The TCF doesn't really A(A)ID – Automatic Privacy Analysis and Legal Compliance of TCF-based Android Applications

The TCF doesn't really A(A)ID – Automatic Privacy Analysis and Legal Compliance of TCF-based Android Apps

Victor Morel
Chalmers University of Technology and University of Gothenburg
Gothenburg, Sweden
morelv@chalmers.se

Cristiana Santos
Utrecht University
Utrecht, The Netherlands
c.teixeirasantos@uu.nl

Pontus Carlsson
Chalmers University of Technology and University of Gothenburg
Gothenburg, Sweden
pontus@carlsson4.se

Joel Ahlinder
Chalmers University of Technology and University of Gothenburg
Gothenburg, Sweden
joelahlinder@hotmail.com

Romaric Duvignau
Chalmers University of Technology and University of Gothenburg
Gothenburg, Sweden
duvignau@chalmers.se

Abstract

The Transparency and Consent Framework (TCF), developed by the Interactive Advertising Bureau (IAB) Europe, provides a *de facto* standard for requesting, recording, and managing user consent from European end-users. Its goal is to help organizations comply with the General Data Protection Regulation (GDPR) and the ePrivacy Directive (ePD). This framework has previously been found to infringe European data protection law and has subsequently been regularly updated. Previous research on the TCF focused exclusively on web contexts, with no attention given to its implementation in mobile apps. No work has systematically studied the compliance implications of the TCF on Android apps. To address this gap, we investigate the prevalence of the TCF in popular Android apps from the Play Store, and assess whether these apps respect users' consent banner choices. The TCF introduced minor changes in its new version (v.2.3) on March 1st, 2026, aimed at reducing ambiguity for vendors; these changes do not impact our results.

We scraped and downloaded 4482 of the most popular Google Play Store apps on an emulated Android device. We automatically identified that 576 (12.85%) of the 4482 downloadable apps implemented the TCF, and we detected potential legal violations within this subset. By automatically interacting with consent banners, we observed that in 15 (2.6%) of these apps, users' choices are stored only when consent is granted. Users who refuse consent are shown the consent banner again each time they launch the app. We analyzed the apps' traffic in two different stages, passive (post interaction with the banner) and active (during banner interaction and post user choices). Network analysis conducted during the passive stage reveals that 66.2% of the analyzed TCF-based apps share personal data through the Google Advertising ID (AAID) without consent – the lawful basis for such processing. Furthermore, 55.3% of apps analyzed during the active stage share AAID before users interact with the apps' consent banners, violating the prior consent requirement. We further expose concerns regarding Google as the dominant Consent Management Provider (CMP) in our dataset (89.76%), structurally accommodating potential legal violations. Our results suggest that mobile implementations of the TCF are prone to significant non-compliance practices, raising concerns about its effectiveness in helping organizations adhere to legal requirements.

Keywords

Android, online tracking, consent banner, online privacy, compliance, TCF v.2.2, legitimate interest, GDPR, ePrivacy Directive

1 Introduction

The majority of Web traffic now originates from mobile devices [91], and in the past five years, Android has remained the most widely used mobile operating system (72.55% in October 2025) [93]. It has become increasingly common to rely on mobile apps – generally distributed through the Google Play Store –, to communicate and interact with devices and services, a phenomenon known as *appification* [15]. However, the widespread use of these apps is accompanied by a large-scale tracking impacting users' privacy [8]. In the European Union (EU), personal data collection and processing is strictly regulated. The General Data Protection Regulation (GDPR) [20] and the ePrivacy Directive (ePD) [32] specify legal requirements for data controllers (herein mobile app publishers[1] and website owners) to process end-users's personal data. In particular, data protection law mandates that controllers identify a valid legal basis for each purpose of processing under Article 6 of the GDPR. Regulatory and enforcement decisions have consistently affirmed that consent is the *only* lawful basis for online behavioral advertising, instead of legitimate interest [10, 24].

To help organizations request user consent according to the legal requirements, the Interactive Advertising Bureau (IAB) Europe – the leading industry association for the digital marketing and advertising ecosystem in Europe – introduced in April 2018 the Transparency and Consent Framework (TCF) [50]. The TCF is

Proceedings on Privacy Enhancing Technologies 2026(3), 6–31

https://doi.org/10.56553/popets-2026-0068

[1]The French DPA (CNIL) qualifies app publishers as data controllers, and note that publishers and developers often merge in practice, although external developers can be considered a different contractual entity [19, p17,p7].

widely seen as the leading industry standard for managing online consent [99], and although academic literature demonstrates instances of its non-compliance practices on the Web [14, 63, 72, 73], fewer work can be found on mobile contexts [64]. Although the TCF purports to help organizations meet EU data protection law obligations, its deployment does not guarantee compliance. Prior analysis has shown that websites relying on earlier TCF versions (*i.e.*, v.1.1) violated data protection law despite formally implementing the framework [72, 77, 97]. Specifically, the Belgian Data Protection Authority (APD) ruled in 2022 [16] that the TCF was non-compliant with the GDPR as it allowed the use of "legitimate interest" for targeted advertising – a legal basis deemed incompatible with the intrusive nature of large-scale behavioral tracking and profiling. The APD therefore required IAB Europe to remove "legitimate interest" as a valid ground for processing data for advertising purposes. Furthermore, the ruling concluded that the framework's consent mechanism failed to meet the GDPR consent requirements. The EU Court of Justice held that the TC String, used to record users' consent preferences, can constitute personal data and it also found that IAB Europe may act as a joint controller with TCF participants even if it does not directly access the data [25].

The framework has undergone several revisions since these rulings. The update (v.2.2) introduced in May 2023 required all TCF participants to implement the new version by November 2023. A major change introduced in this update was the removal of "legitimate interest" as a legal basis for processing personal data to create personalized ads and content [51]. While this reform was intended to be legally compliant, it remains unclear whether the framework is consistently implemented and compliant. V.2.3 superseded v.2.2 on March 1st 2026, without incidence on our results.

In practice, respect of GDPR requirements appears to have a long way to go on mobile. Previous research on the GDPR compliance of Android apps found that 28% of 86000 apps potentially violated the GDPR by sending users' personal data to ad providers before users' consent was obtained [80]. Furthermore, TCF-based websites have frequently been shown to contain potential privacy violations [72], suggesting that similar issues may also occur in TCF-based Android apps. Despite these findings, research on TCF implementations in Android apps remains limited, and no prior studies have examined their use of legitimate interest as a legal basis for data processing. To address this gap, we aim to investigate TCF-based Android apps by answering the following research questions:

RQ1 How prevalent are TCF-based apps in the Google Play Store, and what are their characteristics (*e.g.*, categories, country of origin, etc.)?

RQ2 Do TCF-based apps respect users' consent choices and the TCF's requirements introduced by the v.2.2 not to use legitimate interest for certain purposes?

RQ3 Do TCF-based Android apps respect users' choices regarding personal data collection at runtime?

To address these questions, we collaborated with a legal scholar in EU Data Protection law and we make the following contributions:

(1) We measure the prevalence of TCF in popular Android apps, including the first fine-grain quantification per category, and find a significant increase in its adoption, rising from 6.6% reported in 2023 [64] to 12.85% in our dataset.
(2) We design a methodology to semi-automatically interact with consent banners deployed by major Consent Management Providers (CMPs) in TCF-based Android apps, combining three approaches capturing different choices to data collection: "disagree to all" purposes, "legitimate interest purposes only", and "consent to all".
(3) We perform the first systematic assessment of personal data processing in TCF-based Android apps through traffic analysis. Our results indicate that 15 apps stored consent choices only when provided with "consent to all" data processing, and that most apps (66.2%), with gaming apps as the top violators, share AAID to ad servers against users' choices. We perform a legal analysis to assess compliance with GDPR and ePD requirements, which exposes several potential legal violations. These results suggest a systemic breakdown in the ability of the TCF to facilitate legal compliance, questioning its effectiveness as a privacy-governance mechanism.
(4) We expose concerns regarding Google as the dominant CMP in our dataset (89.76%), structurally accommodating potential legal violations, and offering bad defaults (pre-selected legitimate interest-based purposes).

2 Background Knowledge

This section introduces background related to GDPR and the ePD, AAID, and TCF.

2.1 EU Data Protection Law

The GDPR came into force in 2018, and applies to any organization worldwide that processes personal data from EU users [34], called data controllers in this context. Data controllers (app publishers in our context) "determine the purposes and means of the processing of personal data", they bear legal responsibility for processing. The GDPR imposes obligations on data controllers, paired with hefty fines for non-compliance. The ePrivacy Directive (ePD) provides *supplementary* rules to the GDPR, in particular for the use of tracking technologies. Whenever any information (including cookies and other tracking technologies) is stored and read from the user's device, the ePD [32, Art. 5(3)] requires organizations to request user *consent* to process data for certain *purposes*, such as advertising [30, 31]. The only way to assess with certainty whether consent is required is to analyze the *purpose* of each tracker on a given website (or app in our context) [29, 39, 90].

Personal data. Personal data is *"any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"* [20, Art. 4(1)]. In order to determine whether a person is *identifiable*, account should be taken of all the means likely to be reasonably used by the data controller (herein the app publisher) to identify that person (Recital 26 GDPR). Account should be taken by this actor's specific situation – *i.e.*, whether it has reasonably likely means to determine whether information constitutes personal data, according to the recent interpretation of personal data in case-law [26].

GDPR obligations for data controllers (app publishers in our context). In the following, we consider the relevant requirements and principles derived from both the GDPR and guidelines from the European Data Protection Board (EDPB).[2]

Data controllers can be held responsible and fined if they fail to comply with the following obligations under the GDPR [20, Art. 28(3)(f), 32-36]. Relevant GDPR principles are presented below and numbered with P, and legal requirements for consent revocation are numbered with LR.

- *P1 Lawfulness*: When processing personal data, data controllers must collect personal data only with a valid legal basis (Art. 5(1)(a)), such as consent or legitimate interest (LI). In the context of online tracking for (non-essential) advertising purposes, consent is the lawful legal basis according to Article 5(3) of the ePrivacy Directive. Further, the GDPR imposes strict requirements for valid consent. Consent must be i) prior to any data collection, ii) freely given, iii) specific, iv) informed, v) unambiguous, vi) readable, accessible, and vii) revocable (Articles 4(11) and 7 GDPR) [89]. To be freely given, users must be able to accept or reject consent without facing negative consequences.
- *LR1 Correct registration of consent*: Data controllers must correctly register the user consent revocation decision, and assure that the decision made by the user in the banner interface is identical to the consent that gets registered/stored by the website [20, Arts. 7(1), 30, Rec. 42], [60, 89] (p.9). A *violation* occurs when a registered consent is different from the user's choice.
- *P2 Fairness:* Data controllers must not process personal data in a unjustifiably detrimental, discriminatory, unexpected or misleading way [20, Art.5(1)(a)], [28, para 17].
- *P3 Transparency*: Data controllers must inform users about purposes, recipients, and legal bases when collecting data (Art. 5(1)(a), 13-14);
- *P4 Data Protection by Default*: Data controllers must process data with the highest privacy settings by default (Art. 25(1)(2));
- *P5 Data Protection by Design*: App developers must implement organizational measures and technical safeguards efficiently [35], [20, Art. 25(1)].
- *P6 Security*: Data controllers must ensure data protection to prevent unauthorized access (Art. 5(1)(f), 32);

2.2 Google Advertising ID (AAID) as Personal Data

Google Advertising ID. Google Advertising ID, technically identified as `AAID`, is a unique identifier assigned to every Android mobile device. It is the *de facto* identifier used within the Android ecosystem for targeted advertising [42]. Because the AAID is unique to each device, advertisers rely on it to build personalized ad profiles. Google's own Android Developers documentation instructs app developers to restrict the use of this identifier to "user profiling or ads use cases", and "always respect users' selections regarding ad tracking" when collecting it [4].

AAID as personal data. The online advertising industry, represented by IAB Europe, explicitly acknowledges that mobile advertising identifiers – including AAID – qualify as personal data under the GDPR [59]. This qualification is consistent with GDPR Recital 30, which states that identifiers provided by a user's device, such as IP addresses or other device identifiers, may be used to single out individuals, thereby making them identifiable. The AAID mobile identifier is a direct example of such an "online identifier". It is technically persistent, unique to the device, and is routinely used to track user behavior across apps and services. The French Data Protection Authority (CNIL) takes a similar stance, noting that mobile identifiers like the AAID fall under the scope of Article 5(3) of the ePrivacy Directive [19]. This means their access and storage require user consent.

[2]The EDPB is composed of representatives of all EU Data Protection Authorities (DPAs), EDPB guidelines play a central role in streamlining the interpretation of GDPR.

Table 1: TCF purposes v2.2, where purposes 1, and 3-6 require consent according to the TCF [53].

Nr	Name	Consent
1	Store and/or access information on a device	Required ✓
2	Use limited data to select advertising	
3	Create profiles for personalised advertising	Required ✓
4	Use profiles to select personalised advertising	Required ✓
5	Create profiles to personalise content	Required ✓
6	Use profiles to select personalised content	Required ✓
7	Measure advertising performance	
8	Measure content performance	
9	Understand audiences through statistics or combinations of data from different sources	
10	Develop and improve services	
11	Use limited data to select content	

2.3 IAB's Transparency and Consent Framework and Compliance

The current *de facto* standard for the consent banners in the EU is the IAB Europe Transparency and Consent Framework (TCF). The TCF was created in April 2018 with the goal of helping data controllers process data according to the legal requirements set by the ePD and the GDPR. It was developed for use by its participants: i) Publishers of online content where data can be collected, including app publishers, ii) vendors which process user data gathered by the publishers, iii) and Consent Management Platforms (CMPs) which develop consent banners. CMPs provide consent management as-a-service, through consent banners embedded in websites and in mobile apps, which request consent and inform users the vendors that can access user data, the purposes these vendors process data for, and the legal bases utilized under these purposes [50].

Defined purposes. The current TCF v2.2 [51] defines the *predefined purposes* for processing personal data by CMPs (presented in Table 1), each requiring either consent or legitimate interest as a lawful basis to process data. Versions prior to TCF 2.1 permitted websites and apps to rely on the legal basis of legitimate interest for all the purposes for processing data. Version 2.1 removed legitimate interest for Purpose 1 (*Storage or access data to recognise devices*), and version 2.2 removed legitimate interest from personalization-related purposes (Purposes 3-6) [53]. Despite these changes, recent work still criticizes IAB's interpretations of legal

grounds for these purposes [63], arguing that purposes 2 (Use limited data to select advertising), 6 (Use profiles to select personalised content), 7 (Measure advertising performance), 8 (Measure content performance) and 9 (Understand audiences through statistics or combinations of data from different sources) require consent. Accordingly, such purposes should not be enabled by default in the IAB Europe TC string.

Defined format. The TCF also defines the *format to store the user's choice*, called TC string. When a user interacts with websites or mobile apps which uses the TCF, each website and app will generate a TC string on the user's device containing the user's consent choices. This TC string has been qualified as *personal data* [16]. When interacting with websites, the TC strings are stored as HTTP cookies in the user's browser by CMPs. On mobile devices, the TC strings are stored locally under two separate strings: `IABTCF_PurposeConsents` and `IABTCF_PurposeLegitimateInterests`. Vendors have access to and decode the TC string, and should therefore only process data according to the user's choices [49], [54], [56].

Version 2.3. IAB Europe released on June 19th 2025 version 2.3 of the TCF, with a transition period ending on February 28th 2026 [58]. This new version mostly targets vendors, as it addresses signaling ambiguity. It introduces a new field in the TC string (`IABTCF_DisclosedVendors`) to alleviate ambiguity for vendors declaring two types of purposes ("Special Purpose(s) and Purpose(s) under LI", where a special purpose is a processing purpose for which the user is not given choice by a CMP). CMPs are also impacted since this new `IABTCF_DisclosedVendors` segment must be disclosed in the user-facing CMP UI. This new version does not address any of the issues raised in the present article.

3 Related Work

This section surveys prior work and shows that earlier TCF versions enabled potential GDPR violations on the Web, that websites frequently exploited the legal basis of legitimate interest to extract more user data, and that similar compliance shortcomings persist in Android and iOS mobile apps.

3.1 Potential GDPR Violations in TCF Research

Matte et al. [72, 73] provided one of the earlier accounts of a systematic study of the TCF. In their empirical work, they crawled 22949 websites, of which 1426 were using the TCF. They performed extensive tests on 560 of these websites, and concluded that 54.0% of them were potentially violating both the GDPR and the ePD. Violations included websites sharing user consent through "shared cookies", and storing consent before giving users a choice, preselected choices, amongst others.

