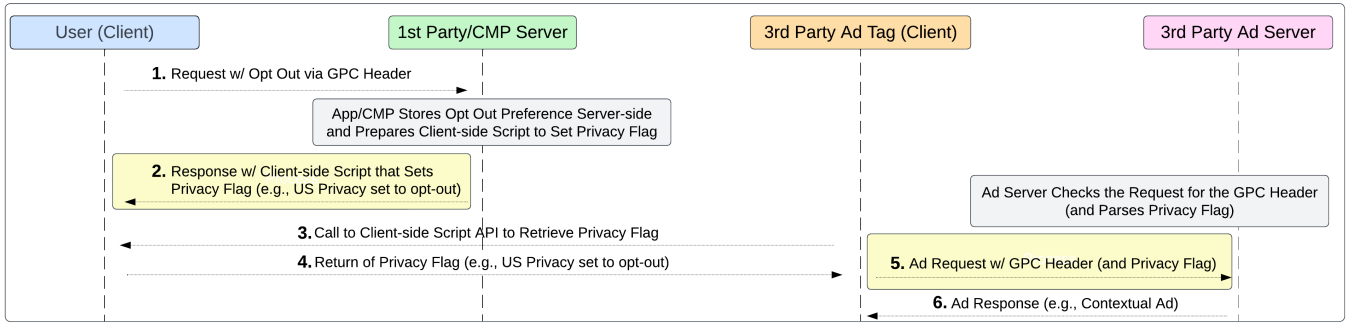


Figure 2: Exercising the opt-out right via GPC. 1. An HTTP request from the user’s device is sent with a GPC header. By sending this header the user is exercising the opt-out right. 2. The HTTP response contains a script for setting a privacy flag client-side. By identifying such a privacy flag and its value we determine whether the opt-out has been respected. App operators can implement the logic for processing privacy flags themselves or use the library of a CMP. 3–4. A third-party ad network queries the privacy flag via its ad tag that the app operator integrated in its app. 5. The flag may be attached to ad requests from the user to the ad network, which is the second point that we use to determine whether the opt-out has been respected. The ad network can also act directly upon receiving GPC signals, which are attached to all requests as headers. 6. The ad network responds to ad requests from opted out users with an ad not based on sold or shared personal information.

4.1 App Dataset

For our evaluation we downloaded a set of popular free apps from the US Google Play store in August 2023. Following previous work [41, 78, 79], we identified the apps based on Google’s lists of popular apps in 49 app categories on the Google Play store. Each list contained 45 apps. The 49 app categories include 17 game categories [29]. The sets of apps in the different categories are disjoint as each app can be assigned one category on the Google Play store [29]. The 45 apps listed for each of the 49 categories are “heavily influenced by popularity” [28].¹⁹ We selected popular free apps for our study because those are most likely to rely on an ad-based business model that implies selling personal information or sharing such with third parties (Section 3.1). Using Raccoon [72], we successfully downloaded 1,896/2,205 (86%) of the listed apps. The remaining apps were incompatible with our test device, removed from the Google Play store before we could download them, or not successfully downloaded. We made two download attempts per app. For our GPC opt-out evaluation we successfully performed a dynamic analysis of 1,811/1,896 (96%) apps resulting in our *app dataset*. For the remaining apps we did not collect any or only little network traffic, for example, due to apps’ crashing during the analysis.

4.2 Measuring Opt-out Effects

We measure the effects of opting out—i.e., whether an app stopped selling or sharing personal information—in three ways: we measure whether an app (1) sets CCPA privacy flags to opt out (such as the US Privacy String [49]), makes fewer connections to ad tracking domains, or (3) discloses fewer device identifiers to third parties. As to the first measure, it is the responsibility of ad networks to provide functionality in their ad libraries for app operators to identify ad requests to which the CCPA opt-out right applies. If an app operator enables such functionality, a privacy flag should be set on the

user’s device and possibly also be attached to outgoing ad requests to third-party ad networks, as shown in Figure 2. Thus, as privacy flags are generally communicated client-to-server, for example, ad networks retrieve the US Privacy String from an Android’s device local SharedPreferences [48], we can use client-side analysis to determine the opt-out status. If a third party receives an ad request with a privacy flag, it knows to discard personal information upon receipt and serve an ad not based on sold or shared personal information.

Beyond changing privacy flag values, a successful opt-out can manifest itself through other observable changes in an app’s behavior. An app can comply by not making any ad calls. Thus, monitoring an app’s connections to third-party ad tracking domains serves as another indicator for opt-out adherence. Further, an app may continue to connect to third-party ad tracking domains but stop the sharing of identifying data. Thus, we also examine the impact of GPC signals on data sharing practices, specifically, the disclosure of device identifiers. A reduction in the sharing of such identifiers can indicate that an opt-out request has been respected since a third party is now more limited in associating particular data with a particular user or device.

Android’s ad ecosystem is integrated into the broader online ad ecosystem and relies on the delivery of ads via the web protocol. An opt-out request, and the corresponding setting of a privacy flag, can be initiated in several ways. Figure 2 shows how a user initiates an opt-out request by sending a GPC header. However, it is likely that many apps do not yet have functionality to process GPC signals. Especially, since Android does not have a platform-level GPC setting, apps operators may not have set up server-side code to detect GPC signals. Thus, we also evaluate to which extent privacy flags are set via in-app opt-out interfaces or disabling the AdID. The lack of platform-level support for GPC, however, does not principally change the legal status of GPC as a mandatory opt-out setting on Android and, more generally, any web-based platform.

¹⁹ Apps in the Communication and Productivity categories had the most installs while those in the Events category had the least. Appendix Figure 12 shows the app install ranges for the apps in all 49 app categories.

4.3 UI Opt-out Evaluation

In our app-level UI opt-out evaluation, for determining whether the CCPA opt-out right is applicable to an app we relied on app operators’ respective declarations in their privacy policies. We first chose from our app dataset 100 random apps whose operators notify California residents in their privacy policies that they have a CCPA opt-out right. To ensure that a privacy policy is applicable to an analyzed app we relied on the link from each app’s US Google Play store Data Safety page to the policy. If necessary, we further followed links from a policy to US state- or California-specific policies. Similar to previous work [52], we categorize each app’s opt-out setting as follows:

- **Opt-out Right Setting:** The app has a dedicated CCPA opt-out setting, e.g., toggle or button, to opt out of the selling or sharing of personal information per the CCPA.
- **Generic/SDK/Cookie Opt-out Setting:** The app has an opt-out setting without mentioning that it relates to the selling or sharing of personal information or that users have a right to opt out. This category covers generic opt-out settings as well as settings for cookie and SDK opt-outs.
- **Opt-out Right Form:** The app has a CCPA right form, e.g., requiring California residents to enter their email address, to opt out of the selling or sharing of personal information or claim other CCPA rights.
- **Privacy Policy:** The app only has a privacy policy link but no opt-out setting inside the app. We do not count opt-out settings that are only accessible via a privacy policy. If there is just a link to a “privacy policy” inside the app, which then links to an opt-out setting, it would not be “clear and conspicuous” and insufficient per the CCPA if the app does not respect opt-out signals via GPC.
- **No Opt-out Setting or Privacy Policy:** The app is missing both an opt-out setting and a privacy policy link.

We evaluated whether an app has an opt-out setting, for example, under a “privacy settings” or “settings” menu. If clicking on such a menu item took us to an external website, we followed the respective procedure there. For a subset of 38 apps—those with opt-out right setting or generic/SDK/cookie opt-out setting—we performed a dynamic analysis. We did not evaluate apps with opt-out right form because submitting such form would not have immediate impact visible in the apps’ network traffic. For 31/38 apps we were able to capture the network traffic in our two test conditions. For the remaining apps we did not collect any or only little network traffic, for example, due to apps’ crashing during the analysis.

The two test conditions under which we evaluated each app are the following:

1. **Not Opted Out:** Use of the main functionality of the app (e.g., if the app is a game, play it) with the app’s opt-out setting, if any, set to not opted out. This condition is the base condition under which we expect an app to sell and share California residents’ personal information.
2. **Opted Out:** Use of the main functionality of the app with the app’s opt-out setting, if any, set to opted out.

During our evaluation we performed for each app a manual dynamic analysis. For each condition, we captured each app’s network

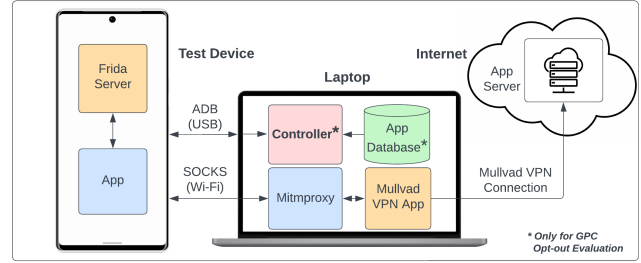


Figure 3: Overview of our dynamic analysis setup for capturing app network traffic. Appendix 11.1 contains a comprehensive description of our dynamic analysis for the UI and GPC opt-out evaluation.

traffic for 30 seconds, similar to previous work [52], using a Google Pixel 6a with Android 13, our *test device*. We found in preliminary tests that this time period is sufficient to understand the app’s ad tracking behavior and that the order of the conditions does not impact the results. If necessary to use the app, we created an account and logged into the app before evaluating the two test conditions. For each app, when switching conditions, we cleared the persistent storage and SharedPreferences of the test device. Upon an app’s request, we granted all permissions except for location permission as an additional measure to prevent apps from detecting our real location as we were not based in California.

For the analysis of network traffic, we followed the state-of-the-art in the literature: use of Mitmproxy [61] and circumvention of certificate pinning with Frida [24]. For capturing an app’s network traffic, we connected the test device to a laptop using Mitmproxy in SOCKS mode [61]. To issue commands to the test device, e.g., to start Mitmproxy, we connected the test device to the laptop via the Android Debug Bridge (ADB) [33]. We obtained a California IP address via a Mullvad VPN server [62] to ensure applicability of the CCPA. During our analysis we also manually took screenshots of the opt-out UI, if any. We performed our analysis in July and August 2025. Figure 3 shows an overview of our analysis setup.

4.4 GPC Opt-out Evaluation

In addition to our UI opt-out evaluation, we performed a GPC opt-out evaluation. The “selling” or “sharing” of personal information by an app operator corresponds to a third party’s “buying” or “collecting” of personal information. Thus, to determine whether an app is selling or sharing personal information we identified the most prevalent third-party tracking domains across all apps in our app dataset. Our starting point for this task was the X-Ray Tracker List [8, 51]. We found that a set of 29 third-party tracking domains from the X-Ray Tracker List lead to a 99% coverage with at least one tracking domain—whose privacy policy allowed to (1) buy or collect or (2) sell or share personal information per the CCPA—in each app in our app dataset (Section 6.1).²⁰ For the privacy policy evaluation we included developer documentation and looked for

²⁰We combined trackers with different subdomains in our app dataset into one domain to match the tracker domains in the X-Ray Tracker List. For example, we combined `app.adjust.com`, `view.adjust.com`, `app.us.adjust.com`, and `s2s.adjust.com` into `adjust.com`.

explicit references that—per the CCPA—allows the buying or collecting of personal information from app operators or the selling or sharing of such.

To illustrate, Meta’s policy [60] indicates that it is buying or collecting personal information per the CCPA via its libraries as it advises app operators integrating those that they may “share with Meta Personal Information about California residents which would otherwise constitute a Sale or Sharing [...]” In another example, per InMobi’s privacy policy [50], “InMobi may be deemed to be ‘selling’ personal information, [...]” indicating InMobi’s further downstream sale of California residents’ personal information after buying or collecting such from the app operators who integrate its libraries. We performed our evaluation conservatively. If a policy stated that a third party does not share or sell personal information per the CCPA, we accepted such statement as true. Our methodology could be applied to cover cases where the operator claims not to sell or share personal information but does so in practice, for example, as it appears from the operator’s app network traffic, possibly in combination with a privacy flag not set to opt-out. In such case the operator needs to either adapt the claim or cease the practice.

To evaluate the likelihood to which an app in our app dataset is part of a business, we selected a random sample of 100 apps from our app dataset for determining whether their operators self-declared to run a “business” in their privacy policies. We performed this analysis on the 83 sample apps in our app dataset that had a Google Play Data Safety page with a link to their privacy policy and were still available at the time of the sampling. Given that an app’s Data Safety page linked to a privacy policy, we assumed that the linked policy applies to the app.

The setup and procedure for our GPC opt-out evaluation is similar to our UI opt-out evaluation, though, automated. After downloading the apps, we ran an automated dynamic analysis for each app individually proceeding in batches for a total of two weeks with the analysis of one app taking about 5 minutes. We performed this analysis for the apps in our app dataset in October 2023. As shown in Figure 3, we instrumented the test device with a shell script, the *controller*, which ran on our laptop. The controller fetched an app from the app database on the laptop, installed it on the test device, ran it in the foreground under four test conditions, and uninstalled it. If an app update was triggered right after installing an app, it would not have been possible to run the app immediately afterwards, which we checked for.²¹

We wanted to find out if California residents can exercise their opt-out rights by sending GPC signals. To which extent do Android apps respect GPC signals despite the lack of platform-level API support for such? We were also interested in the effect of disabling the AdID. Thus, we tested each app under four conditions encompassing all possible combinations of access to the AdID (yes/no) and sending GPC signals (yes/no). Similar to previous work [52], for each condition, we captured each app’s network traffic for 30 seconds. We also added a timeout of 30 seconds before running an app’s first condition so that the app is fully initialized before

capturing of the network traffic begins [65]. The four test conditions under which we evaluated each app in our app dataset are the following:

1. **AdID:** The app has access to the AdID. This condition is the base condition under which we expect some apps to sell and share California residents’ personal information.
2. **AdID + GPC:** The app has access to the AdID, but all HTTP requests are sent with a GPC header. The app operator is prohibited from selling and sharing personal information per the CCPA. The app should notify integrated ad networks of the opt-out via respective privacy flags.
3. **No AdID:** The app does not have access to the AdID. Google prohibits targeting users with personalized advertising [30]. If the app recognizes the AdID setting as a valid opt-out preference per the CCPA, it should notify integrated ad networks of the opt-out via respective privacy flags.
4. **No AdID + GPC:** The app does not have access to the AdID, and all HTTP requests are sent with a GPC header. This condition evaluates the cumulative effect of no AdID access and GPC. The app should notify integrated ad networks of the opt-out via respective privacy flags.

In the AdID + GPC and No AdID + GPC conditions we injected GPC headers into all requests, for both HTTP and HTTPS, using Mitmproxy. In the AdID and No AdID conditions, we injected dummy headers into all requests to minimize any differences that might occur due to header injection in the other two conditions. In all four conditions the controller granted all permissions requested by an analyzed app at install time.²² We tested whether granting or denying permissions made a difference for apps’ ad tracking behavior, which was not the case. When switching conditions, our controller cleared the persistent storage and SharedPreferences of the test device.

4.5 Limitations

Our study has various limitations. First, our evaluation of the applicability of the CCPA opt-out right is based on privacy policies that app operators link from their app’s Play store Data Safety page. It may be that a policy is not applicable to an app or a policy does not distinguish between multiple apps or the operator’s website, each of which may have different data practices. Further, by its very nature, dynamic analysis only runs code partially leaving us with an incomplete picture of apps’ behavior. Also, for our GPC opt-out evaluation we evaluated apps without user interaction save for automatically enabling and disabling the AdID setting.²³ For determining opt-out effects we evaluated privacy flags, domain connections, and sharing of device identifiers. However, those are only proxies. For example, an ad network may simply disregard a user’s right despite a privacy flag being set to opt-out. Our methodology does not allow us to observe server-to-server data sharing, for example, of device identifiers. Further, some apps we evaluated

²¹Appendix 11.1 contains further details of our dynamic analysis with Appendix Figure 10 showing the procedure in detail.

²²Different from the UI Opt-out evaluation (Section 4.3), for the GPC opt-out evaluation we opted to grant apps location permission as we also wanted to explore location tracking. Appendix Figure 13 shows the top 50 permissions that the 1,811 apps in our app dataset declared in their manifest file.

²³Automatically enabling or disabling the AdID may be impacted by pop-up screens or other interruptions. We encountered some apps with unexpected AdID access. We manually re-analyzed these apps and confirmed the results (Section 6.2.3).

	Count	Confidence Interval
Opt-out Right Setting	30	21%–39%
Generic/SDK/Cookie Opt-Out Setting	8	3%–13%
Opt-out Right Form	10	4%–16%
Privacy Policy Link	45	35%–55%
No Opt-out Setting or Privacy Policy Link	7	2%–12%

Table 1: Counts of opt-out settings for the 100 apps for which we performed the UI opt-out evaluation and confidence intervals for the prevalence of respective settings in our app dataset. Figure 4 shows example UIs.

likely used encryption with certificate pinning. While we followed state-of-the-art methods for certificate-unpinning [54, 65, 88], we were likely not able to decrypt all encrypted traffic, which is an inherent limitation of any dynamic analysis of third-party code. For our identification of ad tracking domains we did not perform an independent evaluation and relied on previous research that led to creation of the X-Ray Tracker List [8, 51]. Similar to previous work [56], we used a commercial VPN, Mullvad, to simulate a California location so that the CCPA is applicable. Apps may have identified our real location, e.g., via Mullvad’s IP address or our time zone setting, and behaved differently. Thus, our results may not be an accurate reflection of app behavior for California residents. However, we are not aware of such behavior. Notably, in our GPC opt-out evaluation we did not notice different behavior in apps with and without GPS access.

5 UI Opt-out Evaluation

Main Result: Only 48 of the 100 apps we evaluated implement the legally mandated CCPA opt-out setting, which suggests that CCPA opt-out right compliance on the Android platform is generally low.

5.1 CCPA Opt-out Right Applicability

For all 100 apps for which we performed our UI opt-out evaluation we ensured that the CCPA opt-out right is applicable. The privacy policies of all 100 apps included respective statements.

5.2 Opt-out Effects

As Table 1 shows, only 48 out of 100 apps implement the legally mandated CCPA opt-out setting. The remaining 52 apps either have just a privacy policy link (45) or no opt-out setting or privacy policy link (7). As an example, calculating the confidence interval for the proportion of 45/100 (45%) apps with just a privacy policy link, using z-scores, indicates that with 95% confidence the true proportion of apps in our app dataset with only such link is 35%–55%. Thus, even without evaluating any network traffic, our results suggest the broad existence of non-compliance. While apps in some game categories tend to have higher percentages of non-compliant apps, non-compliance is generally observable across all app categories (Appendix Table 3).

Turning to our network traffic analysis, some apps did not reflect the opted out state in their privacy flags. Thus, even if California residents opt out, those apps are still selling and sharing personal information. Out of the 14 apps that included the third-party ad network Vungle [87], two apps still set the `ccpa` status flag to

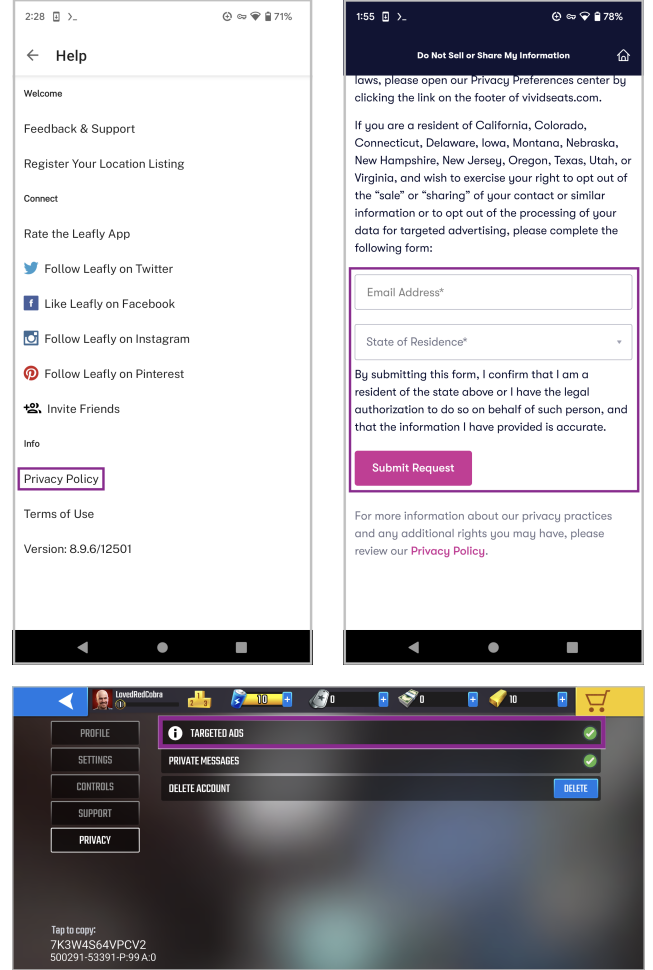


Figure 4: Example UIs of three apps: Leafly: Find Cannabis and CBD [35] with just a privacy policy link (top left), Vivid Seats | Event Tickets [38] with an opt-out right form (top right), and Pure Sniper: Gun Shooter Games [36] with a generic/SDK/cookie opt-out setting (bottom). Figure 1 shows an example UI of a dedicated opt-out right setting.

opted_in in the opted out condition so that Vungle continued to collect and buy personal information. Similarly, one app also still had Google’s Restricted Data Processing (RDP) [27] set to 0. These results show that opt-out rights are not always respected as app operators do not notify third parties of users’ opt-outs so that those remain opted in. We did not see differences for connecting to ad tracking domains and disclosing device identifiers between opted out and not opted out conditions.