Smith et al. [92] studied in 2023 websites using a more recent version of the TCF (v.2.1). It is, to the best of our knowledge, the most recent study of GDPR compliance on websites using the TCF. The authors denied consent in consent banners of 2 230 websites using TCF-based cookie banners. Their results show that a majority of the websites were using legitimate interest for purposes 3-6, which are reserved for personalization and subsequently not allowed in TCF v.2.2 (see Section 2). They concluded from a TCF string analysis that 1.3% of the websites studied had potential GDPR violations, including legitimate interest being used for Purpose 1. Morel et al. [77] found that that websites using cookie paywalls[3] always used the TCF. The authors also found websites that deployed legitimate interest to track users even if they chose to pay a fee.

3.2 Potential Privacy Violations in Mobile Apps

Nguyen et al. [80] conducted the first large scale study of potential GDPR violations in Android mobile applications between 2021 and 2022. The authors initially crawled one million applications over five months, and selected 86000 of these apps for analysis (without banner interaction). Using mitmproxy to analyze the network traffic, and Objection to disable SSL pinning (a necessary technical measure preventing apps from expecting communication with a specific host only), they could confirm when applications transmitted their personal data – such as advertising IDs and location data –, without receiving explicit consent. Their results show that 28% of the studied applications potentially violated the GDPR.

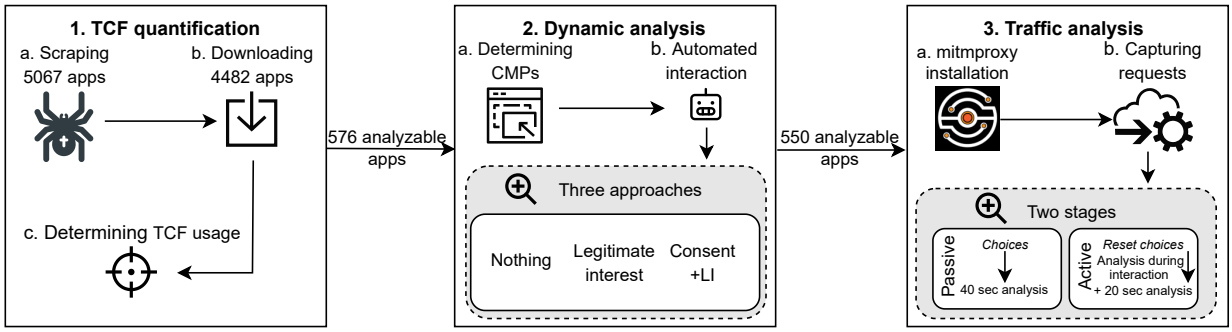
Koch et al. [64] investigated consent banners between 2022 and 2023 in Android and iOS applications. This paper furthers the analysis of Altpeter [2], which performed a similar study in 2022. Altpeter analyzed a dataset of 3421 Android apps, with 2.6% of apps using the TCF. The Android applications studied by Koch et al. were scraped from the top lists of all categories in the Google Play Store, where the authors used the top 100 apps of each category, resulting in a dataset of 3 006 apps. They found that 6.6% of the applications used the TCF. After downloading the applications, they performed a static analysis on the preference folder of the app to assess whether a majority of the applications used the same CMPs. Other than the TCF-compliant CMPs, most applications used their own solutions to inform users and elicit consent. They deepened their analysis using Appium (v2.15.0), a software to automate mobile app testing.[4] They were able to classify how the apps presented their consent banner when launched, where the banners were classified as 1) links, 2) notices, or 3) proper banners. They observed that of the three alternatives, only the proper banners required users to interact by consenting or denying data collection before using the app, while the others stated that data will be collected if the user continues to use the app. Lastly, the authors analyzed the apps' traffic, similarly to the methods presented by Nguyen et al. [80]. The analysis was performed by comparing the data transmitted by applications with what the authors had consented to in the applications. The results show that 43.1% of total studied apps on Android and iOS potentially violated the GDPR. No work had previously systematically studied the privacy implications of the TCF on Android applications.

4 Methodology

We describe in this section our methodology. We begin by explaining in Section 4.1 how we scraped the Google Play Store and downloaded apps to quantify the prevalence of the TCF, addressing **RQ1**. We then describe in Sections 4.2 and 4.3 how we analyzed TCF-based applications through dynamic and traffic analysis, answering **RQ2** and **RQ3** respectively. A visual overview is provided in Figure 1.

[3] Cookie paywalls allow visitors of a website to access its content only after they make a choice between paying a fee or accept tracking.
[4] https://appium.io/docs/en/latest/

Figure 1: Schematic overview of the three steps of the methodology. First, we quantify the TCF in a dataset of 4482 apps scraped on the Play Store (Section 4.1). Second, we automate the interaction with consent banners on 576 apps according to three approaches (Section 4.2). Third, we analyze network traffic of up to 550 apps in two stages (Section 4.3).



Scope and technical setup. This paper only targets TCF-based Android applications, and no applications on other operating systems such as iOS. We crawled the top apps of each category (see also Appendix A for the rationale behind this technical choice) of the Google Play Store (also called Google Play or Play Store) until we collected at least 5000 applications (66% more than the state of the art [64] for a similar type of analysis) between 2025-01-29 and 2025-03-10. All results are based on data gathered from applications in this dataset. We believe our sampling set is representative of Android applications because it represents popular and commonly used apps. We accessed the Google Play Store with a fixed EU vantage point (verified between app launches), ensuring that EU data protection laws (*i.e.*, the GDPR and the ePD) apply. We used a newly created Gmail account dedicated to the project and a phone number automatically generated by the emulator. To avoid inter-app interaction (during the dynamic and traffic analysis), apps were deleted between testing two of them once their analysis was completed.

4.1 Quantifying the Presence of the TCF

4.1.1 Scraping Apps. We first created a dataset consisting of application package names, application names, application category and the date of scraping. We used Selenium[5] (v4.28.1), a software used to automate browser interactions. Our Selenium instance was not logged in our Google account while crawling, and used the same IP and location throughout the scraping. The Play Store possesses top charts for each category: https://play.google.com/store/apps/category/CATEGORY which contain between 60 and 900 applications depending on the category. The Play Store offers 49 categories[6], or 56 with the *family* apps (targeting children). We scraped all categories daily between 2025-01-29 and 2025-03-10, until we obtained 5067 unique applications.

4.1.2 Downloading Apps. We then instantiated an emulated Android device through Android Studio[7], allocated it with 300 GB of storage and gave the device superuser privileges by using Magisk[8], a software used to root Android devices. The device was selected to be a Google Pixel 9 Pro using API 35. Google Pixel 9 Pro was the newest available device in Android Studio at the time of the study, and API 35 was a recent stable release. We created an ad-hoc solution to download applications, building upon the Android Debug Bridge[9] (`adb`), a Unix shell allowing for interaction with emulated and real Android devices. Since the Play Store application worked on the emulated device, we were able to automatically download applications. When launching the Play Store from the emulated device through `adb`, it was possible to provide an app package name to be directly redirected to the app's page in the Play Store and proceed with downloading the application.

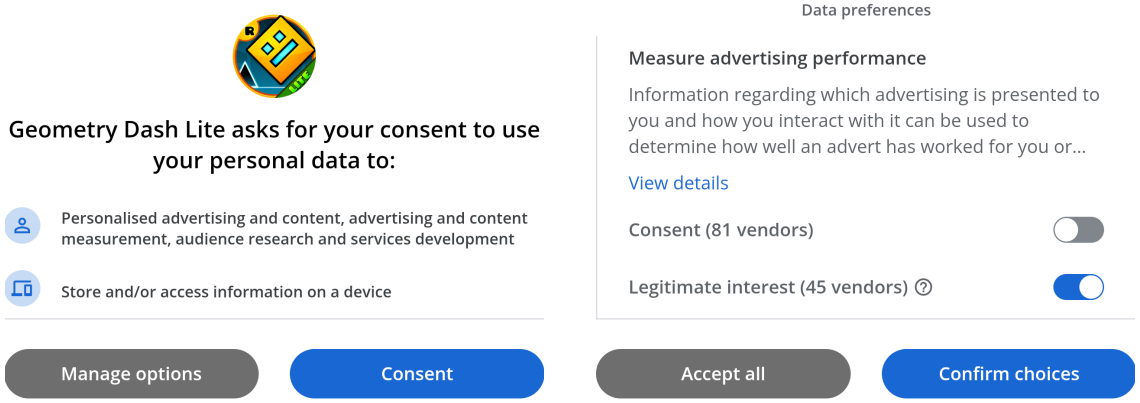
4.1.3 Determining Apps' TCF Usage. According to the IAB's CMP API, applications using the TCF should store their TC Strings (such as `IABTCF_TCString`) in files stored in the `SharedPreferences` directory[10] [49]. We launched and closed apps using the `adb` commands `monkey` [11] and `am force-stop` [12] to generate the `SharedPreferences` directory of applications. The script then executed the Unix-command `grep` (a utility for searching patterns in a file) on all files in the apps' generated `SharedPreferences` directory, searching for mentions of `IABTCF`.

However, apps could well initialize the framework without implementing a banner, we therefore confirmed the presence of the TCF by restricting our data analysis to apps able to present a banner. The previous steps nonetheless provided an initial pruning of the data to a restricted set of candidate apps.

4.2 Dynamic Analysis

To assess whether TCF-based apps correctly store users' choices, we performed a dynamic analysis using `adb` and Appium, as the latter also enables an automatic launch of apps and interaction with their consent banners. Since the design of consent banners are

[5]https://www.selenium.dev/
[6]https://www.searchapi.io/docs/parameters/google-play-store/categories
[7]https://developer.android.com/studio
[8]https://magiskmanager.com/#What_is_Magisk
[9]https://developer.android.com/tools/adb
[10]SharedPreferences is a directory which typically contains files composed of collections of key-value pairs for an Android application.
[11]A command-line tool ran on any emulator instance or on a device, it sends a pseudo-random stream of user events into the system.
[12]To force-stop an activity. In an Android context, an activity is a window where an app has its UI, activities may sometimes float over another activity, such as pop-ups cf https://developer.android.com/guide/components/activities/intro-activities



(a) First layer of the consent banner. **(b) Detail of a purpose. All LI purposes are pre-checked.**

Figure 2: Consent banner settings for Google LLC (CMP 300), from the application Geometry Dash Lite (com.robtopx.geometryjumplite). The two screenshots show default interfaces.

based on the CMP used, we therefore initially researched the most common CMPs in our dataset to streamline our analysis.

4.2.1 Determining CMPs. In a majority of applications, the CMP could simply be found in the app's `preferences.xml` file in its `SharedPreferences` directory by looking at the string `IABTCF_CmpSdkID`. If not, we manually launched the application and inspected its consent banner for patterns. Some applications had their CMP mentioned in other files in their `SharedPreferences` directory, and some applications had their CMP included in their application package name, such as `com.outfit7.mytalkingtom2` where the CMP is Outfit7. After having obtained the CMP of each application, we manually inspected some consent banners of each CMP to establish cases later used to automate the interaction via Appium. A majority of cases consisted of waiting for certain elements to show up on the mobile screen, and then scrolling through the consent banner to interact with buttons and toggle-buttons based on the buttons' content-description- or text-elements.

4.2.2 Automated interaction. To determine which elements we interacted with, we first manually investigated consent banners from each CMPs to find regularly occurring sentences/words on target buttons, we then used those recurring sentences as *target sentences*. These target sentences were used as input into a Python function using the multilingual sentence similarity model `paraphrase-multilingual-MiniLM-L12-v2` [85, 86]. The function also takes a list of expected texts and then outputs the element most likely to be the one we want to interact with according to a threshold. The model created was later passed as instructions to Appium. If our automated interactions failed, *i.e.*, we failed to interact with buttons in a banner, we would manually look at the banner in question and potentially add the sentences from the app's buttons as target sentences, thereby refining the model. We validated our automated banner interactions by confirming on a random sample that the `SharedPreferences` of the sampled apps had the expected values (*e.g.*, no purposes in use if our automatic interaction was denying all purposes).

The most commonly used CMP in our dataset is Google LLC (CMP 300, see Table 3), a screenshot is presented as an example in Figure 2. This CMP allowed us to interact with consent and legitimate interest in a standardized manner after clicking "Manage option". Figure 2b shows a detail of the purpose "Measure advertising performance" and how it includes both legitimate interest and consent, with consent following an opt-in basis and legitimate interest an opt-out basis. Other CMPs provided less standardized interfaces (the UI could greatly vary across different implementations), or had various extra steps to reach the options containing consent and legitimate interest, requiring additional manual tuning.

4.2.3 Banner Interaction Approaches. We interacted with consent banners through three different approaches:

(1) agree to all, denoted **C+LI**,
(2) legitimate interest purposes only, denoted **LI**,
(3) disagree to all, denoted **Ø**.

The first approach enables a broad analysis of the apps' traffic, determining what personal data is being transmitted to different servers when permission is given by the user. The rationale behind the **LI**-approach was to analyze whether any legitimate interest purposes forbidden by the TCF were actually in use, while the **Ø**-approach should yield a lower bound for data collection. We also used the **Ø**-approach to analyze the traffic of applications, and to compare the data transmitted without consent versus the data transmitted with consent to all (**C+LI**-approach). An approach where we provide consent without legitimate interest would be meaningless, as this has no functional difference from the **C+LI**-approach where we agree to everything. A visual representation of the three different approaches can be seen in Table 2.

All three approaches required interacting with each CMP in three different ways. The **C+LI**-approach often solely required pressing an "accept all"-button. The **LI**-approach demanded locating the button allowing a manual change in our banner choices, followed by a confirmation of the choices automatically provided (since legitimate interest is on an opt-out basis). The **Ø**-approach required manually

Table 2: Purposes accepted according to their legal bases during each interaction approach.

Approach	Consent	Legitimate Interest
Agree to all (C+LI)	✓	✓
Leg. Int. purposes (LI)	**X**	✓
Disagree to all (Ø)	**X**	**X**

changing our choices, and then opting-out of every purpose related to legitimate interest.

4.2.4 Confirming Stored Banner Choices. Upon interaction with consent banners, we confirmed the choices stored by the applications in their `preferences.xml` file. We leveraged the Unix-command `grep`, parsing relevant strings such as `IABTCF_PurposeConsents` and `IABTCF_PurposeLegitimateInterests`. These strings act as two TC strings (one for each legal ground), and should therefore reflect users choices. We stored the results from our interactions with consent banners in CSV files.

4.3 Traffic Analysis

We captured network traffic of apps in our dataset to evaluate their respect of user choices (disagree to all, legitimate interest only, agree to all), and analyzed eventual personal data collection. We leveraged the mitmproxy suite[13] (v.11.1.3) to capture traffic, and Objection (v.1.11.0) to disable SSL pinning[14]. Objection is a toolkit powered by Frida [40], which therefore additionally required installing a Frida server on our device.

4.3.1 Traffic Analysis Preparation. We initialized our setup by installing and trusting mitmproxy's certificate authority [76], allowing mitmproxy to decrypt encrypted traffic. The certificate authority was downloaded on our device through a Magisk module [71]. We ensured that our device had a European IP and that the device's GPS coordinates were set in an EU country to ensure that the GDPR and the ePD applied to our device. These coordinates could then be seen in the device's fused location, which is described by Google as a combination of underlying location technologies, such as GPS and Wi-Fi [27]. We accessed the device's coordinates by using the `adb`-command `dumpsys location`.

4.3.2 Traffic Analysis Workflow. We captured traffic by combining the mitmproxy functionality `mitmdump` with a Python script of our choice as a mitmproxy addon, allowing for customization of mitmproxy's behavior. The add-on running alongside `mitmdump` searched through the payload and URL of each HTTP-request on our emulated device for personal data. To identify personal data[15] in requests, we used a) hard-coded strings, b) strings based on running `adb` commands to extract present data on the device – such as `AAID` and location data –, and c) regular expressions for data such as the device's phone number and MAC address, due to the different formats they could be presented in. Informed by the literature, we use the following list: *AAID, public IP, email, phone number, IMEI, MAC address, GPS location, IMSI, ICCID and phone serial number.* If any personal data was found in a request, we stored the following in a Postgres-database: the application package name, the personal data being transmitted and the request method, the request-url, the type of personal data being transmitted, and the date of the request.

We then launched each application through Objection with the startup-command `android sslpinning disable` – which allowed for traffic collection in apps –, and captured traffic before launching the next one (according to two stages further described in Section 4.3.4). Certain applications would detect SSL pinning being disabled and crash. We therefore confirmed the running of the application by monitoring processes on the device. If the process related to the current application was preemptively terminated, we re-executed the app up to two times, before labeling the app as non-analyzable and moving on to the next application.

4.3.3 Device Snapshots. The crash of an app would occasionally cause our device to crash or reboot, slowing down the analysis. We took regular snapshots of our device to work around this mishap, preserving the device's state at the time of the snapshot [6]. Using snapshots was much faster than rebooting the phone and was a necessity as the crashes were frequent during our traffic analysis. We created a snapshot for each dynamic analysis approach, capturing the application state at the point when our banner choices had been stored for that specific approach.

4.3.4 Stages of Traffic Analysis. In addition to capturing traffic during the three approaches previously mentioned, we analyzed apps' traffic in two stages, called *passive*- and *active*-stages.