6 GPC Opt-out Evaluation

Main Result: While we estimate with 95% confidence that 62%–81% of apps in our app dataset must respect the CCPA opt-out right, many apps do not do so. For example, when sending GPC signals and disabling apps’ access to the AdID, 338 apps still had the `ccpa`

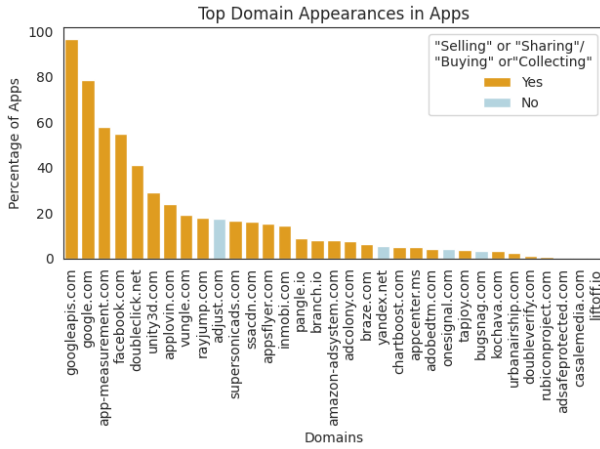


Figure 5: For 29/33 (88%) of the most prevalent ad tracking domains in our app dataset their privacy policies allow the “Selling” or “Sharing”/“Buying” or “Collecting” of personal information per the CCPA.

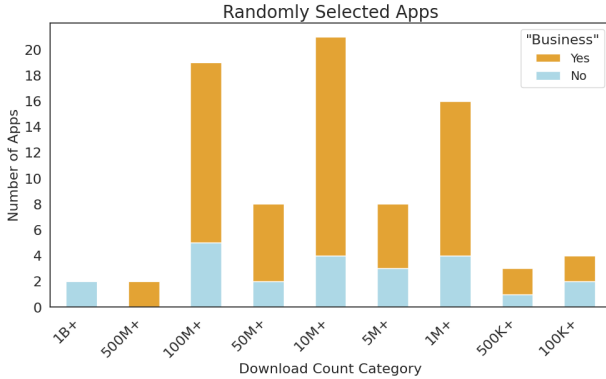


Figure 6: For 60/83 (72%) randomly sampled apps from our app dataset their privacy policies stated that the operators run a “business.”

status of the ad network Vungle set to `opted_in` while only 26 had set it to `opted_out`.

6.1 CCPA Opt-out Right Applicability

Evaluating how many apps are selling or sharing personal information, we find that 1,787/1,811 (99%) of the apps in our app dataset connect to at least one of the most prevalent 29 ad tracking domains with a privacy policy stating to (1) buy or collect or (2) sell or share personal information per the CCPA (Figure 5).²⁴ Further, for the random sample of 83 apps (Section 4.4), 60/83 (72%) of their policies implied that the app operators run a business per the CCPA by mentioning the applicability of the CCPA or the explicit selling or sharing of personal information (Figure 6). Thus, we estimate that $1,787 * 0.72 = 1,287$ apps in our app dataset are subject to the CCPA opt-out right. Calculating the confidence interval for the proportion

²⁴Performing the evaluation for all third-party tracking domains on the X-Ray Tracker List only increases the coverage by two apps to 1,789/1,811 (99%), which highlights the concentration of companies in the online ad industry.

of 60/83 (72%) sample apps, using z-scores, indicates that with 95% confidence the true proportion of app operators running a business is 63%–82%. Applying this range to the 1,787 apps that connect to at least one of the 29 most prevalent tracking domains, we arrive at an estimate of 1,126 to 1,465 (62%–81%) apps in our app dataset being subject to the CCPA opt-out right.

6.2 Opt-out Effects

Overall, we find little evidence that the apps in our app dataset respect GPC. Notably, we observe no substantial impact of GPC on apps’ notifications to third parties via the IAB’s US Privacy String [49] and company-specific privacy flags (Section 6.2.1). We also do not observe a decrease in the number of connections to ad tracking domains (Section 6.2.2) or the disclosure of device identifiers (Section 6.2.3).

6.2.1 Setting CCPA Privacy Flags. The IAB provides an industry-wide CCPA privacy flag in the form of the US Privacy String [49], to be implemented as an HTTP cookie or a JavaScript property.²⁵ We find that when opting out via GPC, privacy flags generally do not change to reflect the CCPA opt-out status. However, some apps opt out users regardless of whether they receive GPC signals or have access to the user’s AdID.

US Privacy String. For 199/1,811 (11%) apps in our app dataset we found a US Privacy String key, `us_privacy`, and a corresponding US Privacy String value in their network traffic. However, the value of the US Privacy String was rarely set to opt-out, that is, rarely had a Y in its third position, which would indicate a “Yes” for a California resident’s status of being opted out [49] (Figure 7). Also, disabling the AdID did not lead to substantially different opt-out rates as the comparison between the AdID and No AdID conditions shows (Appendix Figure 14). Overall, the rate of 1YY- US Privacy String values, which indicate that a California resident’s opt-out right is respected, is low regardless of the tested condition. Our results suggest that turning on GPC does not help California residents to exercise their CCPA opt-out right as measured via the US Privacy String. Disabling the AdID did not change this result.

Company-specific Privacy Flags. Our evaluation of company-specific privacy flags further confirms our findings. We evaluated privacy flags of three companies: Google, Supersonic/Unity, and Vungle. Table 2 shows counts and percentages of apps in our app dataset with left-column values indicating company-specific privacy flags set to opt-in status, middle-column values indicating opt-out status, and right-column values indicating opt-out percentages. Just as for the US Privacy String, company-specific privacy flags rarely changed when disabling the AdID or sending GPC signals. Generally, the apps for which we detected privacy flags with opt-out values had this status regardless of the GPC and AdID

²⁵On January 31, 2024 the US Privacy String was deprecated and integrated into the IAB’s Global Privacy Platform (GPP) that covers privacy flags for multiple US states and international jurisdictions [46]. The IAB now recommends use of GPP instead of the US Privacy String. GPP contains the usca California privacy section corresponding to the US Privacy String [47]. Since we performed our analysis before the deprecation date we focus here on the US Privacy String. Both the US Privacy String as well as its GPP equivalent can be stored on Android devices using `SharedPreferences` for the app context [46, 48].

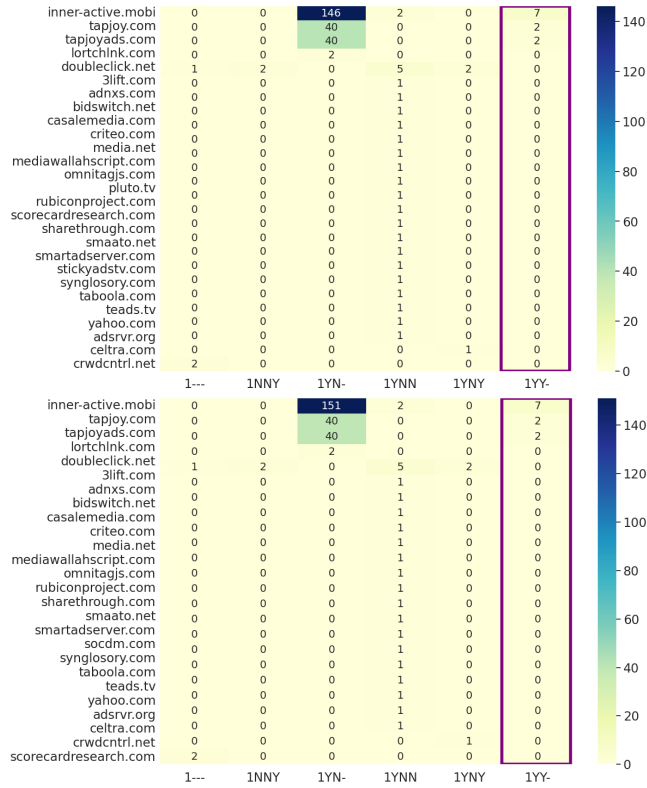


Figure 7: Counts of US Privacy String values in the No AdID (top) and No AdID + GPC (bottom) conditions. The rightmost columns show the opt-out counts of US Privacy String values that apps in our app dataset sent to third-party domains. For example, in the No AdID condition only 7/155 apps sent a 1YY- value to inner-active.mobi indicating the opt-out status while the remaining apps sent 1YN- (146/155) and 1YNN (2/155) values indicating the opt-in status. These results did not substantially change when enabling GPC in the No AdID + GPC condition. Notably, the number of apps sending a 1YY- value stayed the same (7/160). The counts are per app and mutually exclusive for a given domain but not across domains as one app can connect to multiple domains. We only include domains with at least one US Privacy String value in our network traffic.

	Google rdp 0, 1, %	Supersonic/Unity do_not_sell false, true, %	Vungle ccpa status opted_in, opted_out, %
AdID	12, 29, 71%	152, 2, 1%	339, 23, 6%
AdID + GPC	12, 30, 71%	154, 2, 1%	341, 23, 6%
No AdID	12, 31, 72%	156, 2, 1%	337, 24, 7%
No AdID + GPC	12, 31, 72%	155, 4, 3%	338, 26, 7%

Table 2: Counts and percentages of apps that set company-specific privacy flags. For example, when sending GPC signals and disabling apps’ access to the AdID, 338 apps still had the ccpa status of the ad network Vungle set to opted_in while only 26 had set it to opted_out, which corresponds to only 26/364 (7%) of the total apps.

setting. It seems that apps opt out all California residents by default or trigger the opt-out status when they detect requests from a

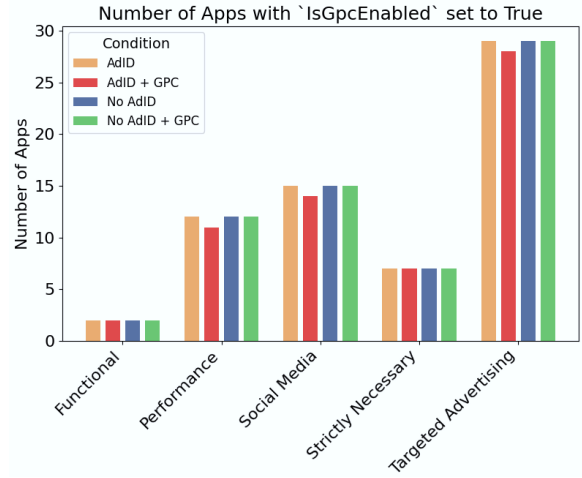


Figure 8: Counts of apps with IsGpcEnabled set to True for each category across test conditions. An app can set IsGpcEnabled for multiple categories.

California IP address. Notably, Google’s rdp flag was more often set to opt-out than to opt-in, albeit, at comparatively low levels. Generally it is evident that sending GPC signals does not make a substantial difference overall. Sending GPC signals does not have a major effect for opting out California residents per the CCPA as measured via company-specific privacy flags. Disabling the AdID does not lead to a different result either.

Consent Management Platform Flags. There are 43 apps in our app dataset that implement OneTrust [71], a popular CMP. For each app we analyzed under which condition it sets OneTrust’s IsGpcEnabled flag to True. Apps’ HTTP responses for setting the flag fall into different categories. However, since app operators do not use consistent category names, the categorization of the IsGpcEnabled flag is not directly possible. Therefore, we identified and manually coded the observed category names into five overarching opt-out categories, similar to cookie categories: Functional, Performance, Social Media, Strictly Necessary, and Targeted Advertising. After our categorization, consistent with our previous results, we observed no substantial differences in the IsGpcEnabled flag values within each category across the four conditions (Figure 8).²⁶ Notably, the IsGpcEnabled flag values for Targeted Advertising did not change substantially across conditions.

6.2.2 Connecting to Ad Tracking Domains. Evaluating the counts of apps in our app dataset that make ad tracking domain connections, we do not find substantial differences across conditions. However, there are minor differences. Notably, the count of apps that connect to the app-measurement.com domain in the AdID condition is higher (1,047 apps) than in the No AdID + GPC condition (808 apps). The reason for this difference could be a compounding effect where disabling the AdID and sending GPC signals each leads to a slight

²⁶Most apps received a single response from OneTrust except com.greencopper.countryjam. This app received two identical responses, which we counted as one response. One app, com.disney.wdw.android, did not receive a OneTrust response for the AdID + GPC condition, indicated by the shorter red bars in Figure 8. A few apps’ categories did not fit any of our categories. We omitted those from our analysis.

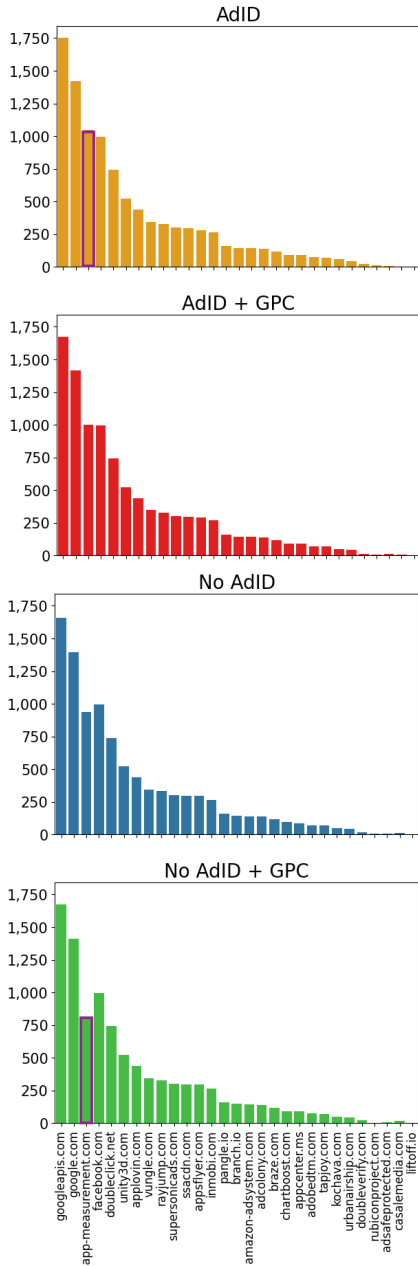


Figure 9: Counts of apps in our app dataset connecting to the 29 most prevalent ad tracking domains that are subject to the CCPA opt-out right (Figure 5). There are no substantial differences across conditions.

decrease. Overall, however, the number of apps connecting to ad tracking domains in the different conditions does not indicate that sending GPC signals is an effective means for exercising the CCPA opt-out right. The same is true for disabling the AdID. Figure 9 illustrates our results.

One other point is noteworthy. In our app dataset, all apps that connected to first-party servers also connected to third-party

servers. However, 12% of apps connected exclusively to third-party servers. Those apps will receive GPC headers directly from a user’s device without reliance on redirects from a first-party server. For those apps we did not observe substantially different levels of GPC compliance. Thus, it does not appear that the communication model—receiving GPC signals via redirects from first parties vs direct GPC signals from a user’s device—plays a role for GPC compliance. This is in line with the GPC specification, which does not differentiate between the two [91]. Third parties are obligated to listen for GPC signals regardless from whom they come.

6.2.3 Disclosing Device Identifiers. Overall, the rates of device identifier disclosures under the four conditions are similar. The Android ID, serial number, and MAC address of our test device was not disclosed in any condition. In some requests to googleapis.com, we found our test device’s IMEI, which, however, is not correlated to any particular condition. Further, we found the public IP address of our test device in some third-party request or response bodies, though, again, not correlated to any particular condition. Interestingly, a small number of domains still received the AdID in the No AdID and No AdID + GPC conditions.²⁷ We re-ran our analysis, which confirmed our results, leaving us uncertain about the reason.

Since we quit each app and cleared its cache and data in between conditions, the AdID from a previous condition run could not have been left stored in the app’s storage at the time of the next condition run. Generally, the app could also not have written the AdID to other apps’ external storage on our test device. While our controller granted each app all permissions it requested at install time, the app would generally need direct user consent to read and write to other apps’ files [4]. A plausible explanation is that the AdID was stored at the backend and associated with another identifier that was then synced once the app was run again in the new condition. We inquired with the respective companies but did not hear back.

7 Discussion: Implementing Opt-out Rights on Android and Improving User Privacy

Our results suggest that many Android apps do not provide California residents with an effective way to exercise their CCPA opt-out right. We see this shortcoming as a platform-level challenge. To broadly improve the privacy of Android users the Android platform would benefit from an opt-out setting to exercise opt-out rights under applicable law in place of its current AdID setting.

7.1 Android’s Opt-out Right Gap

As we have seen (Section 6.2), the long-established Android AdID setting has no substantial effect on apps’ opt-out behavior. Apps’ sharing and selling of personal information also generally continues despite sending GPC signals. At the app-level, our results suggest that many apps do not have a dedicated CCPA opt-out setting, and some that do are not propagating California residents’ opt-out preferences to third parties (Section 5.2). Given that 63%–82% of apps in our app dataset are required to respect the CCPA opt-out right (Section 6.1), our results suggest that many apps violate the CCPA as they do not enable California residents to exercise

²⁷Three of the domains are Google domains — app-measurement.com, googleapis.com, and google-analytics.com — and three are non-Google domains — omtrdc.net, gadsme.com, and wizz.chat.

their right. Our results suggest that many apps do not provide functionality for California residents to exercise their opt-out right.

There could be various reasons for why that is the case. First, traditionally the core business model of the ad online ecosystem has been directly opposed to respecting opt-out preferences [93]. Until the recent enforcement actions by the Office of the California Attorney General and other attorneys general offices [81–83] the risk of being caught for not doing so was low. Some app operators may simply accept the risk. After all, dark patterns are ostensibly proliferating because companies’ A-B testing has revealed them to be profit maximizing [59]. The same could be true for not providing opt-out functionality.

In our view, technical and ecosystem complexities also play a major role for the lack of opt-out right compliance. Opting out is a complex coordination problem with distributed responsibilities among first parties, ad networks, CMPs, and other parties, all of whose activities and motivations are not aligned [43]. These different responsibilities become difficult to manage without addressing them at the platform-level. Thus, in our view, our results indicate that app-level opt-out preferences are just not feasible. We need a platform-level opt-out right architecture.

7.2 Two Settings for One Task

As it stands, Android has two types of opt-out settings: the platform-level AdID and app-level CCPA UI opt-out settings. The AdID setting is not intended for exercising the opt-out right per the CCPA or other privacy laws. However, according to Google, if a user has disabled the AdID, operators “may not use the advertising identifier for creating user profiles for advertising purposes or for targeting users with personalized advertising” [30]. Similarly, the CCPA prohibits the sharing of personal information for purposes of cross-context behavioral advertising, which is defined as the “targeting of advertising to a consumer based on the consumer’s personal information” and which covers “consumer profiles” per the CCPA Regulations.²⁸ Thus, the intended effect of the AdID setting is similar to what the CCPA opt-out right is intended for. However, despite this similarity the AdID setting is without legal meaning outside the contractual relationship that Google has with the app operators.

This separation of the AdID setting from the opt-out right is based on its historical development predating the introduction of the CCPA (Section 2.2). In our view, it would benefit the Android platform if both were united and the opt-out right would be available on Android as a native setting. There should be only one opt-out setting on Android. The current separation is confusing from a user perspective. Users have to both disable the AdID and perform app-level opt-outs to accomplish one task. If there were only one setting, it would give users a consistent experience and also relieve app operators from compliance burdens they may not be sufficiently equipped to tackle. Thus, we propose to re-purpose the existing Android AdID setting as an opt-out right setting with legal meaning under the CCPA and other privacy laws.

7.3 Re-purposing the AdID Setting

Disabling the AdID should be interpreted as exercising the opt-out right. This would immediately make the opt-out right on Android

available to a wide audience in line with previous results suggesting that many users have interest in such setting [92]. Such re-purposing would unify and streamline the current two types of settings—the platform-level AdID setting and the app-level opt-out right settings—into one and lead to greater legal clarity. The current AdID API can be modified to return an opt-out signal (akin to GPC’s Sec-GPC: 1 header) instead of a string of zeros when a user opts out [26]. Notably, opting out via GPC and the AdID setting are both intended as universal settings and have nearly identical scope (Appendix 11.2). However, ultimately, whether this uniform setting is a GPC setting or other opt-out right setting is secondary.

Evolving the AdID setting and APIs towards the opt-out right requires a combination of technological and policy changes on the Android platform. However, creating a platform-level API that apps and their integrated libraries can query for the user’s opt-out status is a standard feature for an operating system or other platform-level software layer. To make users aware of their opt-out right, Android should surface a prompt for universally opting out as part of the setup of a new or reset Android device. Android could also surface such prompt upon the first start of an app that is selling or sharing personal information. Crucially, such prompt should contain an option for applying a user’s preference universally across all apps, e.g., via generalizable active privacy choice [90], since a number of laws require universal opt-out options.

To make it applicable to various laws the setting should be described to users in a wording that is not specific to one particular law but broadly covers all potentially applicable laws, for example, “you can enable the toggle to exercise your opt-out right to the extent of the law applicable in your region.” The description could also be custom-tailored to specific laws if it is known which laws are applicable from a user’s account settings, via the user’s location, or otherwise. Before any selling or sharing of personal information could occur, third-party ad networks need to query a user’s opt-out status via a call to the new opt-out right API, as re-purposed from the current AdID API. If not yet known at the time of the call, a user should be prompted to select a preference, again, with a universal option. If users opt out, they should be opted out to the maximum extent per the applicable law.