Passive-stage: we analyzed apps' traffic for 40 seconds while the apps remained passive, when the banner choices were already stored. The rationale of this stage was simply to observe the traffic *ex-post* to the user choices communicated in the banner, without any additional interaction with the banner from our side (hence, the name *passive*).

Active-stage: we reset all banner choices, and then analyzed traffic during display or navigation of the apps' consent banners (before the user confirms consent choices), and also while idling for 20 seconds after a choice was made. The rationale behind this second stage was to enable observation of the network traffic *during* the interaction with consent banners (hence, the name *active*).

5 Results

This section presents the number of applications scraped and the percentage of them using the TCF, answering **RQ1**. It then introduces the results of our dynamic analysis, assessing the registration of banner choices, addressing **RQ2**. Last, it presents the results of our traffic analysis, across the three approaches (described in Section 4.2.3) and the two stages (described in Section 4.3.4), answering **RQ3**. The raw data used to produce the results can be found in our public repository [1].

[13] Suite of tools that provides an interactive HTTPS-capable interceptor proxy: https://mitmproxy.org/

[14] Method used by Android apps to prevent man-in-the-middle attacks: https://www.indusface.com/learning/what-is-ssl-pinning-a-quick-walk-through/

[15] We focused on unique identifiers, since the definition of personal data in the GDPR leaves little room for interpretation: "an identifier such [...] an identification number, location data, **an online identifier**" (emphasis is ours).

Table 3: Consent Management Platforms (CMPs) found in TCF-based applications, including their prevalence. The ID is used by the TCF to identify CMPs.

ID	Name	Number of apps	Proportion
300	**Google LLC**	**517**	**89.76%**
5	Usercentrics	16	2.78%
350	Easybrain Ltd	14	2.43%
No id	Data Unavailable	11	1.90%
348	Outfit7 Limited	9	1.56%
7	Didomi	7	1.22%
28	OneTrust LLC	2	0.35%

5.1 Quantifying the TCF

The Play Store was scraped daily, between 2025-01-29 and 2025-03-10, resulting in an initial dataset of 5067 apps. Downloading was performed between 2025-02-04 and 2025-03-12. 585 of the 5067 apps presented issues during downloading, for a total of 4482 downloaded apps. Some apps were premium and required a payment to install, a few apps were pre-registrations and did not provide an installable option at the time, and some applications were removed from the Play Store between the creation of our dataset and our attempted download. The most prevalent reason was the detection of an emulated device, the installation button was then replaced with the message: "Your device isn't compatible with this version.". We did not record the distribution of the failure analysis.

5.1.1 Google is by far the main CMP found in TCF-based apps. We encountered twelve different CMPs in our dataset, presented in Table 3. The most common CMP in the dataset was Google LLC with a large majority, amounting to **89.76%** of apps. The distribution follows a power law distribution, with one CMP being clearly more prevalent than the others, and a long tail of five CMPs amounting to less than 10% of the total, indicating an extremely unbalanced distribution amongst CMPs.

Table 4: Top 10 TCF-based app categories

App Category	TCF usage
PERSONALIZATION	54/101 (53.47%)
LIBRARIES_AND_DEMO	26/76 (34.21%)
ART_AND_DESIGN	27/79 (34.18%)
VIDEO_PLAYERS	20/67 (29.85%)
TOOLS	26/90 (28.89%)
PHOTOGRAPHY	22/77 (28.57%)
MAPS_AND_NAVIGATION	22/86 (25.58%)
PRODUCTIVITY	16/67 (23.88%)
MUSIC_AND_AUDIO	20/85 (23.53%)
WEATHER	15/65 (23.08%)

5.1.2 TCF-based apps can be found in all Play Store categories and many countries outside the EU. As we scraped the Play Store per app category, we were able to provide the first quantification of TCF-based Android apps per category and country. The most common app categories using the TCF in our dataset are: Personalization (53.47%), Libraries and Demo (34.21%), and Art and Design (34.18%) (see Table 4, and Table 10 for the comprehensive data).

We additionally quantified the country of origin of apps in our dataset. We found that **82.14% of apps were developed in non-EEA countries**. Only one country (Cyprus) in this top 10 is part of the EU/EEA (see Table 5), with three other adequate in the sense of GDPR Article 45 according to the EU Commission [33] (USA, Israel, UK). See Table 11 in the Appendix for the comprehensive data.

Summary: In total, 576 apps were identified as implementing the TCF (842 initialize the framework, but 576 were confirmed to use the TCF), representing 12.85% of the downloaded apps. TCF-based apps are widely spread across categories, although Personalization has a significant lead (53.47%, vs. 34.21% for the runner-up). Most of the TCF-based apps are developed outside the EU/EEA or adequate countries (in the sense of GDPR Article 45).

Table 5: Distribution of the top 10 countries where TCF-based apps in our dataset were developed

Country	Number of TCF-based apps in our dataset (N = 576)
Vietnam	94 (16.32%)
Hong Kong	60 (10.42%)
Cyprus	41 (7.12%)
China	41 (7.12%)
Israel	36 (6.25%)
India	36 (6.25%)
United States	27 (4.69%)
Pakistan	22 (3.82%)
United Kingdom	17 (2.95%)
United Arab Emirates	15 (2.6%)

5.2 Dynamic Analysis

Regardless of the interaction method, none of the 576 analyzed apps used legitimate interest-based purposes forbidden by the TCF (see Section 2.3). However, 15 apps only stored our choices if provided with consent to all data processing, the user would otherwise be prompted with a consent banner to provide consent again on the next launch of the app: *Sweet Beauty Camera Filter, Geotag Photo: Camera Location, Control Center Simple, Draw Animation - Anim Creator, Silly Smiles Live Wallpaper 4K, AR Draw Sketch: Trace & Paint, Easy Piano Keyboard - Piano88, Find Phone by Clap, Whistle, Caller ID Name, Location & SMS, Chat AI - AI Chatbot Friend, Dating - Chat & Meet Singles, Locate Mobile by Number, Phone Tracker By Number, Books - Read and Download, PDF Viewer: PDF Fill & Sign* (see Table 12 for the package names).

Summary: In total, **15 apps only stored our choices if provided with consent to all data processing**, but our analysis did not capture apps misimplementing TCF purposes.

Table 6: Traffic analysis results per phase of interaction. The last column contains the active-stage results amended with data from apps sharing AAID during consent banner interaction OR during a given approach.

Banner Interaction	Passive-stage (N = 550)	Active-stage (N = 513)	Active-stage Amended (N = 513)
LI-Approach	351 (63.8%)	192 (37.4%)	339 (66.1%)
Ø-Approach	364 (66.2%)	145 (28.2%)	330 (64.3%)
C+LI-Approach	367 (66.7%)	217 (42.3%)	347 (67.6%)
During Interaction	-	284 (55.3%)	-

5.3 Traffic Analysis

We detail the prevalence of personal data (see Footnote 15) shared by TCF-based apps in our dataset to third-party domains (see Section 5.3.3), according to the two stages of analysis performed (*passive* and *active*) and across the three interaction approaches (**Ø**, **LI**, and **C+LI**). The only types of data captured in our analysis are AAID and IP addresses. Since an IP address is also collected for communication purposes in order to initiate HTTP requests, we only present results regarding AAID collection. A summary of our results can be found in Table 6. Assuming that our sample is representative of TCF-based apps, **up to 66% of apps share AAID without consent**.

5.3.1 Passive-stage. Of the 561 apps that we could interact with in the dynamic analysis, 550 apps (98.03%) had their traffic analyzed during the *passive*-stage between 2025-03-23 and 2025-05-17. 11 apps could not have their traffic analyzed as they would instantly crash or deny SSL pinning being disabled. Using the **LI**-approach, 351 applications were found to transmit AAID. Using the **Ø**-approach, 364 applications were found to transmit AAID. Using the **C+LI**-approach, 367 applications were found to transmit AAID.

5.3.2 Active-stage. We obtained slightly different results for the *active*-stage, during which we analyzed the traffic before and while interacting with apps' consent banners. This analysis was conducted between 2025-05-15 and 2025-05-21, during which we inspected network traffic for 513 apps (91.44% of the apps analyzed in Section 4.2). 37 additional apps could not have their traffic analyzed in this stage since they had been removed from the Play Store, no longer presented a consent banner, or instantly crashed on launch. During this stage, we found 284 apps that transmitted AAID before or during banner interaction, prior to obtaining consent. Using the **LI**-approach, 192 applications were found to transmit AAID. Using the **Ø**-approach, 145 applications were found to transmit AAID. Using the **C+LI**-approach, 217 applications were found to transmit AAID.

5.3.3 Domains Receiving AAID. We collected the domains (as a combination of SLD and TLD, we do not differentiate subdomains in our analysis) most often contacted with AAID across all interactions approaches per app (see Figure 3). The five most common domains receiving AAID are:

(1) Facebook.com
(2) Rayjump.com[16]
(3) Adjust.com
(4) Unity3D.com
(5) Google.com

[16]Note that rayjump.com is widely seen as a scam/malicious website [7, 75].

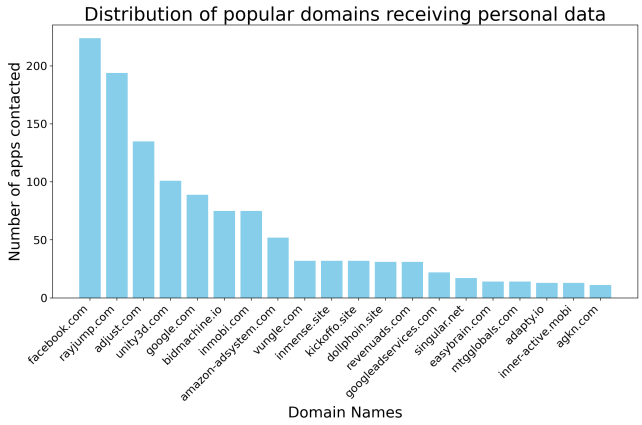


Figure 3: Distribution of popular domains (minimum 10 apps) receiving personal data.

5.3.4 Games are the top app categories sharing AAID without consent. A cross-examination on the categories of apps (combined passive and active stages, on both **LI**- and **Ø**-approaches) yields that game apps are the top apps sharing AAID without consent. Table 7 presents the top 10 categories of apps that share AAID without consent, see Table 13 for the comprehensive data.

Table 7: Top 10 categories of apps that shared AAID (combined passive and active stages, on both LI- and Ø-approaches)

Category	Violation %
GAME_SIMULATION	12/12 (100.0%)
GAME_ARCADE	12/12 (100.0%)
GAME_SPORTS	11/11 (100.0%)
GAME_CASUAL	10/10 (100.0%)
GAME_CASINO	4/4 (100.0%)
EDUCATION	3/3 (100.0%)
AUTO_AND_VEHICLES	2/2 (100.0%)
GAME_BOARD	12/13 (92.31%)
GAME	23/26 (88.46%)
PRODUCTIVITY	14/16 (87.5%)

5.3.5 Results per developer and per CMP. We grouped our results per developer to investigate whether developers adopt the same

Table 8: Violating apps per CMP in passive stage

CMP	Violation %
Easybrain Ltd	14/14 (100.0%)
Outfit7 Limited	9/9 (100.0%)
Usercentrics	15/16 (93.75%)
Google LLC	323/517 (62.48%)
Didomi	4/7 (57.14%)
Onetrust LLC	1/2 (50.0%)
Data Unavailable	0/11 (0%)

Table 9: Violating apps per CMP in active stage

CMP	Violation %
Easybrain Ltd	14/14 (100.0%)
Outfit7 Limited	7/9 (77.78%)
Usercentrics	12/16 (75.0%)
Google LLC	303/517 (58.61%)
OneTrust LLC	1/2 (50.0%)
Didomi	3/7 (42.86%)
Data Unavailable	0/11 (0%)

practices across their different apps. The developer name and contact is provided on an app's webpage in the Play store.

The vast majority of developers either *always* provide apps sharing AAID without consent, *i.e.*, all their apps share AAID in either the **LI**- and **Ø**-approach (238 developers in the passive stage, 221 in the active stage), or *never*, *i.e.*, none of their app share AAID (131 in the passive stage, 146 in the active stage). Only a handful of developers have mixed results (12 in the passive stage and 14 in the active stage), see Tables 14 and 15. This result confirms that apps behave differently across developers, although the number of "rogue" developers is high, excluding the hypothesis of a few developers making up the majority of "bad" apps.

We also noted that *the two top rogue developers in the passive stage also happen to be CMPs* (EasyBrain Ltd and Outfit7 Limited, with EasyBrain Ltd also having a 100% rate in the active stage). Further examination into the proportion of apps sharing AAID without consent per CMP yields that these two CMPs were often used by apps sharing AAID without consent (see Tables 8 and 9).

Summary: In the *passive*-stage of traffic analysis, **66.2%** of analyzed apps share personal data when using the **Ø**-approach. During the *active*-stage of analysis, **55.3%** of apps also share personal data before the user confirms consent choices (*i.e.*, during banner display or navigation). Based on these observations, **the majority of the surveyed TCF-based Android apps do not respect users' banner choices at runtime and collect personal data regardless of users choices**. We also observe that games are the categories most impacted by potential violations, and that developers often tend to have homogenous practices amongst their apps (*i.e.*, either always or never sharing AAID without consent).

6 Discussion

In this section, we contextualize our findings within prior work and discuss the implications of our results. First, in Section 6.1, we situate our results in relation to existing research. We then connect our findings to our research questions in Sections 6.1.1 to 6.1.4. Alongside, we examine the legal implications of our results in light of the data protection requirements outlined in Section 2.1. We outline the limitations of our research in Section 6.2 and identify research avenues for future work in Section 6.3.

6.1 Contextualization and Implications

6.1.1 Growing prevalence of the TCF. Our results show that 12.85% of downloaded apps use the TCF. The most recent work on TCF-based Android apps – Koch et al. [64] – reported in 2023 that 6.6% of the apps in their dataset implemented the TCF. This already reflected a substantial rise compared to Altpeter's [2] findings, who found only 1.9% of apps in 2022. Our findings of 12.85% indicates that TCF adoption *in Android apps has grown by a factor of 1.95 over the past two years* compared to previous work, although part of this increase may be attributable to improved technical detection. Such rapid growth makes it even more important that a standard as widely deployed as the TCF provides reliable legal compliance.

6.1.2 Not all apps correctly store user's consent banner choices. We found 15 apps that only store user' banner choices when the user gave consent to all data processing. When the user withheld consent for one or more purposes, the consent banner would reappear upon every subsequent launch of the app. Because the user's choice is never registered (as demanded by the accountability principle under Article 7(1) of the GDPR), repeated prompts can pressure users to accept out of fatigue, potentially influencing their choices and bringing into question the freedom of consent expressed [19], which ultimately may infringe a *freely given consent* and thus the *Lawfulness principle* (P1), the *correct consent registration* requirements (LR1), and the principle of Data Protection by Design (P5). To this scope, such *nagging* practices, commonly identified as a dark pattern, appear closely tied to incorrect registration of consent banner choices [89].

Another related practice to "incorrect consent registration" that occurred during dynamic analysis was inconsistent registration of banner choices across apps using the same CMP. Indeed, different apps implementing banners from the same CMP stored user's choices regarding legitimate interest differently, despite the user having clicked a visually identical "disagree to all" button in each case. Besides increasing the effort required for our analysis (we had to manually opt out of every individual purpose for the **Ø**-approach), this inconsistency arguably deceives user. Users may reasonably expect that a "disagree to all" actually applies to all processing purposes, not only those requiring consent. When this expectation is not met, a discrepancy arises between the user's understanding and the actual legal effect of their choice. Such practices may conflict with the *Fairness principle* (P2) [37, para 9]. Consent interfaces must not mislead users about the effect of their choices. A "disagree to all" button that only applies to a subset of purposes, without clearly indicating this limitation, can create a mismatch with users' reasonable expectations and the actual processing that follows.

6.1.3 TCF-based apps share AAID without consent at scale. Even when users rejected consent, at least 64.3% of the analyzed apps

transmitted AAID (**Ø**-approach, in the active stage). IAB Europe previously stated that online identifiers, such as IP addresses and AAID, constitute personal data under the GDPR [55]. Google's ad service, AdMob, declares that *it is necessary to obtain consent from users in the EEA to use personal data, such as AAID* [45]. Android documentation further describes the AAID as the recommended identifier for building profiles of users and enabling tracking. The same documentation also mentions that if the user opts out of personalization using AAID – in their Android device's settings –, AAID will be removed and made unidentifiable [4]. This implies that AAID is intended specifically for advertising-related tracking and personalization purposes. Given that consent is the legal ground for targeted advertising (see Section 2.1), and that AAID is a dedicated targeted advertising identifier, *data controllers are required to obtain consent before collecting it – a position consistently reflected by stakeholders, including IAB, Google, and DPAs such as the CNIL [19].* Yet, almost 2/3 of TCF-based apps in our dataset shared AAID without consent, thereby questioning the legitimacy of the TCF to facilitate legal compliance. Our results, from both the *passive* and *active* stages of traffic analysis, show that **when TCF-based apps share users' personal data, they will in a majority of cases do so regardless of the users' banner choices**. The only workaround for users who do not want to share their data with apps would be to manually remove their AAID in their Android device's settings, as mentioned by Android's developers documentation [4]. This solution however relies on an opt-out solution, and therefore does not meet the *Data Protection by Default principle* (P4), as it shifts the responsibility for preventing data sharing onto users rather than enforcing it by default at the application level.

6.1.4 Game apps are the top violators. Our analysis reveals that game apps constitute the primary sources of GDPR violations. As demonstrated in Section 5.3.4, we found that game-related apps transmit AAID to third-parties prior to obtaining valid user consent. This behavior shows systemic disregard for the *prior consent requirement*, thereby invalidating the legal basis for processing and directly infringing the GDPR's *Lawfulness* (P1) principle. The implications of this practice are amplified by the demographic composition of the affected user base. Recent industry data [70] indicates that 48% of mobile gamers (worldwide) are aged between 18–34, while minors aged 13-17 account for an additional 16% of the mobile gaming user base. These results are in line with a 2024 survey by the Oxcom (the UK Office of Communications), which states that 52% of 16-24 years old play on mobile, and 49% of 25-34 y.o. [83, p.327]. Consequently, users, including children, are subjected to tracking before having any opportunity to make a meaningful choice, raising heightened concerns regarding fairness and their vulnerability. Children's vulnerability in online gaming is currently under scrutiny, with the Irish's Garda National Cyber Crime Bureau warning that children are being "exploited on online gaming platforms at an *alarming scale*" [88]. BEUC (the European Consumer Organisation) already denounced in 2024 that children are "are even more vulnerable to [...] manipulative tactics" [11]. These findings are particularly timely in light of the EU's forthcoming Digital Fairness Act (DFA), currently in draft form, which aims to curtail harmful practices in gaming ecosystems [21].

6.1.5 Google dominance. The significant imbalance in CMP distribution observed — with Google LLC acting as the CMP for 89.76% of all TCF-based apps in our dataset (see Table 3) — raises concerns about *platform gatekeeper power* within the Android ecosystem. Google simultaneously owns Android (the Operating System), the Play Store (the distribution channel to download apps for most end-users), it is the biggest CMP for TCF-based apps by large (89.76%), and amongst the top data broker for mobile advertising receiving personal data in our analysis (number 5, see Section 5.3.3). Google is even pushing further its dominant position by requiring Android developers to register centrally [5], a move which triggered reactions from small players also distributing apps on Android, such as F-droid,[17] before backing down [3]. This concentration allows Google to shape how consent is obtained and to influence which forms of data collection are facilitated or constrained at scale. For instance, Google claims that "[publishers] are responsible to obtain users consent on [their] website or app or any data [they] upload to Google." [43]. However, its Android 'consent mode' [74] documentation – intended to guide developers in configuring SDK behavior based on a user's consent status – provides a revealing example: it suggests setting all 'consent default states' to "true", including those related to ad personalization signals [44]. In effect, research shows that developers tend to rely on default CMP configurations [94, 96]. *Observed violations therefore likely result from both developer choices and platform-level design.* As a result, the compliance issues identified in Section 5 cannot be attributed solely to individual app publishers: they may be structurally amplified by Google, as a platform gatekeeping actor [79] that sets the technical environment, provides the consent mechanism, and participates as a major data recipient. This suggests that effective regulatory oversight must also consider the responsibilities of dominant platform providers, and not limit accountability to app-level practices. Google leverages control of a core platform component to reinforce its position in the advertising and tracking ecosystem, and dominates the browser market (Chrome). These behaviors may therefore reflect structural properties of an ecosystem organized around Google's vertically integrated interests.

6.1.6 Google structurally accommodates potential legal violations as a CMP. Each purpose for processing personal data can rely on only one lawful basis. Because Google's CMP solicits consent as the chosen legal basis, this decision effectively precludes reliance on any other lawful basis. In other words, the app developer is prevented from invoking other legal grounds under Article 6(1) of the GDPR [36, para 10][81] – such as legitimate interest – as illustrated in Figure 2b. This choice directly implicates the *Lawfulness principle* (P1), as it constrains the controller's ability to determine and rely upon an appropriate legal basis for processing. Moreover, according to the European Data Protection Board (EDPB) [28, para 121-123], a data controller must disclose the applicable legal basis prior to data collection, and in direct relation to each specific purpose. This entails that if an app publisher claims to rely on consent for the processing while, in practice, another lawful basis is used,

[17] "In addition to demanding payment of a registration fee and agreement to their (non-negotiable and ever-changing) terms and conditions, Google will also require the uploading of personally identifying documents, including government ID, by the authors of the software[...]" [38].

this constitutes a fundamentally unfair practice toward data subjects. Consequently, the publisher cannot switch from consent to another legal basis, such as legitimate interest [77]. As explained in Section 2.1, advertising and related ad measurement purposes require consent. Attempting to rely on legitimate interest for advertising purposes risks violating the *Lawfulness principle* (P1) [67]. Empirical evidence from user studies further supports this interpretation. Several studies show that users are uncomfortable with the sharing of their data for the purposes of "personalized ad delivery and measurement" and "personalized content delivery and measurement" [17, 66, 67]. Furthermore, users disapprove of websites that list multiple advertising purposes under the legal basis of legitimate interest, a practice that is not compliant with data protection law [23, para 118][68]. Given that Google's CMP relies on legitimate interest in some contexts while simultaneously defaulting consent to "accept" for ad-related purposes, it is arguable that Google's CMP may process personal data for its own purposes. Under such circumstances, Google's role could be interpreted as that of a joint controller alongside app developers, thereby requiring it to comply with the full set of GDPR obligations. The rate of potential violations observed in other CMPs (Easybrain Ltd and Outfit7 Limited, 100% of apps caught sharing AAID without consent in both stages of our analysis, see Section 5.3.5) also supports the consideration of a *more careful examination of the role of CMPs in mobile contexts*.

6.1.7 Bad defaults used by the CMP Google LLC. As exemplified in Figure 2 of Section 4.2.2, the purpose of *measuring advertising performance* shows the legal basis of consent deselected and legitimate interest selected for 45 vendors. In practice, all banners in our dataset provided by CMP 300 (Google) preselected all legitimate interest purposes for all vendors. When data settings are preselected, users are subject to a specific data protection level, determined by the provider by default, rather than by users. The "salient field" of the consent banner provides the most important information to aid the user's decision. Making some buttons more salient is an example of design outcomes that are intended to surreptitiously nudge users by making a pre-chosen and intended choice more salient [41, pp. 19-20]. As the most data invasive option is enabled by default, this constitutes the dark pattern of *preselection or bad defaults* [37, 47]. Bad defaults subvert user's reasonable expectation that default settings will be in their best interest, instead requiring users to take active steps to change settings that may cause harm or unintentional disclosure of personal data [48]. The practice of preselection is prohibited by the Court of Justice of the EU [82, para 57, 63], and by the EDPB [37, para 54]. Such practices may also violate the *Data Protection by Default principle* (P4), as they shift the burden of privacy protection from the controller to the user.

6.1.8 Potential US personal data transfers without required safeguards. The results show in Section 5.1.2 that 82.14% of TCF-based apps are developed outside the EU/EEA. Because the GDPR applies extraterritorially to actors processing personal data of EU users (Article 3), these app publishers are still subject to its requirements. Moreover, when personal data is transmitted to a third-country, the GDPR's international data transfer rules are triggered. Apps send personal data to ad-tech servers that belong to companies headquartered in the US (see Section 5.3.3). While we cannot conclusively determine the physical location of the servers involved – given the well-known difficulty of geolocating infrastructure behind domains [69] and the widespread use of Content Delivery Networks (CDNs) –, we cannot exclude the possibility that personal data is transferred to the US. This uncertainty is further compounded by the possibility of subsequent ex-post transfers for processing. Under EU data protection law, transfers of personal data to the US are restricted due to the risk of US intelligence access. EU-US data transfers require explicit consent, contractual, organizational, and technical measures to prevent access by US intelligence services. Consequently, the transmission of unique identifiers and IP addresses to US-based entities may raise compliance concerns where no valid transfer mechanism or adequate safeguards are in place. In such circumstances, the level of protection required under Article 44 GDPR may be undermined, potentially implicating the *Lawfulness* (P1) and *Security* (P6) principles.

6.2 Limitations

6.2.1 Dataset limitations. Our dataset comprises several limitations, our results should therefore be interpreted in this light. First, we limited our collection to top apps per category, which excluded less popular apps. Second, 585 (11.5%) of apps failed to download for various reasons (such as the detection of an emulated device, see Section 5.1). Third, we only studied a subset of the CMPs available on mobile. The TCF lists 50 different CMPs on mobile (exclusive, and combined web/mobile) at the time of this study [52], these CMPs provide visually different banners and therefore require different heuristics to interact with. We captured 12 different CMPs amongst apps initializing the framework, and we interacted with six out of the 12. Each of the six CMPs we did not interact with either only appeared once in unique apps (5/6), or had a unique design in each app (1/6), we therefore discarded their analysis (only 1.90% of apps were discarded for this reason in this step of the analysis). Our data analysis is therefore biased towards apps relying on standardized CMPs, and the potential violations detected may not be fully representative of the broader Android ecosystem.

6.2.2 Capturing transformed data. Although we filtered a range of personal data (see Section 4.3.2), our analysis does not account for *transformed data*, *i.e.*, hashed (SHA) or encoded (Base64) data. A manual investigation into an arbitrary sample of decrypted packets did not reveal transformed data, we thus proceeded by not performing additional analysis. However, we acknowledge that an extended analysis may have captured other types of personal data. Since, the list of data considered is static and relatively small, a precomputation of the hashes and encodings can bring the evaluation to a reasonable cost.

6.2.3 Network traffic on emulated devices. The reliance on emulated devices, instead of physical devices [64, 80], may have altered the network behavior of analyzed apps. This design choice however enabled us to streamline the analysis (see Section 4.3.3), and we contend that the risk of having our results compromised is limited. To the best of our knowledge, a systematic comparison between traffic generated by physical and emulated devices has not yet been reported. However, emulators are commonly adopted in prior traffic analysis studies as a practical, reproducible, and accepted experimental platform. Surveys and papers on mobile traffic analysis and

tracking do not mention it as a limitation [12, 13, 62]. Although Pegioudis et al. [84] warn that it could alter behavior in other contexts (mobile browser traffic) since websites could detect such a "non-realistic" visit, we argue that our technical setting is incomparable: websites are third-parties, while apps are first-parties in our context. In a widely cited survey on mobile network traffic analysis, Conti et al. [22] actually present emulated devices are a valid alternative to palliate the difficulty of automating tests: "it constitutes an ideal point of capturing for mobile traffic. This approach is particularly useful if the focus of the analysis is on the network traffic of a specific mobile app".

6.2.4 Analyzing other operating Systems. The methodology used in this paper is dependent on adb which is unique for Android devices, making extensions of our methodology to other operating systems complicated. Furthermore, iOS apps ask for users' permission to use advertising IDs [65] (opt-in basis, unlike AAID), making it less likely for apps to transmit user data unknowingly [9]. Note also that Android is the most widely used operating system [93]. Lastly, only focusing on Android allows for a more in-depth analysis. Indeed, Apple prevents the rooting of its devices, making a MITM approach difficult, only leaving as a valid approach the tampering with a certificate to later decrypt the content of the network traffic. Recent work on iOS still relies on metadata analysis [78].

6.3 Future Work

6.3.1 Extending the dataset. Assessing the presence of the TCF on an app required downloading it, amounting to a significant overhead (87.15% of downloaded apps did not use the TCF). During interactions with consent banners, we noticed that many apps using the TCF were published by the same developers. In the Google Play Store, each application has a link to its developer,[18] meaning that, given an app, a simple heuristic consisting in scraping all apps from the same developer can rapidly expand our dataset of TCF-based apps. We tried this method on a set of 842 applications initializing the framework, and found 4741 apps initializing the TCF too, all published by developers using the TCF in other apps. This method can bootstrap the creation of a larger dataset, enabling further privacy analysis, with the downside of not providing further data on proportions of TCF usage in the Play Store, and possibly biasing the representativeness of results. Another possibility of extension is to use a different sampling method, by downloading not only top apps but also long tail apps with fewer downloads.

6.3.2 Further interaction with apps. Our traffic analysis was only conducted on apps while interacting with their consent banners, and then while idling afterward. Our automated interactions may therefore not have accurately captured realistic human-like interactions. This leaves most of the applications' functionalities untouched, potentially missing out sharing of personal data. Further interaction with apps and additional collection points may yield better insights into data collection in this context. For instance, data could be collected before any interaction, or after realistic simulation with an app's features. However, automating interactions with apps is challenging, since apps are unique. Additionally, how users interact with consent banners on mobile has only been little studied [61], which forces us to formulate hypotheses in the absence of literature on the topic (*i.e.*, that users behave similarly than with web consent banners [67]). A longitudinal study [100] with real participants over a longer period of time may address this challenge, and provide a different picture. The combination of realistic interactions and analysis of transformed data (see Section 6.2.2) frames an interesting yet challenging research avenue.

6.3.3 Comparing emulated and physical devices. Another promising research avenue is the comparison between emulated and physical devices. As discussed in Section 6.2.3, the use of emulators is considered standard practice for network traffic analysis. However, there is no strict guarantee that this aspect of our setup did not impact our results. Therefore, future work should encompass both emulated and physical devices to provide a clearer picture.

6.3.4 The state of affairs on iOS. As mentioned in Section 6.2.4, the present paper only focuses on the analysis of Android apps. Our results cover issues related to Google/Alphabet's dominant position (as owner of the platform distributing apps, the OS, main CMP, and data broker), which visibly allows legal violations at scale. While the main mobile OS provider, Apple, historically relied on its image as a privacy-conscious company [98, 101], a claim not always met in reality [87]. A natural and promising research avenue therefore is the study of the TCF on iOS, to systematically assess whether apps distributed through the App Store (Apple's equivalent of the Play Store) genuinely respect users' consent choices.

7 Conclusion

This paper investigates the prevalence and the usage of the TCF in Android applications. To quantify the usage of the TCF in Android apps, we scraped and downloaded 4482 of the most popular apps in the Google Play Store. We found that **576 apps were identified as implementing the TCF, representing 12.85%** of the downloaded apps. This indicates a significant increase in usage of the framework compared to the closest related work [2, 64]. The TCF can be found in apps of all categories, developed in various countries including outside the EU/EEA, with Google being by far the main CMP in our dataset (89.76%). We automatically interacted with consent banners of 576 applications and confirmed their stored banner choices. As a result, we found that **15 applications only stored our choices if provided with consent to all data processing**, suggesting that certain TCF-based apps do not respect users' banner choices. We analyzed network traffic in two stages: passive (post-choices) and active (during interaction with the banner/before choices were enacted). Our results show that **66.2% of applications transmitted AAID**, a unique identifier dedicated to targeted advertising, when disagreeing to all in the **passive**-stage. While **55.3% of apps also transmitted AAID while we were interacting with the apps' banners** (before choices were made) during the **active**-stage of our analysis. Games are the top app categories sharing AAID without consent. We conclude that the TCF fails to facilitate legal compliance at scale on Android apps. Although IAB Europe announced in June 2025 a new minor version of the TCF (v.2.3) [57] (see Section 2.3), it is unlikely that the modifications will address the issues identified in this paper [95].

[18] The Play Store refers to the developer, although the legal responsibility is first on the publisher [19].

Acknowledgments

This work was partially supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation, and by the Utrecht Centre for Regulation and Enforcement in Europe (RENFORCE). The authors would like to thank the reviewers for helping us improve this paper.