Exercising the opt-out right may have impact on other platform-level privacy settings, which would need to be aligned. Notably, while recently pared-back substantially [32], Google’s Privacy Sandbox, a privacy framework for the web and Android, includes various settings that could be impacted. In general, if users exercise their opt-out right, any setting that would run contrary to what the right requires would need to be turned off, e.g., under the CCPA, settings that would enable the selling or sharing of personal information. The opt-out right setting should also be available to users on devices without Google Play Services, i.e., on alternative Android distributions. As the simplest solution, those could re-implement the Google APIs as, e.g., GrapheneOS [39] and /e/OS [21], already do. Overall, the emerging legal landscape requiring online ads to be served in a privacy-preserving manner presents an opportunity for Google to re-purpose the AdID setting towards the opt-out right and align it with the mandatory legal requirements in California and other jurisdictions.

²⁸CCPA §1798.140(k), CCPA Regulations §7025(c)(1).

7.4 Legislative and Regulatory Support

In our view, the platform-level implementation of an opt-out setting would benefit from additional legislative and regulatory support. The online ad industry has shown to be resistant to change in the past. A frictionless and universal opt-out setting presented prominently to users would likely see a high adoption rate as was the case for Apple’s App Tracking Transparency framework [55]. Such setting would reduce the amount of data available for ad personalization and potentially impact ad networks’ revenue given their current business model.

On the legislative side a promising proposal had been adopted in California with Assembly Bill 3048 [10]. This Bill required Google and other companies to implement in mobile operating systems a setting that enables consumers to send opt-out preference signals. However, following lobbying by the online ad industry, the California Governor chose to veto the Bill stating that “to ensure the ongoing usability of mobile devices, it’s best if design questions are first addressed by developers, rather than by regulators” [69]. Platform operators have, however, not taken on the task, and we are not aware of major efforts currently under way.

After Assembly Bill 3048 failed, a new Assembly Bill 566, the California Opt Me Out Act, was introduced [11]. This time the Bill was signed by the California Governor and will become law in January 2027 amending the CCPA. It requires businesses to “not develop or maintain a browser that does not include functionality configurable by a consumer that enables the browser to send an opt-out preference signal.” However, the language of the former Assembly Bill 3048 on mobile app operating systems is absent.²⁹ Thus, the California Opt Me Out Act will generally not improve the situation for users of mobile platforms.

However, even without further legislative action, regulatory agencies have an opportunity to step in. Notably, the California Privacy Protection Agency (CPPA) has published the CCPA Regulations stating that consumers must be able to opt out of the sale and sharing of their personal information without having to make individualized requests with each business.³⁰ Consumers have a right to opt out on every “device,” i.e., “any physical object that is capable of connecting to the internet, directly or indirectly, or to another device.”³¹ To achieve this goal the CPPA can “[p]rovide guidance to businesses regarding their duties and responsibilities.”³² Thus, the CCPA Regulations provide the CPPA with a tool to guide platform operators toward the implementation of an opt-out right setting. We firmly believe that this regulatory support would help to establish the CCPA opt-out right on Android and other platforms.

8 Conclusions

We studied the effectiveness of opting out per the CCPA from ad tracking via GPC and app-level opt-out UIs. We find that the CCPA opt-out right applies to 62%–81% of the top-free Android apps on the US Google Play store and that many apps are not compliant. For example, when sending GPC signals and disabling apps’ access

to the AdID, 338 apps still had the `ccpa` status of the ad network Vungle set to `opted_in` while only 26 had set it to `opted_out`. The fundamental challenge is that the opt-out right is not supported by a platform-level setting. Moving forward, as the current AdID setting is not aligned with users’ opt-out right, it should be re-purposed towards an opt-out right setting. As we focused on Android, the opt-out compliance on iOS and other platforms remains an open question. It may be that the App Tracking Transparency framework [5] does not help users with their opt-out right either resulting in similar levels of non-compliance as we found here for Android. In general, it would be a worthwhile endeavor to evaluate the extent to which opt-out rights are respected on different platforms and under different laws as well as to measure the impact of legislative and regulatory activities.

9 Ethical Considerations

We designed and conducted our study to minimize risk and adhere to ethical research principles. All data collection was limited to the personal information of the researchers. As the study did not involve external human subjects, it did not require Institutional Review Board approval. The impact on the evaluated apps’ infrastructure was minimal as it was limited to approximately 30 seconds for the initialization and each test condition per app. In line with responsible disclosure principles, we have notified all companies whose services we observed accessing the Android AdID after we had disabled it. We also contacted the app operators we identified in our UI opt-out evaluation who stated that the CCPA opt-out right is available to California residents in their privacy policy but failed to provide a corresponding setting in their app.

10 Availability of Artifacts

Setup instructions and scripts for performing the described dynamic analysis are publicly available at <https://github.com/privacy-tech-lab/gpc-android>.

Acknowledgments

We thank our anonymous reviewers and our shepherd for their improvement suggestions. Don Marti and Aram Zucker-Scharff provided valuable feedback and industry expertise on our draft. We also thank former Wesleyan University students Wesley Tan, Samir Cerrato, Eliza Kuller, and Bella Tassone for support of the research in its earlier stages. We are grateful to the National Science Foundation for their support of this research (Award #2055196). We also thank Wesleyan University, its Department of Mathematics and Computer Science, and the Anil Fernando Endowment for their additional support. Conclusions reached or positions taken are our own and not necessarily those of our supporters, its trustees, officers, or staff.

References

- [1] Yuvraj Agarwal and Malcolm Hall. 2013. ProtectMyPrivacy: Detecting and Mitigating Privacy Leaks on iOS Devices Using Crowdsourcing. In *Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services - MobiSys '13*. ACM Press, Taipei, Taiwan, 97. <https://doi.org/10.1145/2462456.2464460>
- [2] Android Developers Blog. 2018. DNS over TLS support in Android P Developer Preview. <https://android-developers.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html>. Accessed: December 26, 2025.

²⁹ A former version of Assembly Bill 566 also covered “browser engines,” which was intended to include WebViews and similar web technologies on mobile devices. However, this wording was removed from the final version [7].

³⁰ CCPA Regulations §7025(a).

³¹ CCPA §1798.140(o).

³² CCPA §1798.199.40(f).