References

[1] 2025. Android-TCF-Analysis-Data. https://github.com/carlssonp/Android-TCF-Analysis-Data/ Accessed: 2025-11-18.
[2] Benjamin Altpeter. 2022. *Informed consent? A study of "consent dialogs" on android and iOS.* Master's thesis. Technische Universität Braunschweig.
[3] Android. 2025. *Android developer verification: Early access starts now as we continue to build with your feedback.* https://android-developers.googleblog.com/2025/11/android-developer-verification-early.html Accessed: 2025-11-12.
[4] Android. 2025. Best practices for unique identifiers. https://developer.android.com/identity/user-data-ids#ads Accessed: 2025-05-05.
[5] Android. 2025. *A new layer of security for certified Android devices.* https://android-developers.googleblog.com/2025/08/elevating-android-security.html Accessed: 2025-11-06.
[6] Android. 2025. Snapshots. https://developer.android.com/studio/run/emulator-snapshots Accessed: 2025-05-13.
[7] AnyRun. 2025-11-25. *Malware analysis rayjump.com Malicious activity | ANY.RUN - Malware Sandbox Online.* https://report.any.run/2926f23016bf3629a270a25d870d7e8a59385a9841820864a71753cc6769fa3d/12fce59d-4814-49d5-998a-a3701608c5a0 Accessed: 2025-11-25.
[8] AP News. 2025-09-04. *Google facing $425.7 million in damages for nearly a decade of improper smartphone snooping.* https://apnews.com/article/google-smartphone-surveillance-verdict-damages-c93e0150089fd47ec396f1d0abacb4a8 Accessed: 2025-11-17.
[9] Apple. 2025. User privacy and data use. https://developer.apple.com/app-store/user-privacy-and-data-use/ Accessed: 2025-07-14.
[10] Article 29 Data Protection Working Party. 2010. *Opinion 2/2010 on Online Behavioural Advertising.* Technical Report WP171. European Commission. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf Adopted on 22 June 2010..
[11] BEUC. 2024-09-12. *Consumer groups denounce video games' manipulative spending tactics.* https://www.beuc.eu/press-releases/consumer-groups-denounce-video-games-manipulative-spending-tactics Accessed: 2025-11-25.
[12] Reuben Binns. 2022. Tracking on the Web, Mobile and the Internet of Things. In *Foundations and Trends® in Web Science.*
[13] Reuben Binns, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. 2018-11-30. Measuring Third-party Tracker Power across Web and Mobile. In *ACM Transactions on Internet Technology.*
[14] Dino Bollinger, Karel Kubicek, Carlos Cotrini, and David Basin. 2022. Automating cookie consent and GDPR violation detection. In *31st USENIX Security Symposium (USENIX Security 22).*
[15] Amber Case. 2019-09-17. *The Appification of Everything & Why it Needs to End.* https://caseorganic.medium.com/the-appification-of-everything-why-it-needs-to-end-8a2214c1968f Accessed: 2025-11-17.
[16] Belgian Data Protection Authority (Litigation Chamber). 2022. Decision on the merits 21/2022 of 2 February 2022: Complaint relating to Transparency & Consent Framework (DOS-2019-01377). https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-en.pdf. Case No. DOS-2019-01377; decision of 2 February 2022.
[17] Farah Chanchary and Sonia Chiasson. 2015. User perceptions of sharing, advertising, and tracking. In *Proceedings of the Eleventh Symposium On Usable Privacy and Security (SOUPS 2015).* Ottawa, Canada.
[18] Cloudflare. 2025. What is robots.txt? | How a robots.txt file works. https://www.cloudflare.com/learning/bots/what-is-robots-txt/ Accessed: 2025-05-12.
[19] CNIL. 2025-08-04. Recommendation on mobile applications. https://www.cnil.fr/sites/cnil/files/2025-05/recommendation-mobiles-app.pdf
[20] EU Commission. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679.
[21] European Commission. 2025. Questions and Answers on the Digital Fairness Act. https://ec.europa.eu/commission/presscorner/detail/en/qanda_24_4909 Press corner Q&A on the Digital Fairness Act, accessed 2025-09-09.
[22] Mauro Conti, Qian Qian Li, Alberto Maragno, and Riccardo Spolaor. 2018. The dark side (-channel) of mobile devices: A survey on network traffic analysis. In *IEEE communications surveys & tutorials.*
[23] Court of Justice of the European Union. 2023. Judgment of the Court (Grand Chamber) of 4 July 2023, Case C-252/21, Meta Platforms Inc. and Others v. Bundeskartellamt. ECLI:EU:C:2023:537. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0252
[24] Court of Justice of the European Union. 2023. Judgment of the Court (Grand Chamber) of 4 July 2023, Meta Platforms Inc. and Others v Bundeskartellamt, Case C-252/21. https://curia.europa.eu/juris/document/document.jsf?text=&docid=275530&doclang=EN. Case C-252/21, concerning the interpretation of the GDPR in the context of competition law enforcement by the Bundeskartellamt..
[25] Court of Justice of the European Union. 2024. Judgment of the Court (Fourth Chamber) in Case C-604/22: IAB Europe v. Gegevensbeschermingsautoriteit (Transparency and Consent Framework). https://curia.europa.eu/juris/document/document.jsf?text=&docid=284330&pageIndex=0&doclang=EN Case concerning the qualification of the TC String as personal data and IAB Europe's role as joint controller under the GDPR..
[26] First Chamber Court of Justice of the European Union. 2025-09-04. European Data Protection Supervisor (EDPS) v. Single Resolution Board (SRB). https://curia.europa.eu/juris/document/document.jsf?docid=303863&doclang=EN
[27] Developers Google. 2025. Fused Location Provider API. https://developers.google.com/location-context/fused-location-provider Accessed: 2025-05-22.
[28] EDPB. 2020. *Guidelines on Consent under Regulation 2016/679.* Technical Report.
[29] European Data Protection Board (EDPB). 2012. Opinion 04/2012 on Cookie Consent Exemption (WP 194).
[30] European Data Protection Board (EDPB). 2013. Opinion 03/2013 on purpose limitation (WP 203). Available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.
[31] European Data Protection Board (EDPB). 2013. Working Document 02/2013 providing guidance on obtaining consent for cookies, adopted on 2 October 2013. Available at https://www.pdpjournals.com/docs/88135.pdf.
[32] ePD-09 2009. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136, accessed on 2019.10.31.
[33] EU commission. 2025-11-21. *Data protection adequacy for non-EU countries.* https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en Accessed: 2025-11-21.
[34] European Data Protection Board. 2007. Opinion 4/2007 on the concept of personal data (WP 136), adopted on 20.06.2007. https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2007/wp136_en.pdf.
[35] European Data Protection Board. 2020. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf. Version 2.0, adopted on 20 October 2020.
[36] European Data Protection Board. 2024. Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR. https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf. Version 1.0, adopted on 8 October 2024.
[37] European Data Protection Board (EDPB). 2023. *Guidelines 03/2022 on Dark Patterns in Social Media Platform Interfaces: How to Recognise and Avoid Them.* Technical Report. European Data Protection Board. https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf Adopted 14 February 2023, Version 2.0.
[38] F-Droid. 2025. *F-Droid and Google Developer Registration Decree.* https://f-droid.org/2025/09/29/google-developer-registration-decree.html Accessed: 2025-11-06.
[39] Imane Fouad, Cristiana Santos, Feras Al Kassar, Nataliia Bielova, and Stefano Calzavara. 2020. On Compliance of Cookie Purposes with the Purpose Specification Principle. In *Proc. International Workshop on Privacy Engineering (IWPE).*
[40] Frida. 2025. Dynamic instrumentation toolkit for developers, reverse-engineers, and security researchers. https://frida.re/ Accessed: 2025-03-14.
[41] Frobrukerrådet (Norwegian Consumer Council). 2018. Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy. https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design
[42] Google. 2025. *Target mobile apps with IDFA or AAID - Authorized Buyers Help.* https://support.google.com/authorizedbuyers/answer/3221407 Accessed: 2025-11-06.
[43] Google. 2025-11-24. *Consent mode overview | Tag Platform.* https://developers.google.com/tag-platform/security/concepts/consent-mode Accessed: 2025-11-24.
[44] Google. 2025-11-24. *Set up consent mode for apps | Tag Platform.* https://developers.google.com/tag-platform/security/guides/app-consent Accessed: 2025-11-24.
[45] Google AdMob. 2025. GDPR IAB support. https://developers.google.com/admob/android/privacy/gdpr Accessed: 2025-05-05.

[46] Google Play. 2025. Google Play robot.txt. https://play.google.com/robots.txt Accessed: 2025-03-13.

[47] Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, and Damian Clifford. 2021. Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*.

[48] Colin M. Gray, Cristiana Teixeira Santos, Nataliia Bielova, and Thomas Mildner. 2024. An Ontology of Dark Patterns Knowledge: Foundations, Definitions, and a Pathway for Shared Knowledge-Building. In *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)*.

[49] IAB Europe. 2024. Consent Management Platform API. https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20CMP%20API%20v2.md Accessed: 2024-11-29.

[50] IAB Europe. 2024. Transparency & Consent Framework. https://iabeurope.eu/transparency-consent-framework/ Accessed: 2024-11-23.

[51] IAB Europe. 2024. Understanding the Transparency & Consent Framework v2.2 . https://iabeurope.eu/understanding-the-upcoming-transparency-consent-framework-v2-2/ Accessed: 2024-11-28.

[52] IAB Europe. 2025. CMP List. https://iabeurope.eu/cmp-list/ Accessed: 2025-04-30.

[53] IAB Europe. 2025. IAB Europe Transparency & Consent Framework Policies. https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/ Accessed: 2025-03-17.

[54] IAB Europe. 2025. TCF for Vendors. https://iabeurope.eu/tcf-for-vendors/ Accessed: 2025-01-31.

[55] IAB Europe. 2025. THE DEFINITION OF PERSONAL DATA. https://iabeurope.eu/wp-content/uploads/20180718_IABEU-GIG-Working-Paper02_Personal-Data_v1.1.pdf Accessed: 2025-05-05.

[56] IAB Europe. 2025. Transparency and Consent String with Global Vendor & CMP List Formats. https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20Consent%20string%20and%20vendor%20list%20formats%20v2.md#how-should-a-transparency--consent-string-be-store Accessed: 2025-02-12.

[57] IAB Europe. 2025-11-24. *The release of TCF v.2.3 - Mandatory 'Disclosed Vendors' Section + Update Contact Info Reminder.* https://iabeurope.eu/wp-content/uploads/TCF_V-CMP_comms_TheReleaseOfTCFv.2.3-Mandatory%E2%80%98DisclosedVendorsSectionUpdateContactInfo-Reminder_190625_IABEurope.pdf Accessed: 2025-11-24.

[58] IAB Europe. 2025-12. *All You Need to Know About the Transition to TCF v2.3.* https://iabeurope.eu/all-you-need-to-know-about-the-transition-to-tcf-v2-3/ Accessed: 2026-02-05.

[59] IAB Europe GDPR Implementation Working Group. 2018-07-18. THE DEFINITION OF PERSONAL DATA Working Paper 02/2017. https://iabeurope.eu/wp-content/uploads/20180718_IABEU-GIG-Working-Paper02_Personal-Data_v1.1.pdf Accessed: 2025-11-06.

[60] Irish Data Protection Commission. 2025. Guidance note on cookies and other tracking technologies. https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf

[61] Nikhil Jha, Martino Trevisan, Marco Mellia, Rodrigo Irarrazaval, and Daniel Fernandez. 2023. I Refuse if You Let Me: Studying User Behavior with Privacy Banners at Scale. In *2023 7th Network Traffic Measurement and Analysis Conference (TMA)*. ieee.

[62] Haojian Jin, Minyi Liu, Kevan Dodhia, Yuanchun Li, Gaurav Srivastava, Matthew Fredrikson, Yuvraj Agarwal, and Jason I Hong. 2018. Why are they collecting my data? inferring the purposes of network traffic in mobile apps. In *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*.

[63] Gayatri Priyadarsini Kancherla, Nataliia Bielova, Cristiana Santos, and Abhishek Bichhawat. 2025. Johnny can't revoke consent either: measuring compliance of consent revocation on the web. In *Proceedings on Privacy Enhancing Technologies (PoPETS)*.

[64] Simon Koch, Benjamin Altpeter, and Martin Johns. 2023. The OK is not enough: A large scale study of consent dialogs in smartphone applications. In *32nd USENIX Security Symposium (USENIX Security 23)*.

[65] Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns, and Nigel Shadbolt. 2022-06-21. Goodbye Tracking? Impact of iOS App Tracking Transparency and Privacy Labels. In *2022 ACM Conference on Fairness Accountability and Transparency*.

[66] Anastasia Kozyreva, Philipp Lorenz-Spreen, Ralph Hertwig, Stephan Lewandowsky, and Stefan M. Herzog. 2021. Public attitudes towards algorithmic personalization and use of personal data online: Evidence from Germany, Great Britain, and the United States. In *Humanities and Social Sciences Communications*.

[67] Lin Kyi, Sushil Ammanaghatta Shivakumar, Cristiana Teixeira Santos, Franziska Roesner, Frederike Zufall, and Asia J Biega. 2023. Investigating deceptive design in GDPR's legitimate interest. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI '23)*.

[68] Lin Kyi, Abraham Mhaidli, Cristiana Santos, Franziska Roesner, and Asia J. Biega. 2024. "It doesn't tell me anything about how my data is used": User Perceptions of Data Collection Purposes. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems (CHI '24)*.

[69] Augustin Laouar, Loïc Desgeorges, Paul Schmitt, and Franceso Bronzino. 2025. Rethinking Geolocalization on the Internet. In *Proceedings of the 24th ACM Workshop on Hot Topics in Networks*.

[70] Robert A. Lee. 2025-06-05. *Mobile Games Statistics 2025: Demographics, Monetization, and Market Leaders.* https://sqmagazine.co.uk/mobile-games-statistics/ Accessed: 2025-11-24.

[71] Magisk. 2025. Magisk Module. https://magiskmodule.gitlab.io/ Accessed: 2025-03-14.

[72] Célestin Matte, Nataliia Bielova, and Cristiana Santos. 2020. Do cookie banners respect my choice?: Measuring legal compliance of banners from iab europe's transparency and consent framework. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE.

[73] Célestin Matte, Cristiana Santos, and Nataliia Bielova. 2020. Purposes in IAB Europe's TCF: Which Legal Basis and How Are They Used by Advertisers?. In *Privacy Technologies and Policy (APF 2020)*.

[74] Gilles Mertens, Nataliia Bielova, Vincent Roca, and Cristiana Santos. 2025. You Can't Trust Your Tag Neither: Privacy Leaks and Potential Legal Violations within the Google Tag Manager. In *EuroS&P 2025-10th IEEE European Symposium on Security and Privacy*.

[75] Tomas Meskauskas. 2024-11-30. *Rayjump.com POP-UP Redirect.* https://www.pcrisk.com/removal-guides/13432-rayjump-com-pop-up-redirect

[76] mitmproxy. 2025. About Certificates. https://docs.mitmproxy.org/stable/concepts-certificates/ Accessed: 2025-03-14.

[77] Victor Morel, Cristiana Santos, Viktor Fredholm, and Adam Thunberg. 2023. Legitimate Interest is the New Consent-Large-Scale Measurement and Legal Compliance of IAB Europe TCF Paywalls. In *Proceedings of the 22nd Workshop on Privacy in the Electronic Society*.

[78] Zahra Moti, Tom Janssen-Groesbeek, Steven Monteiro, Andrea Continella, and Gunes Acar. 2025. WhisperTest: A Voice-Control-based Library for iOS UI Automation. In *Conference on Computer and Communications Security, CCS 2025*.

[79] Shaoor Munir, Konrad Kollnig, Anastasia Shuba, and Zubair Shafiq. 2025. Google's Chrome Antitrust Paradox. In *Vanderbilt Journal of Entertainment and Technology Law*.

[80] Trung Tin Nguyen, Michael Backes, Ninja Marnau, and Ben Stock. 2021. Share First, Ask Later (or Never?) Studying Violations of GDPR Explicit Consent in Android Apps. In *30th USENIX Security Symposium (USENIX Security 21)*.

[81] noyb. 2021. News Sites: Readers need to "buy back" their own data at an exorbitant price?! https://noyb.eu/en/news-sites-readers-need-buy-back-their-own-data-exorbitant-price

[82] Court of Justice of the European Union. 2019-10-01. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH. ECLI:EU:C:2019:801.

[83] Ofcom. 2024. OFCOM ADULT MEDIA LITERACY. https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/data/statistics/2025/adults-media-literacy-tracker/adults-media-literacy-core-survey-2024-data-tables.pdf?v=389036 Accessed: 2025-11-25.

[84] John Pegioudis, Emmanouil Papadogiannakis, Nicolas Kourtellis, Evangelos P. Markatos, and Panagiotis Papadopoulos. 2023-10-24. Not only E.T. Phones Home: Analysing the Native User Tracking of Mobile Browsers. In *Proceedings of the 2023 ACM on Internet Measurement Conference*.

[85] Nils Reimers and Iryna Gurevych. 2019. Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks. In *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing*.

[86] Nils Reimers and Iryna Gurevych. 2025. sentence-transformers/paraphrase-multilingual-MiniLM-L12-v2. https://huggingface.co/sentence-transformers/paraphrase-multilingual-MiniLM-L12-v2 Accessed: 2025-04-23.

[87] Moin Roberts-Islam. 2025-03-01. *Siri Privacy Breach: Apple To Pay $95 Million Settlement Amid Spying Claims.* https://www.forbes.com/sites/moinroberts-islam/2025/01/03/siri-privacy-breach-apple-to-pay-95m-settlement-amid-spying-claims/ Accessed: 2025-11-18.

[88] RTE. 2025-11-27. *Senior garda warns of 'alarming' scale of child grooming in games.* https://amp.rte.ie/amp/1546044/ Accessed: 2025-11-28.

[89] Cristiana Santos, Nataliia Bielova, and Célestin Matte. 2020. Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. In *Technology and Regulation (TechReg)*.

[90] Cristiana Santos, Arianna Rossi, Lorena Sanchez Chamorro, Kerstin Bongard-Blanchy, and Ruba Abu-Salma. 2021. Cookie Banners, What's the Purpose? Analyzing Cookie Banner Text Through a Legal Lens. In *Proceedings of the 20th Workshop on Privacy in the Electronic Society*.

[91] similarweb. 2025. Mobile vs. Desktop vs. Tablet Traffic Market Share. https://www.similarweb.com/platforms/ Accessed: 2025-02-11.

[92] Michael Smith, Antonio Torres-Agüero, Riley Grossman, Pritam Sen, Yi Chen, and Cristian Borcea. 2024. A study of GDPR compliance under the transparency and consent framework. In *Proceedings of the ACM Web Conference 2024*.
[93] Statcounter. 2025. Mobile Operating System Market Share Worldwide. https://gs.statcounter.com/os-market-share#monthly-202001-202501/ Accessed: 2025-02-11.
[94] Michael Tóth, Nataliia Bielova, and Vincent Roca. 2022. On Dark Patterns and Manipulation of Website Publishers by CMPs. In *Proceedings on Privacy Enhancing Technologies (PoPETS)*.
[95] Usercentrics. 2025-11-24. *IAB TCF 2.2: IAB Transparency and Consent Framework Guide*. https://usercentrics.com/knowledge-hub/iab-tcf-2-3-transparency-and-consent-framework-quick-guide/ Accessed: 2025-11-24.
[96] Christine Utz, Sabrina Amft, Martin Degeling, Thorsten Holz, Sascha Fahl, and Florian Schaub. 2023. Privacy Rarely Considered: Exploring Considerations in the Adoption of Third-Party Services by Websites. In *Proceedings on Privacy Enhancing Technologies (PoPETS)*.
[97] Michael Veale, Maarten Nouwens, and Cristina Santos. 2022. Impossible Asks: Can the Transparency and Consent Framework Ever Authorise Real-Time Bidding After the Belgian DPA Decision?. In *Technology and Regulation*.
[98] James Vincent. 2016-06-13. *Apple promises to deliver AI smarts without sacrificing your privacy*. https://www.theverge.com/2016/6/13/11924080/apple-ai-on-device-privacy-wwdc-2016 Accessed: 2025-11-18.
[99] Heidi Waem, Verena Grentzenberg, and Luca Sawatzki. 2025-06-11. *EU: Brussels Court of Appeal rules on IAB Europe and the TC String – Implications for GDPR Compliance*. https://privacymatters.dlapiper.com/2025/06/eu-brussels-court-of-appeal-rules-on-iab-europe-and-the-tc-string-implications-for-gdpr-compliance/ Accessed: 2025-11-17.
[100] Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov. 2017. The feasibility of dynamically granted permissions: Aligning mobile privacy with user preferences. In *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE.
[101] Shoshana Zuboff. 2023. The age of surveillance capitalism. In *Social theory re-wired*. Routledge.

A Ethical Considerations

Our compliance assessment of TCF-based apps is constrained by the availability of apps in our dataset, which was shaped by ethical and technical boundaries. A critical consideration was adherence to the Play Store's `robots.txt` [46]. This file defines permissible and prohibited interactions for automated systems [18], ensuring respect for the platform's terms of use. Notably, the `robots.txt` restrictions explicitly prohibit non-human users, such as web scrapers, from utilizing the Play Store search bar. However, it permitted access to top apps by category, as this was not restricted. To maintain ethical compliance, we limited our dataset to apps accessible through these means, prioritizing respect for platform guidelines over broader data collection.

Prior to publication, we performed a responsible disclosure to developers of apps sharing AAID without consent. We also plan to share our results with the European Data Protection Board, data protection regulators, as well as with IAB Europe.

B Tables

Table 10: App categories from our dataset and their usage of the TCF

Category	Usage %
PERSONALIZATION	54/101 (53.47%)
LIBRARIES_AND_DEMO	26/76 (34.21%)
ART_AND_DESIGN	27/79 (34.18%)
VIDEO_PLAYERS	20/67 (29.85%)
TOOLS	26/90 (28.89%)
PHOTOGRAPHY	22/77 (28.57%)
MAPS_AND_NAVIGATION	22/86 (25.58%)
PRODUCTIVITY	16/67 (23.88%)
MUSIC_AND_AUDIO	20/85 (23.53%)
WEATHER	15/65 (23.08%)
FAMILY_EDUCATION	2/11 (18.18%)
GAME_BOARD	13/92 (14.13%)
COMMUNICATION	8/57 (14.04%)
GAME_WORD	13/93 (13.98%)
GAME_TRIVIA	9/66 (13.64%)
BEAUTY	7/52 (13.46%)
HEALTH_AND_FITNESS	12/91 (13.19%)
GAME_ARCADE	12/93 (12.9%)
EVENTS	11/86 (12.79%)
GAME_MUSIC	10/85 (11.76%)
GAME_PUZZLE	13/113 (11.5%)
PARENTING	7/62 (11.29%)
ENTERTAINMENT	8/75 (10.67%)
FAMILY	9/86 (10.47%)
GAME_SIMULATION	12/115 (10.43%)
GAME_SPORTS	11/107 (10.28%)
DATING	6/60 (10.0%)
NEWS_AND_MAGAZINES	6/61 (9.84%)
SOCIAL	7/80 (8.75%)
GAME_CARD	6/75 (8.0%)
HOUSE_AND_HOME	5/64 (7.81%)
BOOKS_AND_REFERENCE	6/77 (7.79%)
GAME_CASUAL	10/130 (7.69%)
GAME_RACING	8/105 (7.62%)
GAME_ADVENTURE	8/108 (7.41%)
GAME_ACTION	12/162 (7.41%)
GAME_ROLE_PLAYING	8/119 (6.72%)
GAME_EDUCATIONAL	10/156 (6.41%)
LIFESTYLE	5/80 (6.25%)
GAME_CASINO	4/66 (6.06%)
COMICS	3/53 (5.66%)
GAME	26/484 (5.37%)
FAMILY_CREATE	2/40 (5.0%)
SPORTS	5/100 (5.0%)
BUSINESS	4/82 (4.88%)
GAME_STRATEGY	4/98 (4.08%)
AUTO_AND_VEHICLES	2/51 (3.92%)

EDUCATION	3/82 (3.66%)
TRAVEL_AND_LOCAL	3/94 (3.19%)
MEDICAL	1/32 (3.12%)
APPLICATION	4/144 (2.78%)
FAMILY_MUSICVIDEO	1/44 (2.27%)
FOOD_AND_DRINK	1/74 (1.35%)
SHOPPING	0/62 (0%)
FAMILY_BRAINGAMES	0/66 (0%)
FINANCE	0/71 (0%)
FAMILY_PRETEND	0/16 (0%)
FAMILY_ACTION	0/54 (0%)
Data Unavailable	0/11 (0%)

Table 11: Distribution of countries where TCF-based apps in our dataset were developed

Country	**Apps using the TCF (N = 576)**
Vietnam	94 (16.32%)
Hong Kong	60 (10.42%)
Cyprus	41 (7.12%)
China	41 (7.12%)
Israel	36 (6.25%)
India	36 (6.25%)
App Removed	28 (4.86%)
United States	27 (4.69%)
Pakistan	22 (3.82%)
United Kingdom	17 (2.95%)
United Arab Emirates	15 (2.6%)
Sweden	14 (2.43%)
Morocco	14 (2.43%)
Data Unavailable	11 (1.91%)
Singapore	11 (1.91%)
South Korea	10 (1.74%)
Türkiye	10 (1.74%)
Spain	10 (1.74%)
Japan	9 (1.56%)
Andorra	5 (0.87%)
Poland	5 (0.87%)
Canada	5 (0.87%)
Germany	5 (0.87%)
Romania	4 (0.69%)
Moldova	4 (0.69%)
Serbia	3 (0.52%)
Brazil	3 (0.52%)
Hungary	3 (0.52%)
Portugal	3 (0.52%)
Italy	2 (0.35%)
Czechia	2 (0.35%)
Russia	2 (0.35%)
Mexico	2 (0.35%)
Cayman Islands	2 (0.35%)
British Virgin Islands	2 (0.35%)
Australia	2 (0.35%)
Lithuania	1 (0.17%)
Netherlands	1 (0.17%)
Malaysia	1 (0.17%)
France	1 (0.17%)
Estonia	1 (0.17%)
Ukraine	1 (0.17%)
Switzerland	1 (0.17%)
Malta	1 (0.17%)
Yemen	1 (0.17%)
Azerbaijan	1 (0.17%)
New Zealand	1 (0.17%)
Bangladesh	1 (0.17%)
Indonesia	1 (0.17%)
Marshall Islands	1 (0.17%)
Uruguay	1 (0.17%)
Norway	1 (0.17%)

Table 12: Apps incorrectly registering banner choices.

App names and packages
Sweet Beauty Camera Filter com.camera.sweet.beauty.fillter.cameraeditor
Geotag Photo: Camera Location com.cameratag.geotagphoto.gpscamera
Control Center Simple com.tools.control.center.simplecontrol
Draw Animation - Anim Creator com.banix.drawsketch.animationmaker
Silly Smiles Live Wallpaper 4K com.silly.smilewallpaper.sillywallpaper
AR Draw Sketch: Trace & Paint com.ardrawing.sketch.trace.paint.drawsketch.aipainting.paper
Easy Piano Keyboard - Piano88 com.banix.piano.learnpiano
Find Phone by Clap, Whistle com.bigsoft.clap.myphone
Caller ID Name, Location & SMS com.indiastudio.caller.truephone
Chat AI - AI Chatbot Friend com.antonio.chat.ai.free.artificial.intelligence
Dating - Chat & Meet Singles com.appgame.dating.app.free.chat.flirt.dating
Locate Mobile by Number com.appgame.phone.number.locator.by.number
Phone Tracker By Number com.antonio.family.locator.phone.tracker
Books - Read and Download com.appgame.free.books.read.free.books
PDF Viewer: PDF Fill & Sign com.fillpdf.pdfeditor.pdfsign

Table 13: The share of TCF-based applications in each category from our dataset (combined passive and active stages, on both LI- and Ø-approaches), that transmitted AAID

Category	Violation %
GAME_SIMULATION	12/12 (100.0%)
GAME_ARCADE	12/12 (100.0%)
GAME_SPORTS	11/11 (100.0%)
GAME_CASUAL	10/10 (100.0%)
GAME_CASINO	4/4 (100.0%)
EDUCATION	3/3 (100.0%)
AUTO_AND_VEHICLES	2/2 (100.0%)
GAME_BOARD	12/13 (92.31%)
GAME	23/26 (88.46%)
PRODUCTIVITY	14/16 (87.5%)
GAME_ADVENTURE	7/8 (87.5%)
GAME_ROLE_PLAYING	7/8 (87.5%)
ENTERTAINMENT	7/8 (87.5%)
MUSIC_AND_AUDIO	17/20 (85.0%)
GAME_PUZZLE	11/13 (84.62%)
GAME_WORD	11/13 (84.62%)
GAME_ACTION	10/12 (83.33%)
NEWS_AND_MAGAZINES	5/6 (83.33%)
DATING	5/6 (83.33%)
GAME_CARD	5/6 (83.33%)
GAME_MUSIC	8/10 (80.0%)
SPORTS	4/5 (80.0%)
HEALTH_AND_FITNESS	9/12 (75.0%)
GAME_RACING	6/8 (75.0%)
WEATHER	11/15 (73.33%)
TOOLS	19/26 (73.08%)
MAPS_AND_NAVIGATION	16/22 (72.73%)
SOCIAL	5/7 (71.43%)
ART_AND_DESIGN	19/27 (70.37%)
VIDEO_PLAYERS	14/20 (70.0%)
PHOTOGRAPHY	15/22 (68.18%)
GAME_TRIVIA	6/9 (66.67%)
BOOKS_AND_REFERENCE	4/6 (66.67%)
PERSONALIZATION	35/54 (64.81%)
LIFESTYLE	3/5 (60.0%)
APPLICATION	2/4 (50.0%)
HOUSE_AND_HOME	2/5 (40.0%)
COMMUNICATION	3/8 (37.5%)
EVENTS	4/11 (36.36%)
COMICS	1/3 (33.33%)
TRAVEL_AND_LOCAL	1/3 (33.33%)
LIBRARIES_AND_DEMO	8/26 (30.77%)
PARENTING	2/7 (28.57%)
BEAUTY	2/7 (28.57%)
GAME_STRATEGY	1/4 (25.0%)
GAME_EDUCATIONAL	1/10 (10.0%)
Data Unavailable	0/11 (0%)
FAMILY	0/9 (0%)
BUSINESS	0/4 (0%)
FAMILY_CREATE	0/2 (0%)
FAMILY_EDUCATION	0/2 (0%)
FAMILY_MUSICVIDEO	0/1 (0%)
FOOD_AND_DRINK	0/1 (0%)
MEDICAL	0/1 (0%)

Table 14: Developer passive stage data

Developer (name/email)	Violation %
Easybrain	14/14 (100.0%)
Outfit7 Limited	9/9 (100.0%)
BoomBit Games	7/7 (100.0%)
CrazyLabs LTD	5/5 (100.0%)
Battery Stats Saver	5/5 (100.0%)
gameone	4/4 (100.0%)
RobTop Games	4/4 (100.0%)
nguyenluan@lutech.ltd	4/4 (100.0%)
hoahuongduong170120@gmail.com	4/4 (100.0%)
SayGames Ltd	3/3 (100.0%)
Coco Play By TabTale	3/3 (100.0%)
Prometheus Interactive LLC	3/3 (100.0%)
LoveColoring Game	3/3 (100.0%)
KAYAC Inc.	3/3 (100.0%)
ZenLife Games Ltd	3/3 (100.0%)
ThemeKit	3/3 (100.0%)
trusted.mobile.app@gmail.com	3/3 (100.0%)
IVYGAMES	3/3 (100.0%)
FMPROJECT LIMITED	2/2 (100.0%)
LifeSim	2/2 (100.0%)
KamaGames	2/2 (100.0%)
publishing.apero@gmail.com	2/2 (100.0%)
LifePulse Puzzle Game Studio	2/2 (100.0%)
Gameberry Labs	2/2 (100.0%)
GAME OFFLINE HAY	2/2 (100.0%)
Hippo Lab	2/2 (100.0%)
MAGIC SEVEN CO., LIMITED	2/2 (100.0%)
HDuo Fun Games	2/2 (100.0%)
Maxlabs Photo Editor	2/2 (100.0%)
Color App Team	2/2 (100.0%)
FunGear inc	2/2 (100.0%)
Eyewind	2/2 (100.0%)
Braly JSC	2/2 (100.0%)
vinhdn07@gmail.com	2/2 (100.0%)
admin@vtn.global	2/2 (100.0%)
SUPERIOR STUDIO	2/2 (100.0%)
Appwest Limited	2/2 (100.0%)
Metaverse Labs	2/2 (100.0%)
Beat Blend Labs	2/2 (100.0%)
Red Sky Labs	2/2 (100.0%)
Solitaire Aquarium	2/2 (100.0%)
Mortys Games	2/2 (100.0%)
HK Hero Entertainment Co., Limited	2/2 (100.0%)
Adkins Studio	2/2 (100.0%)
Dainik Bhaskar Group	2/2 (100.0%)
Gianluca Cisana	1/1 (100.0%)
DIC-o	1/1 (100.0%)
mobileapps@tubema.ltd	1/1 (100.0%)
Rainberry, Inc.	1/1 (100.0%)
ORANGE GAME	1/1 (100.0%)

Fearless Games sp. j.	1/1 (100.0%)
TabTale	1/1 (100.0%)
Escape Adventure Games	1/1 (100.0%)
WONDER GROUP	1/1 (100.0%)
Estoty	1/1 (100.0%)
Supercent, Inc.	1/1 (100.0%)
cerdillac	1/1 (100.0%)
mulanidhvani@gmail.com	1/1 (100.0%)
FALCON GAME	1/1 (100.0%)
TFive Labs	1/1 (100.0%)
changpeng	1/1 (100.0%)
Dream Tap	1/1 (100.0%)
OUTLOU:D GAMES	1/1 (100.0%)
Better World Games	1/1 (100.0%)
Nebuchadnezzar DOO	1/1 (100.0%)
KTW Apps	1/1 (100.0%)
Free VPN Planet	1/1 (100.0%)
Digipom	1/1 (100.0%)
Audify Player.	1/1 (100.0%)
Colorful Point	1/1 (100.0%)
dammuhzaj@gmail.com	1/1 (100.0%)
Siti Berkah Studio	1/1 (100.0%)
Diavostar PTE. LTD	1/1 (100.0%)
developer@vottak.app	1/1 (100.0%)
ASD Dev Video Player for All Format	1/1 (100.0%)
Lotum one GmbH	1/1 (100.0%)
Clappy LLC	1/1 (100.0%)
Qiiwi Games AB	1/1 (100.0%)
Andrey Solovyev	1/1 (100.0%)
Qbis Studio	1/1 (100.0%)
Buddies Games Inc.	1/1 (100.0%)
Loop Games	1/1 (100.0%)
ZenTint Creations	1/1 (100.0%)
7788‘s	1/1 (100.0%)
MOUNTAIN GAME	1/1 (100.0%)
Doodle Mobile Ltd.	1/1 (100.0%)
CanaryDroid	1/1 (100.0%)
Macro Tap	1/1 (100.0%)
1SOFT	1/1 (100.0%)
Emily Yu	1/1 (100.0%)
Prop studio	1/1 (100.0%)
haphuong4251@gmail.com	1/1 (100.0%)
Fancolor	1/1 (100.0%)
Miniclip.com	1/1 (100.0%)
CASUAL AZUR GAMES	1/1 (100.0%)
Theago Liddell	1/1 (100.0%)
Warrior Game	1/1 (100.0%)
Pixel Art - draw in fun	1/1 (100.0%)
AppQuantum	1/1 (100.0%)
EasyFun Puzzle Game Studio	1/1 (100.0%)