- [3] Android Open Source Project. 2025. Data Saver mode. <https://source.android.com/docs/core/data/data-saver>. Accessed: December 26, 2025.
- [4] Android Open Source Project. 2025. Scoped storage. <https://source.android.com/docs/core/storage/scoped>. Accessed: December 26, 2025.
- [5] Apple Developer. 2025. App Tracking Transparency. <https://developer.apple.com/documentation/apptrackingtransparency>. Accessed: December 26, 2025.
- [6] Xavier Becerra. 2021. <https://twitter.com/AGBecerra/status/1354850758236102656>. accessed: December 26, 2025.
- [7] Adam Bender. 2025. Browser Engines Carved Out From California Opt-Out Preference Bill. <https://privacy-daily.com/article/2025/07/02/browser-engines-carved-out-from-california-optout-preference-bill-2507020016>. Accessed: December 26, 2025.
- [8] Reuben Binns, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. 2018. Measuring Third-party Tracker Power across Web and Mobile. *ACM Trans. Internet Technol.* 18, 4, Article 52 (aug 2018), 22, pages. <https://doi.org/10.1145/3176246>
- [9] California Legislative Information. 2003. California Online Privacy Protection Act. https://leginfo.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC. Accessed: December 26, 2025.
- [10] California Legislative Information. 2024. AB-3048 California Consumer Privacy Act of 2018: opt-out preference signal. https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB3048. Accessed: December 26, 2025.
- [11] California Legislative Information. 2025. California Assembly Bill 566. <https://legiscan.com/CA/bill/AB566/2025>. Accessed: December 26, 2025.
- [12] California Privacy Protection Agency. 2024. California Consumer Privacy Act Regulations. https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf. Accessed: December 26, 2025.
- [13] Yi Chen, Mingming Zha, Nan Zhang, Dandan Xu, Qianqian Zhao, Xuan Feng, Kan Yuan, Fnu Suya, Yuan Tian, Kai Chen, XiaoFeng Wang, and Wei Zou. 2019. Demystifying Hidden Privacy Settings in Mobile Apps. In *2019 IEEE Symposium on Security and Privacy, SP 2019, San Francisco, CA, USA, May 19-23, 2019*. IEEE, San Francisco, 570–586. <https://doi.org/10.1109/SP.2019.00054>
- [14] Colorado Department of Law. 2024. Universal Opt-Out and the Colorado Privacy Act. <https://coag.gov/uoom/>. Accessed: December 26, 2025.
- [15] Consumer Reports. 2025. Permission Slip. <https://permissionslipcr.com/>. Accessed: December 26, 2025.
- [16] Lorrie Faith Cranor, Brooks Dobbs, Serge Egelman, Giles Hogben, Jack Humphrey, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, Joseph M. Reagle, Matthias Schunter, David A. Stampley, and Rigo Wenning. 2006. The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. <https://www.w3.org/TR/P3P11/>.
- [17] Lorrie Faith Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, and Joseph M. Reagle. 2002. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. <https://www.w3.org/TR/P3P/>.
- [18] Jelmer de Hen. 2025. MagiskBypassCertificateTransparencyError. <https://github.com/JelmerDeHen/MagiskBypassCertificateTransparencyError>. Accessed: December 26, 2025.
- [19] Anokhy Desai and Cobun Zweifel-Keegan. 2023. How should mobile apps prepare for California’s privacy scrutiny? <https://iapp.org/news/a/how-should-mobile-apps-prepare-for-californias-privacy-scrutiny>. Accessed: December 26, 2025.
- [20] Digital Advertising Alliance. 2025. Download the AppChoices Tool. <https://youradchoices.com/appchoices>. Accessed: December 26, 2025.
- [21] e Foundation. 2024. /e/OS is a complete, fully “deGoogled,” mobile ecosystem. <https://e.foundation/e-os/>. Accessed: December 26, 2025.
- [22] William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. Sheth. 2010. TaintDroid: An Information-flow Tracking System for Realtime Privacy Monitoring on Smartphones. In *Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation (OSDI’10)*. USENIX Association, Vancouver, BC, 393–407.
- [23] Roy T. Fielding and David Singer. 2019. Tracking Preference Expression (DNT). <https://www.w3.org/TR/tracking-dnt/>. Accessed: December 26, 2025.
- [24] Frida. 2025. Frida. <https://frida.re/>. Accessed: December 26, 2025.
- [25] Google. 2024. Play services AdvertisingIdClient.Info. <https://developers.google.com/android/reference/com/google/android/gms/ads/identifier/AdvertisingIdClient.Info>. Accessed: December 26, 2025.
- [26] Google. 2025. Advertising ID. <https://support.google.com/googleplay/android-developer/answer/6048248>. Accessed: December 26, 2025.
- [27] Google. 2025. Helping advertisers comply with the U.S. states’ privacy laws in Google Ads. <https://support.google.com/google-ads/answer/9614122>. Accessed: December 26, 2025.
- [28] Google. 2025. Play Console Help — App Discovery and Ranking. <https://support.google.com/googleplay/android-developer/answer/9958766?hl=en>. Accessed: December 26, 2025.
- [29] Google. 2025. Play Console Help — Choose a category and tags for your app or game. <https://support.google.com/googleplay/android-developer/answer/9859673?hl=en&zippy=%2Cgames%2Capps>. Accessed: December 26, 2025.
- [30] Google. 2025. Play Console Help Ads. <https://support.google.com/googleplay/android-developer/answer/9857753>. Accessed: December 26, 2025.
- [31] Google. 2025. Play Console Help User Data. <https://support.google.com/googleplay/android-developer/answer/10144311>. Accessed: December 26, 2025.
- [32] Google. 2025. Update on Plans for Privacy Sandbox Technologies. <https://privacysandbox.google.com/blog/update-on-plans-for-privacy-sandbox-technologies>. accessed: December 26, 2025.
- [33] Google for Developers. 2025. Android Debug Bridge (adb). <https://developer.android.com/tools/adb>. Accessed: December 26, 2025.
- [34] Google Maps Help. 2025. Control access point inclusion in Google’s Location services. <https://support.google.com/maps/answer/1725632#zippy=%2Chow-do-i-opt-my-access-point-out-of-google-location-services>. Accessed: December 26, 2025.
- [35] Google Play. 2025. Leafly: Find Cannabis and CBD. <https://play.google.com/store/apps/details?id=leafly.android>. Accessed: December 26, 2025.
- [36] Google Play. 2025. Pure Sniper: Gun Shooter Games. <https://play.google.com/store/apps/details?id=com.miniclip.realsniper>. Accessed: December 26, 2025.
- [37] Google Play. 2025. TuneIn Radio: Music & Sports. <https://play.google.com/store/apps/details?id=tunein.player>. Accessed: December 26, 2025.
- [38] Google Play. 2025. Vivid Seats | Event Tickets. <https://play.google.com/store/apps/details?id=com.vividseats.android>. Accessed: December 26, 2025.
- [39] GrapheneOS. 2025. GrapheneOS The Private and Secure Mobile OS. <https://grapheneos.org/>. Accessed: December 26, 2025.
- [40] Daniel Greene and Katie Shilton. 2018. Platform Privacies: Governance, Collaboration, and the Different Meanings of “Privacy” in iOS and Android Development. *New Media & Society* 20, 4 (2018), 1640–1657. <https://doi.org/10.1177/1461444817702397>
- [41] Catherine Han, Irwin Reyes, Álvaro Feal, Joel Reardon, Primal Wijesekera, Amit Elazari, Kenneth A Bamberger, and Serge Egelman. 2020. The Price Is (Not) Right: Comparing Privacy in Free and Paid Apps. In *PETS. De Gruyter Open / Sciendo, Online*, 21.
- [42] Katherine Hausladen, Oliver Wang, Sophie Eng, Jocelyn Wang, Francisca Wijaya, Matthew May, and Sebastian Zimmeck. 2025. Websites’ Global Privacy Control Compliance at Scale and over Time. <https://www.usenix.org/conference/usenixsecurity25/presentation/hausladen>. In *34th USENIX Security Symposium (USENIX Security 2025)*. USENIX Association, Seattle, WA, 5837–5856.
- [43] Maximilian Hils, Daniel W. Woods, and Rainer Böhme. 2021. Privacy Preference Signals: Past, Present and Future. *Proceedings on Privacy Enhancing Technologies* 2021, 4 (07 2021), 249–269. <https://doi.org/10.2478/popets-2021-0069>
- [44] Soheil Human, Harshvardhan J. Pandit, Victor Morel, Cristiana Santos, Martin Degeling, Arianna Rossi, Wilhelmina Botes, Vitor Jesus, and Irene Kamara. 2022. Data Protection and Consenting Communication Mechanisms: Current Open Proposals and Challenges. In *Proceedings - 7th IEEE European Symposium on Security and Privacy Workshops (2022 IEEE European Symposium on Security and Privacy Workshops)*. IEEE, United States, 231–239. <https://doi.org/10.1109/eurospw55150.2022.00029>
- [45] Soheil Human, Max Schrems, Alan Toner, Gerben, and Ben Wagner. 2021. Advanced Data Protection Control (ADPC). <https://www.dataprotectioncontrol.org/>. Accessed: December 26, 2025.
- [46] IAB Tech Lab. 2022. Global Privacy Platform. https://iabtechlab.com/wp-content/uploads/2022/06/global_privacy_platform_rfc_june_2022.pdf. Accessed: December 26, 2025.
- [47] IAB Tech Lab. 2024. GPP Extension: IAB Privacy’s California Privacy Technical Specification. <https://github.com/InteractiveAdvertisingBureau/Global-Privacy-Platform/tree/main/Sections/US-States/CA>. Accessed: December 26, 2025.
- [48] IAB Tech Lab. 2024. US Privacy User Signal Mechanism “USP API”. <https://github.com/InteractiveAdvertisingBureau/USPrivacy/blob/master/CCPA/USP%20API.md>. Accessed: December 26, 2025.
- [49] IAB Tech Lab. 2025. USPrivacy. <https://github.com/InteractiveAdvertisingBureau/USPrivacy>. Accessed: December 26, 2025.
- [50] InMobi. 2024. Privacy Policy. <https://advertising.inmobi.com/privacy-policy>. Accessed: December 26, 2025.
- [51] Konrad Kollnig. 2023. xray-blacklist.json. <https://github.com/TrackerControl/tracker-control-android/blob/master/app/src/main/assets/xray-blacklist.json>. Accessed: December 26, 2025.
- [52] Konrad Kollnig, Pierre Dewitte, Max Van Kleek, Ge Wang, Daniel Omeiza, Helena Webb, and Nigel Shadbolt. 2021. A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Berkeley, CA, 181–196. <https://www.usenix.org/conference/soups2021/presentation/kollnig>
- [53] Konrad Kollnig and Nigel Shadbolt. 2022. TrackerControl: Transparency and Choice around App Tracking. *Journal of Open Source Software* 7, 75 (2022), 4270. <https://doi.org/10.21105/joss.04270>
- [54] Konrad Kollnig, Anastasia Shuba, Reuben Binns, Max Van Kleek, and Nigel Shadbolt. 2022. Are iPhones Really Better for Privacy? A Comparative Study of iOS and Android Apps. In *Proceedings on Privacy Enhancing Technologies*, Vol. 2022. Privacy Enhancing Technologies Symposium Advisory Board, Sydney, Australia, 6–24. Issue 2. <https://doi.org/10.2478/popets-2022-0033>