ZiMAD	1/1 (100.0%)
RED BRIX COMPUTER SYSTEMS	1/1 (100.0%)
Focus apps	1/1 (100.0%)
Kitten Doll HK	1/1 (100.0%)
Kitten doll	1/1 (100.0%)
Meeto Team	1/1 (100.0%)
BUZZMEDIA INC.	1/1 (100.0%)
Smart AI DEV	1/1 (100.0%)
checksmartapp@gmail.com	1/1 (100.0%)
cghxstudio@gmail.com	1/1 (100.0%)
sunflower studio	1/1 (100.0%)
aimirror-support@polyversestudio.com	1/1 (100.0%)
Outdoing Apps	1/1 (100.0%)
Pixl Concerto Tech	1/1 (100.0%)
ITO Technologies, Inc.	1/1 (100.0%)
o16i Apps	1/1 (100.0%)
Clever Apps Pte. Ltd.	1/1 (100.0%)
Coreup Teknoloji Limited Şirketi	1/1 (100.0%)
Scopely	1/1 (100.0%)
uschultz	1/1 (100.0%)
Funny Design Keyboard Themes	1/1 (100.0%)
Delicate theme for Android App	1/1 (100.0%)
Esame Marketing Limited	1/1 (100.0%)
Fancy Studio Mods	1/1 (100.0%)
Live Wallpapers and Emoji Keyboard Themes	1/1 (100.0%)
App Soft Studio	1/1 (100.0%)
chudang@9codestudio.com	1/1 (100.0%)
CNT Interaktif Bilgi Tek. Yaz. San. ve Tic. A.S.	1/1 (100.0%)
EZTech Apps	1/1 (100.0%)
QR SCAN Team	1/1 (100.0%)
Security Lab.	1/1 (100.0%)
Ultimate Guitar USA LLC	1/1 (100.0%)
Radio FM Online Free	1/1 (100.0%)
LUCKY YOUTH AND FAMILY SERVICES INC	1/1 (100.0%)
RadioFM	1/1 (100.0%)
tobbychan21@gmail.com	1/1 (100.0%)
Appgeneration - Radio, Podcasts, Games	1/1 (100.0%)
Letterboxd Limited	1/1 (100.0%)
MeetMe.com	1/1 (100.0%)
Skywork AI Pte. Ltd.	1/1 (100.0%)
Gamehaus Network	1/1 (100.0%)
JoyMore GAME	1/1 (100.0%)
BrainMount Ltd	1/1 (100.0%)
LeeNgooc	1/1 (100.0%)
Poki	1/1 (100.0%)
Boom Studio Limited	1/1 (100.0%)
BattleCry HQ Studio	1/1 (100.0%)
Cricbuzz.com	1/1 (100.0%)
Gluak srl	1/1 (100.0%)
HealthTracker Apps	1/1 (100.0%)

Lite Tools Games	1/1 (100.0%)
PlayStudioInc	1/1 (100.0%)
ZeptoLab	1/1 (100.0%)
Smart Widget Labs Co Ltd	1/1 (100.0%)
Severex	1/1 (100.0%)
LinkDesks - Jewel Games Star	1/1 (100.0%)
supermt	1/1 (100.0%)
Cricim world	1/1 (100.0%)
MEDIADECODE	1/1 (100.0%)
Peaksel Ringtones Apps	1/1 (100.0%)
Goldlab Pro	1/1 (100.0%)
PlayCreek Games	1/1 (100.0%)
TAKBIR	1/1 (100.0%)
Blackout Lab	1/1 (100.0%)
CloudWest Technology	1/1 (100.0%)
Touchzing Media Private Limited	1/1 (100.0%)
neilbenecke529@gmail.com	1/1 (100.0%)
Smart Utils Dev Team	1/1 (100.0%)
ruivop	1/1 (100.0%)
Wavez Technology Ltd	1/1 (100.0%)
Simple Design Ltd.	1/1 (100.0%)
AI Screen Translator	1/1 (100.0%)
Sad Panda Studios Ltd	1/1 (100.0%)
Slimmerbits LLC	1/1 (100.0%)
Bright Prospect	1/1 (100.0%)
Rear Window Limited	1/1 (100.0%)
Appcentric Team	1/1 (100.0%)
Trusted Android App	1/1 (100.0%)
blurbackgroundstudio@gmail.com	1/1 (100.0%)
Apfolife	1/1 (100.0%)
abdallahshure99@gmail.com	1/1 (100.0%)
musicechofeedback@outlook.com	1/1 (100.0%)
Naz Digital	1/1 (100.0%)
tuyetnhungpham2710@gmail.com	1/1 (100.0%)
TEEWEE LIMITED	1/1 (100.0%)
Tiki Punch Studio	1/1 (100.0%)
MBit Music Inc.	1/1 (100.0%)
Zayzik : LED Keyboard Studio	1/1 (100.0%)
Live Wallpapers by Wave Studio	1/1 (100.0%)
Digital Dreamworks Studio	1/1 (100.0%)
Color Joy	1/1 (100.0%)
Weather Radar Team	1/1 (100.0%)
Maxlabs Graphic Design Tools	1/1 (100.0%)
kahlochSto	1/1 (100.0%)
GreenTTeaGame	1/1 (100.0%)
GuonianGame	1/1 (100.0%)
CHAPTER 4	1/1 (100.0%)
Playa Games	1/1 (100.0%)
3D Viet Ha	1/1 (100.0%)
Bilge Bulut Mobile	1/1 (100.0%)

profoundboradwang@gmail.com	1/1 (100.0%)
Dream Space	1/1 (100.0%)
Ringtone Phone App	1/1 (100.0%)
blomsterstudio1733@gmail.com	1/1 (100.0%)
BG.Studio	1/1 (100.0%)
GREEVIL'S GREED	1/1 (100.0%)
Wego.com	1/1 (100.0%)
Hitapps Games	1/1 (100.0%)
AppOn Innovate	1/1 (100.0%)
SZYJ Technology	1/1 (100.0%)
AVIRISE LIMITED HK	1/1 (100.0%)
Hydodo	1/1 (100.0%)
YoYo Dress Up Games	1/1 (100.0%)
Addons and Mods for Minecraft	1/1 (100.0%)
WE CENTER	1/1 (100.0%)
Nguyen Công Phuong	1/1 (100.0%)
JoyArk Official-Cloud Games	1/1 (100.0%)
rosytales	1/1 (100.0%)
dreamphotolab2016@gmail.com	1/1 (100.0%)
Studio Sol Comunicação Digital	1/1 (100.0%)
Dream Tools	1/1 (100.0%)
nttc.studio@gmail.com	1/1 (100.0%)
haiyanstore	1/1 (100.0%)
LANGUAGE POWER	1/1 (100.0%)
1MB Apps Studio	1/1 (100.0%)
GOMIN MOBILE	1/1 (100.0%)
Beloud.com	1/1 (100.0%)
Opera	1/1 (100.0%)
Tradera	1/1 (100.0%)
NIGHP SOFTWARE	1/1 (100.0%)
Golden Gate Media	1/1 (100.0%)
No dev found	16/24 (66.67%)
Vidmark Inc.	2/3 (66.67%)
GeniusTools Labs	2/3 (66.67%)
Cards	3/5 (60.0%)
Galaxy studio apps	2/4 (50.0%)
CEM SOFTWARE LTD	2/4 (50.0%)
Gamma Play	1/2 (50.0%)
Vidow™	1/2 (50.0%)
Fillog Studio	1/2 (50.0%)
gobistudio88@gmail.com	1/2 (50.0%)
DogByte Games	1/3 (33.33%)
XGAME STUDIO	1/3 (33.33%)
Data Unavailable	0/11 (0%)
KIGLE	0/8 (0%)
GunjanApps Studios	0/6 (0%)
One Music Player	0/4 (0%)
App Game Development Solutions	0/3 (0%)
Shadow soft	0/3 (0%)
Baram FZE	0/3 (0%)
Dumitru Boico	0/3 (0%)

P & L Studio	0/3 (0%)
ElePant: Kids Learning Games for Toddlers & Baby	0/3 (0%)
Three Cookers Game	0/3 (0%)
Awesome Game Studio	0/2 (0%)
WallForApps	0/2 (0%)
TarrySoft	0/2 (0%)
IDZ Digital Private Limited	0/2 (0%)
InShot Video Editor	0/2 (0%)
Anfona Tech	0/2 (0%)
MayZing Tech	0/2 (0%)
FastSoft	0/2 (0%)
Flavapp	0/2 (0%)
Masivapp	0/2 (0%)
Stillfront Supremacy GmbH	0/2 (0%)
Yangmei Studios	0/2 (0%)
Banix Studio	0/2 (0%)
DOSA Apps	0/2 (0%)
Firehawk	0/2 (0%)
Weather Forecast & Widget & Radar	0/2 (0%)
Amila	0/2 (0%)
dev@pocketclubs.com	0/2 (0%)
Fabulous Fun	0/1 (0%)
Panteon	0/1 (0%)
Catchy Tools	0/1 (0%)
M2Catalyst, LLC.	0/1 (0%)
trantheanhmkt@gmail.com	0/1 (0%)
Kongs	0/1 (0%)
Amobear Studio	0/1 (0%)
Binary Cores	0/1 (0%)
Atlantis Ultra Station	0/1 (0%)
Launchers World	0/1 (0%)
recorder & smart apps	0/1 (0%)
CoolDev Co Ltd	0/1 (0%)
VIDEOSHOW Video Editor & Maker & AI Chat Generator	0/1 (0%)
Video & Photo Editor Apps	0/1 (0%)
Fast Tour Booking - Flights & Hotels	0/1 (0%)
100Pi Labs	0/1 (0%)
hello@yangmeistudios.com	0/1 (0%)
Yanstar Studio OU	0/1 (0%)
Generation z apps	0/1 (0%)
Apps You Love	0/1 (0%)
Arioch Pds - Apps & Games	0/1 (0%)
Muslim Worldapp	0/1 (0%)
Jolt Global Apps - VPN, Ai, Keyboard & Learning	0/1 (0%)
Mabixa	0/1 (0%)
GeDa DevTeam	0/1 (0%)
SincMobile Apps	0/1 (0%)
renvosoft@gmail.com	0/1 (0%)
anhtuannt3011@gmail.com	0/1 (0%)
Appsomniacs LLC	0/1 (0%)
SOUSSI NIAIMI Badr-Eddine	0/1 (0%)
Mediocre	0/1 (0%)
HAU SALA GAME COMPANY LIMITED	0/1 (0%)
Flirtify: Live Chat & Dating	0/1 (0%)
Stillfront Supremacy Ltd	0/1 (0%)
Apps Resort - Daily Tool Apps	0/1 (0%)
phamnguyetnt89@gmail.com	0/1 (0%)
Love Photo Frames	0/1 (0%)
Fitify Workouts s.r.o.	0/1 (0%)
Litera Games	0/1 (0%)
Okapps	0/1 (0%)
Pixel Kraft Studios	0/1 (0%)
Wow Themes & Fulll HD Themes	0/1 (0%)
Gigo Ltc	0/1 (0%)
TM company	0/1 (0%)
tnifoui wallpaper	0/1 (0%)
Appache apps and games ltd	0/1 (0%)
ng-labs	0/1 (0%)
Freepik Company	0/1 (0%)
ChargeFinder	0/1 (0%)
Quality App Zone	0/1 (0%)
BoostVision	0/1 (0%)
StarPham	0/1 (0%)
text messages	0/1 (0%)
Bringar Apps	0/1 (0%)
Quarzo Apps	0/1 (0%)
JMGame	0/1 (0%)
Travel Maps Tech	0/1 (0%)
Copa Fácil	0/1 (0%)
Messier31	0/1 (0%)
Accurate Weather Forecast & Weather Radar Map	0/1 (0%)
TOH Talent Team	0/1 (0%)
Block Puzzle Games 2018	0/1 (0%)
EriitoDraw	0/1 (0%)
Music Apps - Allmusic	0/1 (0%)
nguyenquynhtrangkt08@gmail.com	0/1 (0%)
neraldoverland342@gmail.com	0/1 (0%)
BoBo World Games	0/1 (0%)
probadoSoft	0/1 (0%)
TOH Games	0/1 (0%)
Minibuu	0/1 (0%)
Tool Apps Hub	0/1 (0%)
App Bards	0/1 (0%)
Digital App Valley	0/1 (0%)
SoftAxes	0/1 (0%)
GjangHa	0/1 (0%)
IApplication	0/1 (0%)
Konnect Apps	0/1 (0%)
abdulmuttalip.er4680@gmail.com	0/1 (0%)
Marcel Bartecki	0/1 (0%)

Splaish Studio	0/1 (0%)
Kolmo Games	0/1 (0%)
Plus AI	0/1 (0%)
QR Code Scanner & Barcode Reader	0/1 (0%)
Kamrej Apps	0/1 (0%)
Nova Apps Studios	0/1 (0%)
BigSoft inc.	0/1 (0%)
Sun global	0/1 (0%)
Easy Language Translator	0/1 (0%)
nhuomtv@cemsoftwareltd.com	0/1 (0%)
mobirix	0/1 (0%)
Lincod Studio	0/1 (0%)
Fit Health Inc.	0/1 (0%)
Tulip Sports TV	0/1 (0%)
Dictionary World11	0/1 (0%)
Appslogie	0/1 (0%)
appwave333@gmail.com	0/1 (0%)
genie islam	0/1 (0%)
PhucArts	0/1 (0%)
Mi Game Pro Uru	0/1 (0%)
Rubén Mayayo	0/1 (0%)
Tools Generation Hub	0/1 (0%)
tracyhoggappstore@gmail.com	0/1 (0%)
Radiant Islamic Apps	0/1 (0%)
UniTiki	0/1 (0%)
InPics	0/1 (0%)
highsecure	0/1 (0%)
QY Studio	0/1 (0%)
Greenstream Apps	0/1 (0%)
Simple Mobile Tool	0/1 (0%)
Viaplay	0/1 (0%)

Table 15: Developer active stage data

Developer (name/email)	Violation %
Easybrain	14/14 (100.0%)
BoomBit Games	7/7 (100.0%)
CEM SOFTWARE LTD	4/4 (100.0%)
RobTop Games	4/4 (100.0%)
nguyenluan@lutech.ltd	4/4 (100.0%)
hoahuongduong170120@gmail.com	4/4 (100.0%)
SayGames Ltd	3/3 (100.0%)
Prometheus Interactive LLC	3/3 (100.0%)
LoveColoring Game	3/3 (100.0%)
KAYAC Inc.	3/3 (100.0%)
ZenLife Games Ltd	3/3 (100.0%)
ThemeKit	3/3 (100.0%)
XGAME STUDIO	3/3 (100.0%)
IVYGAMES	3/3 (100.0%)
FMPROJECT LIMITED	2/2 (100.0%)
LifeSim	2/2 (100.0%)
KamaGames	2/2 (100.0%)
publishing.apero@gmail.com	2/2 (100.0%)
LifePulse Puzzle Game Studio	2/2 (100.0%)
Gameberry Labs	2/2 (100.0%)
GAME OFFLINE HAY	2/2 (100.0%)
Hippo Lab	2/2 (100.0%)
MAGIC SEVEN CO., LIMITED	2/2 (100.0%)
HDuo Fun Games	2/2 (100.0%)
Maxlabs Photo Editor	2/2 (100.0%)
Color App Team	2/2 (100.0%)
FunGear inc	2/2 (100.0%)
Eyewind	2/2 (100.0%)
Braly JSC	2/2 (100.0%)
vinhdn07@gmail.com	2/2 (100.0%)
admin@vtn.global	2/2 (100.0%)
SUPERIOR STUDIO	2/2 (100.0%)
Appwest Limited	2/2 (100.0%)
Metaverse Labs	2/2 (100.0%)
Beat Blend Labs	2/2 (100.0%)
Red Sky Labs	2/2 (100.0%)
Solitaire Aquarium	2/2 (100.0%)
Weather Forecast & Widget & Radar	2/2 (100.0%)
Fillog Studio	2/2 (100.0%)
Mortys Games	2/2 (100.0%)
gobistudio88@gmail.com	2/2 (100.0%)
Adkins Studio	2/2 (100.0%)
Dainik Bhaskar Group	2/2 (100.0%)
DIC-o	1/1 (100.0%)
mobileapps@tubema.ltd	1/1 (100.0%)
Rainberry, Inc.	1/1 (100.0%)
ORANGE GAME	1/1 (100.0%)
Fearless Games sp. j.	1/1 (100.0%)
Escape Adventure Games	1/1 (100.0%)
WONDER GROUP	1/1 (100.0%)

Estoty	1/1 (100.0%)
Supercent, Inc.	1/1 (100.0%)
cerdillac	1/1 (100.0%)
mulanidhvani@gmail.com	1/1 (100.0%)
FALCON GAME	1/1 (100.0%)
trantheanhmkt@gmail.com	1/1 (100.0%)
TFive Labs	1/1 (100.0%)
changpeng	1/1 (100.0%)
Amobear Studio	1/1 (100.0%)
Dream Tap	1/1 (100.0%)
OUTLOU:D GAMES	1/1 (100.0%)
Better World Games	1/1 (100.0%)
Nebuchadnezzar DOO	1/1 (100.0%)
KTW Apps	1/1 (100.0%)
Free VPN Planet	1/1 (100.0%)
Digipom	1/1 (100.0%)
recorder & smart apps	1/1 (100.0%)
Audify Player.	1/1 (100.0%)
Colorful Point	1/1 (100.0%)
dammuhzaj@gmail.com	1/1 (100.0%)
Diavostar PTE. LTD	1/1 (100.0%)
CoolDev Co Ltd	1/1 (100.0%)
VIDEOSHOW Video Editor & Maker & AI Chat Generator	1/1 (100.0%)
developer@vottak.app	1/1 (100.0%)
Lotum one GmbH	1/1 (100.0%)
Clappy LLC	1/1 (100.0%)
Andrey Solovyev	1/1 (100.0%)
Qbis Studio	1/1 (100.0%)
Loop Games	1/1 (100.0%)
ZenTint Creations	1/1 (100.0%)
7788‘s	1/1 (100.0%)
MOUNTAIN GAME	1/1 (100.0%)
Doodle Mobile Ltd.	1/1 (100.0%)
CanaryDroid	1/1 (100.0%)
Macro Tap	1/1 (100.0%)
1SOFT	1/1 (100.0%)
renvosoft@gmail.com	1/1 (100.0%)
Emily Yu	1/1 (100.0%)
Prop studio	1/1 (100.0%)
haphuong4251@gmail.com	1/1 (100.0%)
Fancolor	1/1 (100.0%)
Miniclip.com	1/1 (100.0%)
CASUAL AZUR GAMES	1/1 (100.0%)
Theago Liddell	1/1 (100.0%)
Warrior Game	1/1 (100.0%)
Pixel Art - draw in fun	1/1 (100.0%)
AppQuantum	1/1 (100.0%)
EasyFun Puzzle Game Studio	1/1 (100.0%)
ZiMAD	1/1 (100.0%)
RED BRIX COMPUTER SYSTEMS	1/1 (100.0%)

Focus apps	1/1 (100.0%)
Kitten Doll HK	1/1 (100.0%)
Kitten doll	1/1 (100.0%)
Flirtify: Live Chat & Dating	1/1 (100.0%)
Meeto Team	1/1 (100.0%)
BUZZMEDIA INC.	1/1 (100.0%)
Apps Resort - Daily Tool Apps	1/1 (100.0%)
Smart AI DEV	1/1 (100.0%)
checksmartapp@gmail.com	1/1 (100.0%)
cghxstudio@gmail.com	1/1 (100.0%)
aimirror-support@polyversestudio.com	1/1 (100.0%)
Outdoing Apps	1/1 (100.0%)
Pixl Concerto Tech	1/1 (100.0%)
o16i Apps	1/1 (100.0%)
Clever Apps Pte. Ltd.	1/1 (100.0%)
Coreup Teknoloji Limited Şirketi	1/1 (100.0%)
Funny Design Keyboard Themes	1/1 (100.0%)
Delicate theme for Android App	1/1 (100.0%)
Wow Themes & Fulll HD Themes	1/1 (100.0%)
Esame Marketing Limited	1/1 (100.0%)
Fancy Studio Mods	1/1 (100.0%)
Live Wallpapers and Emoji Keyboard Themes	1/1 (100.0%)
chudang@9codestudio.com	1/1 (100.0%)
CNT Interaktif Bilgi Tek. Yaz. San. ve Tic. A.S.	1/1 (100.0%)
EZTech Apps	1/1 (100.0%)
QR SCAN Team	1/1 (100.0%)
Security Lab.	1/1 (100.0%)
Ultimate Guitar USA LLC	1/1 (100.0%)
Radio FM Online Free	1/1 (100.0%)
RadioFM	1/1 (100.0%)
tobbychan21@gmail.com	1/1 (100.0%)
Appgeneration - Radio, Podcasts, Games	1/1 (100.0%)
MeetMe.com	1/1 (100.0%)
Skywork AI Pte. Ltd.	1/1 (100.0%)
Gamehaus Network	1/1 (100.0%)
JoyMore GAME	1/1 (100.0%)
BrainMount Ltd	1/1 (100.0%)
LeeNgooc	1/1 (100.0%)
Poki	1/1 (100.0%)
Boom Studio Limited	1/1 (100.0%)
JMGame	1/1 (100.0%)
BattleCry HQ Studio	1/1 (100.0%)
Cricbuzz.com	1/1 (100.0%)
Messier31	1/1 (100.0%)
Gluak srl	1/1 (100.0%)
HealthTracker Apps	1/1 (100.0%)
Lite Tools Games	1/1 (100.0%)
PlayStudioInc	1/1 (100.0%)
ZeptoLab	1/1 (100.0%)
Smart Widget Labs Co Ltd	1/1 (100.0%)

LinkDesks - Jewel Games Star	1/1 (100.0%)
supermt	1/1 (100.0%)
Cricim world	1/1 (100.0%)
MEDIADECODE	1/1 (100.0%)
Peaksel Ringtones Apps	1/1 (100.0%)
PlayCreek Games	1/1 (100.0%)
CloudWest Technology	1/1 (100.0%)
Touchzing Media Private Limited	1/1 (100.0%)
neilbenecke529@gmail.com	1/1 (100.0%)
ruivop	1/1 (100.0%)
Wavez Technology Ltd	1/1 (100.0%)
Tool Apps Hub	1/1 (100.0%)
AI Screen Translator	1/1 (100.0%)
Slimmerbits LLC	1/1 (100.0%)
Bright Prospect	1/1 (100.0%)
Rear Window Limited	1/1 (100.0%)
Appcentric Team	1/1 (100.0%)
Trusted Android App	1/1 (100.0%)
blurbackgroundstudio@gmail.com	1/1 (100.0%)
Apfolife	1/1 (100.0%)
abdallahshure99@gmail.com	1/1 (100.0%)
musicechofeedback@outlook.com	1/1 (100.0%)
GjangHa	1/1 (100.0%)
Naz Digital	1/1 (100.0%)
Konnect Apps	1/1 (100.0%)
tuyetnhungpham2710@gmail.com	1/1 (100.0%)
TEEWEE LIMITED	1/1 (100.0%)
QR Code Scanner & Barcode Reader	1/1 (100.0%)
Tiki Punch Studio	1/1 (100.0%)
MBit Music Inc.	1/1 (100.0%)
Zayzik : LED Keyboard Studio	1/1 (100.0%)
Live Wallpapers by Wave Studio	1/1 (100.0%)
Digital Dreamworks Studio	1/1 (100.0%)
Color Joy	1/1 (100.0%)
Weather Radar Team	1/1 (100.0%)
Maxlabs Graphic Design Tools	1/1 (100.0%)
kahlochSto	1/1 (100.0%)
nhuomtv@cemsoftwareltd.com	1/1 (100.0%)
GreenTTeaGame	1/1 (100.0%)
GuonianGame	1/1 (100.0%)
3D Viet Ha	1/1 (100.0%)
Bilge Bulut Mobile	1/1 (100.0%)
profoundboradwang@gmail.com	1/1 (100.0%)
Dream Space	1/1 (100.0%)
Ringtone Phone App	1/1 (100.0%)
blomsterstudio1733@gmail.com	1/1 (100.0%)
BG.Studio	1/1 (100.0%)
Wego.com	1/1 (100.0%)
Hitapps Games	1/1 (100.0%)
Fit Health Inc.	1/1 (100.0%)

AppOn Innovate	1/1 (100.0%)
SZYJ Technology	1/1 (100.0%)
AVIRISE LIMITED HK	1/1 (100.0%)
Hydodo	1/1 (100.0%)
YoYo Dress Up Games	1/1 (100.0%)
Addons and Mods for Minecraft	1/1 (100.0%)
WE CENTER	1/1 (100.0%)
Nguyen Công Phuong	1/1 (100.0%)
JoyArk Official-Cloud Games	1/1 (100.0%)
rosytales	1/1 (100.0%)
dreamphotolab2016@gmail.com	1/1 (100.0%)
Tools Generation Hub	1/1 (100.0%)
Dream Tools	1/1 (100.0%)
nttc.studio@gmail.com	1/1 (100.0%)
LANGUAGE POWER	1/1 (100.0%)
1MB Apps Studio	1/1 (100.0%)
QY Studio	1/1 (100.0%)
Beloud.com	1/1 (100.0%)
Opera	1/1 (100.0%)
Tradera	1/1 (100.0%)
Golden Gate Media	1/1 (100.0%)
Outfit7 Limited	7/9 (77.78%)
gameone	3/4 (75.0%)
Vidmark Inc.	2/3 (66.67%)
P & L Studio	2/3 (66.67%)
GeniusTools Labs	2/3 (66.67%)
trusted.mobile.app@gmail.com	2/3 (66.67%)
Cards	3/5 (60.0%)
Battery Stats Saver	3/5 (60.0%)
No dev found	13/24 (54.17%)
Galaxy studio apps	2/4 (50.0%)
Gamma Play	1/2 (50.0%)
Vidow™	1/2 (50.0%)
DogByte Games	1/3 (33.33%)
Three Cookers Game	1/3 (33.33%)
Data Unavailable	0/11 (0%)
KIGLE	0/8 (0%)
GunjanApps Studios	0/6 (0%)
CrazyLabs LTD	0/5 (0%)
One Music Player	0/4 (0%)
App Game Development Solutions	0/3 (0%)
Shadow soft	0/3 (0%)
Baram FZE	0/3 (0%)
Coco Play By TabTale	0/3 (0%)
Dumitru Boico	0/3 (0%)
ElePant: Kids Learning Games for Toddlers & Baby	0/3 (0%)
Awesome Game Studio	0/2 (0%)
WallForApps	0/2 (0%)
TarrySoft	0/2 (0%)
IDZ Digital Private Limited	0/2 (0%)
InShot Video Editor	0/2 (0%)

Anfona Tech	0/2 (0%)
MayZing Tech	0/2 (0%)
FastSoft	0/2 (0%)
Flavapp	0/2 (0%)
Masivapp	0/2 (0%)
Stillfront Supremacy GmbH	0/2 (0%)
Yangmei Studios	0/2 (0%)
Banix Studio	0/2 (0%)
DOSA Apps	0/2 (0%)
Firehawk	0/2 (0%)
Amila	0/2 (0%)
HK Hero Entertainment Co., Limited	0/2 (0%)
dev@pocketclubs.com	0/2 (0%)
Gianluca Cisana	0/1 (0%)
TabTale	0/1 (0%)
Fabulous Fun	0/1 (0%)
Panteon	0/1 (0%)
Catchy Tools	0/1 (0%)
M2Catalyst, LLC.	0/1 (0%)
Kongs	0/1 (0%)
Binary Cores	0/1 (0%)
Atlantis Ultra Station	0/1 (0%)
Launchers World	0/1 (0%)
Siti Berkah Studio	0/1 (0%)
Video & Photo Editor Apps	0/1 (0%)
Fast Tour Booking - Flights & Hotels	0/1 (0%)
ASD Dev Video Player for All Format	0/1 (0%)
100Pi Labs	0/1 (0%)
Qiiwi Games AB	0/1 (0%)
hello@yangmeistudios.com	0/1 (0%)
Buddies Games Inc.	0/1 (0%)
Yanstar Studio OU	0/1 (0%)
Generation z apps	0/1 (0%)
Apps You Love	0/1 (0%)
Arioch Pds - Apps & Games	0/1 (0%)
Muslim Worldapp	0/1 (0%)
Jolt Global Apps - VPN, Ai, Keyboard & Learning	0/1 (0%)
Mabixa	0/1 (0%)
GeDa DevTeam	0/1 (0%)
SincMobile Apps	0/1 (0%)
anhtuannt3011@gmail.com	0/1 (0%)
Appsomniacs LLC	0/1 (0%)
SOUSSI NIAIMI Badr-Eddine	0/1 (0%)
Mediocre	0/1 (0%)
HAU SALA GAME COMPANY LIMITED	0/1 (0%)
Stillfront Supremacy Ltd	0/1 (0%)
phamnguyetnt89@gmail.com	0/1 (0%)
sunflower studio	0/1 (0%)
Love Photo Frames	0/1 (0%)
ITO Technologies, Inc.	0/1 (0%)

Fitify Workouts s.r.o.	0/1 (0%)
Litera Games	0/1 (0%)
Scopely	0/1 (0%)
Okapps	0/1 (0%)
Pixel Kraft Studios	0/1 (0%)
uschultz	0/1 (0%)
Gigo Ltc	0/1 (0%)
App Soft Studio	0/1 (0%)
TM company	0/1 (0%)
tnifoui wallpaper	0/1 (0%)
Appache apps and games ltd	0/1 (0%)
ng-labs	0/1 (0%)
Freepik Company	0/1 (0%)
ChargeFinder	0/1 (0%)
Quality App Zone	0/1 (0%)
BoostVision	0/1 (0%)
LUCKY YOUTH AND FAMILY SERVICES INC	0/1 (0%)
Letterboxd Limited	0/1 (0%)
StarPham	0/1 (0%)
text messages	0/1 (0%)
Bringar Apps	0/1 (0%)
Quarzo Apps	0/1 (0%)
Travel Maps Tech	0/1 (0%)
Copa Fácil	0/1 (0%)
Accurate Weather Forecast & Weather Radar Map	0/1 (0%)
TOH Talent Team	0/1 (0%)
Block Puzzle Games 2018	0/1 (0%)
Severex	0/1 (0%)
EriitoDraw	0/1 (0%)
Music Apps - Allmusic	0/1 (0%)
nguyenquynhtrangkt08@gmail.com	0/1 (0%)
Goldlab Pro	0/1 (0%)
neraldoverland342@gmail.com	0/1 (0%)
BoBo World Games	0/1 (0%)
TAKBIR	0/1 (0%)
Blackout Lab	0/1 (0%)
probadoSoft	0/1 (0%)
Smart Utils Dev Team	0/1 (0%)
TOH Games	0/1 (0%)
Minibuu	0/1 (0%)
Simple Design Ltd.	0/1 (0%)
Sad Panda Studios Ltd	0/1 (0%)
App Bards	0/1 (0%)
Digital App Valley	0/1 (0%)
SoftAxes	0/1 (0%)
IApplication	0/1 (0%)
abdulmuttalip.er4680@gmail.com	0/1 (0%)
Marcel Bartecki	0/1 (0%)
Splaish Studio	0/1 (0%)
Kolmo Games	0/1 (0%)

Plus AI	0/1 (0%)
Kamrej Apps	0/1 (0%)
Nova Apps Studios	0/1 (0%)
BigSoft inc.	0/1 (0%)
Sun global	0/1 (0%)
Easy Language Translator	0/1 (0%)
mobirix	0/1 (0%)
CHAPTER 4	0/1 (0%)
Playa Games	0/1 (0%)
Lincod Studio	0/1 (0%)
GREEVIL'S GREED	0/1 (0%)
Tulip Sports TV	0/1 (0%)
Dictionary World11	0/1 (0%)
Appslogie	0/1 (0%)
appwave333@gmail.com	0/1 (0%)
genie islam	0/1 (0%)
PhucArts	0/1 (0%)
Mi Game Pro Uru	0/1 (0%)
Rubén Mayayo	0/1 (0%)
Studio Sol Comunicação Digital	0/1 (0%)
tracyhoggappstore@gmail.com	0/1 (0%)
Radiant Islamic Apps	0/1 (0%)
UniTiki	0/1 (0%)
InPics	0/1 (0%)
haiyanstore	0/1 (0%)
highsecure	0/1 (0%)
GOMIN MOBILE	0/1 (0%)
Greenstream Apps	0/1 (0%)
Simple Mobile Tool	0/1 (0%)
Viaplay	0/1 (0%)
NIGHP SOFTWARE	0/1 (0%)