- [55] Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns, and Nigel Shadbolt. 2022. Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels. In *2022 ACM Conference on Fairness, Accountability, and Transparency* (Seoul, Republic of Korea) (FAccT '22). Association for Computing Machinery, New York, NY, USA, 508–520. <https://doi.org/10.1145/3531146.3533116>
- [56] Renuka Kumar, Apurva Virkud, Ram Sundara Raman, Atul Prakash, and Roya Ensafi. 2022. A Large-scale Investigation into Geodifferences in Mobile Apps. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 1203–1220. <https://www.usenix.org/conference/usenixsecurity22/presentation/kumar>
- [57] Landgericht Berlin. 2023. Landgericht Berlin, Az.: 16 O 420/19, Teil- und Schlussurteil, Verbraucherzentrale Bundesverband e.V. gegen LinkedIn Ireland Unlimited Company. https://www.vzbv.de/sites/default/files/2023-10/Teil-%20und%20Schlussurteil_LG%20Berlin_24.08.2023.pdf. Accessed: December 26, 2025.
- [58] Anh Le, Janus Varmarken, Simon Langhoff, Anastasia Shuba, Minas Gjoka, and Athina Markopoulou. 2015. AntMonitor: A System for Monitoring from Mobile Devices. In *Proceedings of the 2015 ACM SIGCOMM Workshop on Crowdsourcing and Crowdsourcing of Big (Internet) Data - C2B(1)D '15*. ACM Press, London, United Kingdom, 15–20. <https://doi.org/10.1145/2787394.2787396>
- [59] Jamie Luguri and Lior Jacob Strahilevitz. 2021. Shining a Light on Dark Patterns. *Journal of Legal Analysis* 13, 1 (03 2021), 43–109. <https://doi.org/10.1093/jla/laaa006>
- [60] Meta. 2025. State-Specific Terms. <https://www.facebook.com/legal/terms/state-specific>. Accessed: December 26, 2025.
- [61] Mitmproxy Project. 2025. Mitmproxy. <https://mitmproxy.org/>. Accessed: December 26, 2025.
- [62] Mullvad. 2025. Mullvad. <https://mullvad.net/en>. Accessed: December 26, 2025.
- [63] New Jersey Division of Consumer Affairs. 2025. New Jersey Data Privacy Law FAQs. <https://www.njconsumeraffairs.gov/ocp/Pages/NJ-Data-Privacy-Law-FAQ.aspx>. Accessed: December 26, 2025.
- [64] Trung Tin Nguyen, Michael Backes, Ninja Marnau, and Ben Stock. 2021. Share First, Ask Later (or Never?) Studying Violations of GDPR’s Explicit Consent in Android Apps. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Berkeley, CA, 3667–3684. <https://www.usenix.org/conference/usenixsecurity21/presentation/nguyen>
- [65] Trung Tin Nguyen, Michael Backes, and Ben Stock. 2022. Freely Given Consent? Studying Consent Notice of Third-Party Tracking and Its Violations of GDPR in Android Apps. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*. Association for Computing Machinery, New York, NY, USA, 2369–2383. <https://doi.org/10.1145/3548606.3560564>
- [66] NVISOsecurity. 2025. Magisk Trust User Certs. <https://github.com/NVISOsecurity/MagiskTrustUserCerts>. Accessed: December 26, 2025.
- [67] Sean O’Connor, Ryan Nurwono, Aden Siebel, and Eleanor Birrell. 2021. (Un)clear and (In)conspicuous: The Right to Opt-out of Sale under CCPA. In *Proceedings of the 20th Workshop on Privacy in the Electronic Society (Virtual Event, Republic of Korea) (WPES '21)*. Association for Computing Machinery, New York, NY, USA, 59–72. <https://doi.org/10.1145/3463676.3485598>
- [68] Office of the Attorney General. 2025. The Connecticut Data Privacy Act. <https://portal.ct.gov/ag/sections/privacy/the-connecticut-data-privacy-act>. Accessed: December 26, 2025.
- [69] Office of the Governor. 2024. AB 3048 Veto Message. <https://www.gov.ca.gov/wp-content/uploads/2024/09/AB-3048-Veto-Message.pdf>. Accessed: December 26, 2025.
- [70] OneTrust. 2024. Protect mobile app consumer privacy and enable data control. <https://www.onetrust.com/products/mobile-app-consent/>. Accessed: December 26, 2025.
- [71] OneTrust. 2025. <https://www.onetrust.com/>. Accessed: December 26, 2025.
- [72] Onyxbits. 2025. Raccoon — APK downloader. <https://www.onyxbits.de/raccoon>. Accessed: December 26, 2025.
- [73] Amogh Pradeep, Muhammad Talha Paracha, Protick Bhowmick, Ali Davanian, Abbas Razaghpanah, Taejoong Chung, Martina Lindorfer, Narseo Vallina-Rodriguez, Dave Levin, and David Choffnes. 2022. A comparative analysis of certificate pinning in Android & iOS. In *Proceedings of the 22nd ACM Internet Measurement Conference (Nice, France) (IMC '22)*. Association for Computing Machinery, New York, NY, USA, 605–618. <https://doi.org/10.1145/3517745.3561439>
- [74] Privacy4Cars. 2025. OptOutCode. <https://optoutcode.com/>. Accessed: December 26, 2025.
- [75] Joel Reardon, Álvaro Feal, Primal Wijesekera, Amit Elazari Bar On, Narseo Vallina-Rodriguez, and Serge Egelman. 2019. 50 Ways to Leak Your Data: An Exploration of Apps’ Circumvention of the Android Permissions System. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 603–620.
- [76] Jingjing Ren, Ashwin Rao, Martina Lindorfer, Arnaud Legout, and David Choffnes. 2016. ReCon: Revealing and Controlling PII Leaks in Mobile Network Traffic. In *MobiSys '16* (Singapore, Singapore). ACM, New York, NY, USA, 361–374. <https://doi.org/10.1145/2906388.2906392>
- [77] Nikita Samarin, Shayna Kothari, Zaina Siyed, Oscar Bjorkman, Reena Yuan, Primal Wijesekera, Noura Alomar, Jordan Fischer, Chris Hoofnagle, and Serge Egelman. 2023. Lessons in VCR Repair: Compliance of Android App Developers with the California Consumer Privacy Act (CCPA). In *23rd Privacy Enhancing Technologies Symposium (PETS 2023)*, Vol. 2023. PETS, Lausanne, Switzerland, 103–121. Issue 3. <https://doi.org/10.56553/popets-2023-0072>
- [78] Gian Luca Scoccia, Ibrahim Kanj, Ivano Malavolta, and Kaveh Razavi. 2020. Leave My Apps Alone! A Study on How Android Developers Access Installed Apps on User’s Device. In *PETS. De Gruyter Open / Sciendo*, Online, 11.
- [79] Anastasia Shuba and Athina Markopoulou. 2020. NoMoATS: Towards Automatic Detection of Mobile Tracking. *Proceedings on Privacy Enhancing Technologies* 2020, 2 (April 2020), 45–66. <https://doi.org/10.2478/popets-2020-0017>
- [80] Yihang Song and Urs Hengartner. 2015. PrivacyGuard: A VPN-based Platform to Detect Information Leakage on Android Devices. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM '15*. ACM Press, Denver, Colorado, USA, 15–26. <https://doi.org/10.1145/2808117.2808120>
- [81] State of California Department of Justice. 2022. Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act. <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement>. Accessed: December 26, 2025.
- [82] State of California Department of Justice. 2022. CCPA Enforcement Case Examples (Online Retailers Implemented Opt Out Procedures, Including GPC, Wireless Network Provider Updated Request for Information Procedures, Manufacturer and Retailer Stopped Selling Personal Information). <https://oag.ca.gov/privacy/ccpa/enforcement>. Accessed: December 26, 2025.
- [83] State of California Department of Justice. 2025. Attorney General Bonta Announces Largest CCPA Settlement to Date, Secures \$1.55 Million from Healthline.com. <https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-largest-ccpa-settlement-date-secures-155>. Accessed: December 26, 2025.
- [84] Trevor Testwuide. 2022. What is IDFA (Identifier for Advertisers) and is IDFA going away? <https://www.measured.com/faq/what-is-idfa-identifier-for-advertisers-and-is-idfa-going-away/>. Accessed: December 26, 2025.
- [85] TrueVault. 2025. Is “Sharing” the Same as Selling under the CCPA? <https://www.truevault.com/learn/ccpa/is-sharing-the-same-as-selling-under-the-ccpa>. Accessed: December 26, 2025.
- [86] Imdad Ullah, Roksana Boreli, and Salil S. Kanhere. 2023. Privacy in targeted advertising on mobile devices: a survey. <https://doi.org/10.1007/s10207-022-00655-x>. *International Journal of Information Security* 22 (2023), 647–678.
- [87] Vungle. 2025. Advanced Settings. <https://support.vungle.com/hc/en-us/articles/360047780372-Advanced-Settings>. Accessed: December 26, 2025.
- [88] Yue Xiao, Zhengyi Li, Yue Qin, Xiaolong Bai, Jiale Guan, Xiaojing Liao, and Luyi Xing. 2023. Lalaine: Measuring and Characterizing Non-Compliance of Apple Privacy Labels at Scale. In *Proceedings of USENIX Security Symposium*. USENIX Association, Anaheim, CA, 1091–1108. <https://doi.org/10.48550/arXiv.2206.06274>
- [89] Sebastian Zimmeck, Daniel Goldelman, Owen Kaplan, Logan Brown, Justin Casler, Judeley Jean-Charles, Joe Champeau, and Hamza Harkous. 2024. Website Data Transparency in the Browser. In *24th Privacy Enhancing Technologies Symposium (PETS 2024)*. PETS, Bristol, UK, 211–234. Issue 2. <https://doi.org/10.56553/popets-2024-0048>
- [90] Sebastian Zimmeck, Eliza Kuller, Chunyue Ma, Bella Tassone, and Joe Champeau. 2024. Generalizable Active Privacy Choice: Designing a Graphical User Interface for Global Privacy Control. In *24th Privacy Enhancing Technologies Symposium (PETS 2024)*. PETS, Bristol, UK, 258–279. Issue 1. <https://doi.org/10.56553/popets-2024-0015>
- [91] Sebastian Zimmeck, Peter Snyder, Justin Brookman, and Aram Zucker-Scharff. 2025. Global Privacy Control (GPC). <https://w3c.github.io/gpc/>. Accessed: December 26, 2025.
- [92] Sebastian Zimmeck, Oliver Wang, Kuba Alicki, Jocelyn Wang, and Sophie Eng. 2023. Usability and Enforceability of Global Privacy Control. In *23rd Privacy Enhancing Technologies Symposium (PETS 2023)*. PETS, Lausanne, Switzerland, 265–281. Issue 2. <https://doi.org/10.56553/popets-2023-0052>
- [93] Shoshana Zuboff. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books, London, UK.

11 Appendix

11.1 Dynamic Analysis Details

We performed our analysis with Mitmproxy [61]. To decrypt encrypted network traffic we installed the Mitmproxy certificate in the test device’s certificate store with the MagiskTrustUserCert module [66], which enabled the automatic use of the certificate during our analysis upon certificate chain creation. To bypass apps’ certificate pinning, if any, we deployed a Frida server (v16.1.4) [24] on the

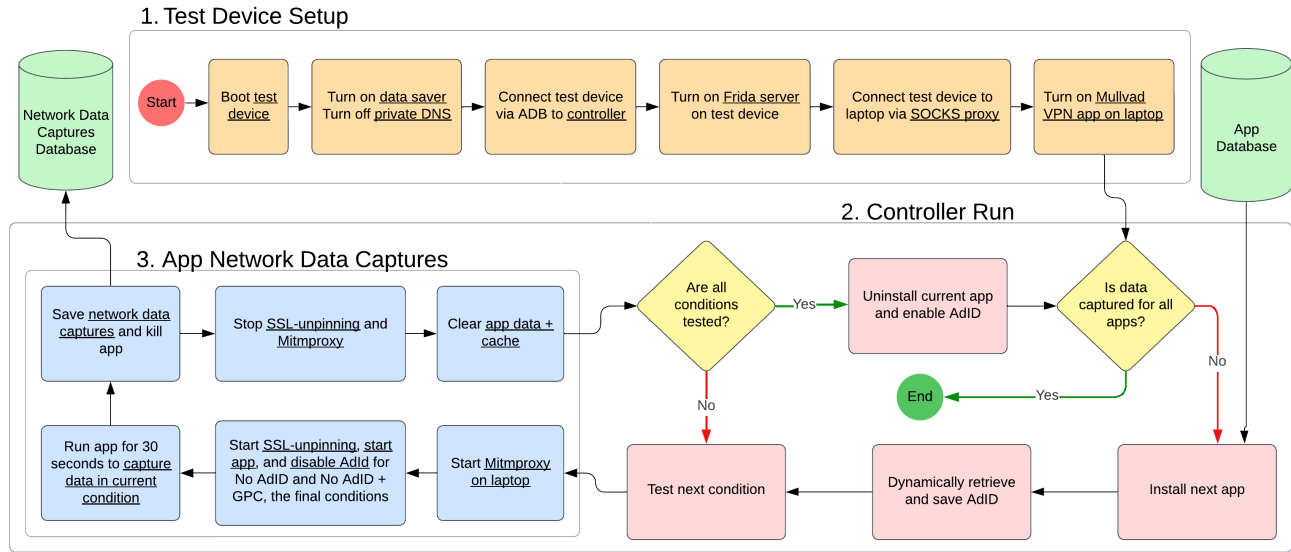


Figure 10: Detailed overview of our dynamic analysis procedure for the apps in our app dataset.

test device running a certificate-unpinning script that we developed based on various open source scripts. Our 4% dynamic analysis failure rate (Section 4.1) falls squarely within the estimated range of 0.9% to 8% of Android apps using certificate pinning [73]. As some apps may automatically open Google Chrome and redirect to a website, for example, for account logins, which could interfere with our capturing of network traffic, we bypassed Chrome Certificate Transparency with the MagiskBypassCertificateTransparencyError module [18].

To minimize background traffic interference via data not originating from the app under scrutiny and increase the reliability of capturing network traffic we turned on “data saver” and turned off “private DNS” on the test device. Turning on “data saver” allowed us to control whether an app has data access depending on whether it runs in the foreground or background [3]. Turning off “private DNS” resulted in more reliably capturing network traffic as apps’ connections to a private DNS provider use encryption and cannot be observed [2].

Since it is not possible to enable or disable the AdID programmatically through ADB, we automated this process for each app analysis in form of dynamically navigating to the AdID setting view and tapping on the respective buttons. For each app, when switching conditions, we cleared the persistent storage and SharedPreferences of the test device.³³ Figure 10 shows a detailed overview of our dynamic analysis procedure.

³³The shell command of our controller to clear an app’s persistent storage and SharedPreferences in a condition is `adb shell su -c pm clear $TARGET_PACKAGE_NAME` with `su -c pm clear` to tell the test device to delete all data associated with a package [33].

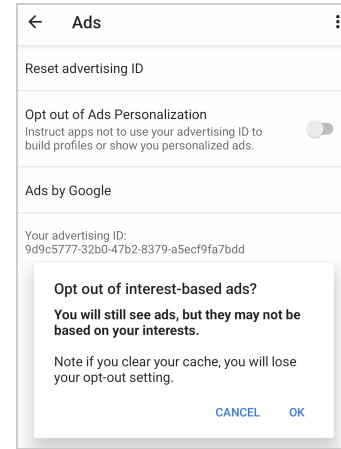


Figure 11: The AdID opt-out setting screen on Android 14.

11.2 Similarities and Differences Between Disabling AdID and GPC Opt-out Setting

Overall, the intended effect of disabling the AdID is very similar to exercising the opt-out right via GPC. Both are designed as universal controls, have nearly identical scope of permitted and prohibited activities, and are generally stateless.

11.2.1 Universal Opt-out Setting. Just as GPC, the AdID setting is intended to be a universal setting for opting out from ad tracking. It enables users to “[i]nstruct apps not to [...] build profiles or show [...] personalized ads” and to “[o]pt out of interest-based ads” (Figure 11). The setting applies device-wide to all installed apps and their third parties and, thus, corresponds to CCPA Regulations, which require

that consumers can opt out from all businesses and controllers they interact with “without having to make individualized requests with each.”³⁴ The AdID is the only identifier that ad networks are allowed to use for personalized advertising for apps distributed via the Google Play store [26]. Using the `getId` method of the `AdvertisingIdClient` class Android apps can retrieve a device’s AdID, and with the `isLimitAdTrackingEnabled` method they can check whether a user has disabled it [25]. Once a user disabled the AdID, `isLimitAdTrackingEnabled` will be true.³⁵ Any attempt to access the AdID when it was disabled will return a string of zeros instead [26].

11.2.2 Scope of Permitted and Prohibited Activities. Both the AdID setting and GPC prohibit the *targeting* and *profiling* of users for ad purposes. Google states that “[i]f a user has enabled [the AdID] setting, [operators] may not use the advertising identifier for creating user profiles for advertising purposes or for targeting users with personalized advertising” [30].³⁶ Similarly, per the CCPA, GPC prohibits the sharing of personal information for purposes of cross-context behavioral advertising, which CCPA §1798.140(k) defines as the “targeting of advertising to a consumer based on the consumer’s personal information” and which covers “consumer profiles” per the CCPA Regulations.³⁷ In this regard, GPC is slightly more permissive than the AdID setting. If users are opted out, first parties can still target ads to users based on their previous activity on the first-party apps or sites [91]. Under both regimes, first parties are prohibited from selling personal information to third parties or share such with them: GPC “convey[s] a person’s request to websites and services to not sell [...] their personal information” [91], and Google prohibits app operators from selling personal user data [31].

11.2.3 Opt-out Status Check on Each Ad Request. Neither the AdID setting nor GPC requires operators to keep state. Just as potential recipients of GPC signals must check for GPC request headers or for the `navigator.globalPrivacyControl` DOM property each time an ad is intended to be served [91], Google requires that “the status of the ‘Opt out of Interest-based Advertising’ or ‘Opt out of Ads Personalization’ setting must be verified on each access of the ID” [30].

11.3 Supplementary Figures and Table

Figure 12 shows the install ranges of apps in our app dataset by category. While the number of installs can be used for evaluating whether an app operator passes the threshold of 100,000 or more consumers or households to qualify as a business per the CCPA, it is just one indicator. If an app operator derives more than 25 million dollars or 50 percent or more of revenues from selling and sharing personal information, it would qualify as a business as well. There are also many operators with more than one app so that the number of installs and their revenue would need to be combined. In our study we rely on privacy policies and other documents to determine whether the CCPA opt-out right applies to an app.

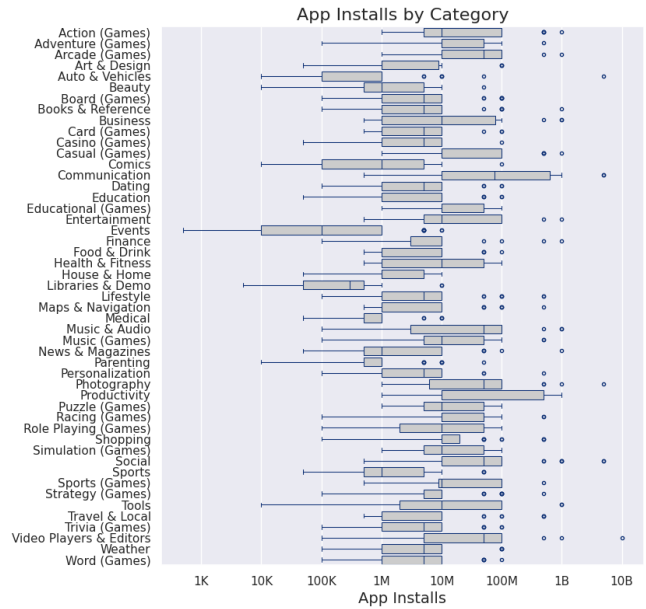


Figure 12: Install ranges of apps in our app dataset ($n = 1,811$) by app category.

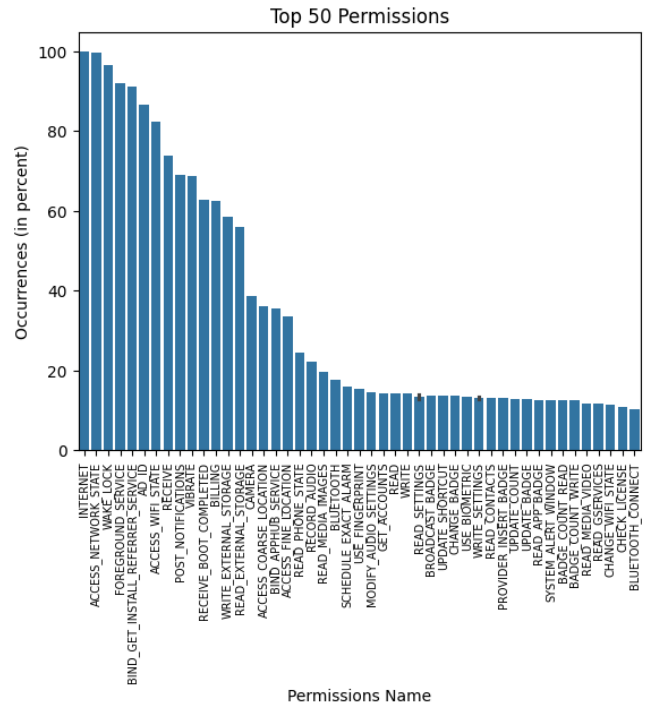


Figure 13: The top 50 permissions declared by apps in our app dataset ($n = 1,811$) in their manifest files.

³⁴CCPA Regulations §7025(a).

³⁵We confirmed this behavior on our test device.

³⁶What Google refers to as “enabl[ing] the [the AdID]” we refer to as “disabling the AdID” throughout the paper.

³⁷CCPA Regulations §7025(c)(1).

	Count	Non-compliance Count	Non-compliance %
Casino (Games)	5	5	100%
Beauty	4	4	100%
Card (Games)	3	3	100%
Books & Reference	2	2	100%
Adventure (Games)	1	1	100%
Board (Games)	1	1	100%
Business	1	1	100%
Comics	1	1	100%
Music (Games)	1	1	100%
Photography	1	1	100%
Productivity	1	1	100%
House & Home	5	4	80%
Role Playing (Games)	4	3	75%
Puzzle (Games)	6	4	67%
Events	3	2	67%
Health & Fitness	3	2	67%
Simulation (Games)	7	4	57%
Word (Games)	6	3	50%
Auto & Vehicles	2	1	50%
Education	2	1	50%
Medical	2	1	50%
Social	2	1	50%
Music & Audio	3	1	33%
Entertainment	3	1	33%
Food & Drink	7	2	29%
News & Magazines	5	1	20%
Shopping	4	0	0%
Sports (Games)	3	0	0%
Action (Games)	2	0	0%
Dating	2	0	0%
Lifestyle	1	0	0%
Maps & Navigation	1	0	0%
Parenting	1	0	0%
Personalization	1	0	0%
Racing (Games)	1	0	0%
Sports	1	0	0%
Tools	1	0	0%
Travel & Local	1	0	0%

Table 3: Counts and percentages of non-compliant apps in our UI opt-out evaluation by app category. We consider an app non-compliant if it either has just a privacy policy link or no opt-out setting or privacy policy link (Table 1).

inner-active.mobi	0	0	147	2	0	5
tapjoy.com	0	0	40	0	0	2
tapjoyads.com	0	0	40	0	0	2
lortchink.com	0	0	1	0	0	0
doubleclick.net	1	0	0	5	2	0
3lift.com	0	0	0	1	0	0
adnxs.com	0	0	0	1	0	0
bidswitch.net	0	0	0	1	0	0
casalemedia.com	0	0	0	1	0	0
critico.com	0	0	0	1	0	0
media.net	0	0	0	1	0	0
mediawallahscript.com	0	0	0	1	0	0
omnitagjs.com	0	0	0	1	0	0
pluto.tv	0	0	0	1	0	0
rubiconproject.com	0	0	0	1	0	0
scorecardresearch.com	1	0	0	1	0	0
sharethrough.com	0	0	0	1	0	0
smaato.net	0	0	0	1	0	0
smartadserver.com	0	0	0	1	0	0
stickyadstv.com	0	0	0	1	0	0
synglosory.com	0	0	0	1	0	0
taboola.com	0	0	0	1	0	0
teads.tv	0	0	0	1	0	0
yahoo.com	0	0	0	1	0	0
adsvr.org	2	0	0	0	0	0
celtra.com	2	0	0	0	0	0
crwdcntrl.net	0	0	0	0	1	0
	1---	1NNY	1YN-	1YNN	1YNY	1YY-
inner-active.mobi	0	0	150	2	0	6
tapjoy.com	0	0	40	0	0	2
tapjoyads.com	0	0	40	0	0	2
lortchink.com	0	0	1	0	0	0
doubleclick.net	1	0	0	5	2	0
3lift.com	0	0	0	1	0	0
adnxs.com	0	0	0	1	0	0
bidswitch.net	0	0	0	1	0	0
casalemedia.com	0	0	0	1	0	0
critico.com	0	0	0	1	0	0
media.net	0	0	0	1	0	0
mediawallahscript.com	0	0	0	1	0	0
omnitagjs.com	0	0	0	1	0	0
rubiconproject.com	0	0	0	1	0	0
sharethrough.com	0	0	0	1	0	0
smaato.net	0	0	0	1	0	0
smartadserver.com	0	0	0	1	0	0
socdm.com	0	0	0	1	0	0
synglosory.com	0	0	0	1	0	0
taboola.com	0	0	0	1	0	0
teads.tv	0	0	0	1	0	0
yahoo.com	0	0	0	1	0	0
adsvr.org	1	0	0	0	0	0
celtra.com	1	0	0	0	0	0
crwdcntrl.net	0	0	0	0	1	0
scorecardresearch.com	2	0	0	0	0	0
	1---	1NNY	1YN-	1YNN	1YNY	1YY-

Figure 14: Counts of US Privacy String values in the AdID (top) and AdID + GPC (bottom) conditions.