A Comprehensive Study on Third-Party User Tracking in Mobile Applications

Federica Paci
University of Verona
Verona, Italy
federica.paci@univr.it

Jacopo Pizzoli
University of Verona
Verona, Italy
jacopo.pizzoli@studenti.univr.it

Nicola Zannone
Eindhoven University of Technology
Eindhoven, The Netherlands
n.zannone@tue.nl

ABSTRACT

Third-party tracking is becoming a prevalent practice in mobile app ecosystems. While providing benefits for app developers, this practice also introduces several privacy issues for end-users. The European General Data Protection Regulation (GDPR) and the ePrivacy Directive (ePD) mandate that mobile apps must obtain user consent before sharing users' personal data with third-party trackers. This work presents an empirical study investigating the compliance of 400 popular mobile apps (200 Android apps and their corresponding version for iOS) with the ePD and GDPR requirements on valid consent. Moreover, we determined whether these mobile apps actually enforce the consent given by users on being tracked and which are the more common third-party tracker domains contacted by the apps. The analysis shows that none of the studied apps fully comply with ePD and GDPR requirements on valid consent. The most common violations were associated with the principles of freely-given, specific, and revocable consent. Moreover, we found that almost half of the analyzed apps contact third-party tracker domains even when the user has not given their consent to be tracked.

CCS CONCEPTS

• **Security and privacy → Privacy protections**; • **Applied computing → Law**; • **Human-centered computing → Mobile phones**.

KEYWORDS

Privacy, valid consent, GDPR, ePD, mobile apps, third-party tracking

ACM Reference Format:
Federica Paci, Jacopo Pizzoli, and Nicola Zannone. 2023. A Comprehensive Study on Third-Party User Tracking in Mobile Applications. In *The 18th International Conference on Availability, Reliability and Security (ARES 2023), August 29-September 1, 2023, Benevento, Italy*. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3600160.3605079

1 INTRODUCTION

Third-party tracking, which involves intentionally collecting, processing, and sharing users' behavioral data with third-party companies [4], has become a prevalent practice in both the web [22] and mobile app ecosystems [15]. The utilization of third-party trackers offers several advantages to app developers, including the provision of analytics to enhance user experience and the ability to deliver personalized advertisements. In particular, the current web and mobile app advertising ecosystem heavily depends on continuous data collection and tracking, enabling advertising companies to profit from collecting vast amounts of personal data. This practice, however, creates a reliance on privacy-invasive data practices, with little awareness among users regarding which data is collected and how it is used.

Data protection and privacy legislation, such as the General Data Protection Regulation (GDPR) [9] and the ePrivacy Directive (ePD) [8] in the EU, establish explicit guidelines for the collection and processing of personal data. These privacy regulations specifically define the concept of *valid consent*, which requires consent to be *freely given*, *specific*, *informed*, and *unambiguous*. Moreover, consent should be obtained *prior* to the collection and processing of data.

As a result of the GDPR and the ePD, users within the EU encounter cookie banners on every mobile app. However, there is little empirical evidence on whether mobile apps implement consent mechanisms that are compliant with ePD and GDPR requirements on valid consent and whether they correctly enforce user consent. The majority of research on third-party tracking in mobile applications has focused on analyzing the prevalent third-party trackers utilized by mobile apps, the data transmitted to these trackers, and the organizations responsible for gathering this data [4, 13, 16, 17]. Additionally, most of these studies primarily concentrated on analyzing either Android or iOS apps exclusively. To the best of our knowledge, there is only one study [13] that determined whether mobile apps request consent before engaging in third-party tracking. However, this study does not investigate the compliance of mobile apps' consent mechanisms with ePD and GDPR requirements on valid consent and whether they enforce the actual consent given by the users.

To address these gaps, we studied 400 popular mobile apps (200 Android apps and their corresponding version for iOS) and analyzed *(i)* whether they comply with the ePD and GDPR's requirements on valid consent, *(ii)* whether they properly enforce users' consent on being tracked, and *(iii)* the top third-party tracker domains the apps communicate with. To assess compliance with legal requirements, we evaluated the cookie banner of each app using an analysis template capturing cases of violations of the requirements. The enforcement of the consent given by users and the top third-party tracker domains were assessed based on the network traffic generated by the applications when consent was given and when the consent was revoked.

ARES 2023, August 29-September 1, 2023, Benevento, Italy

ACM ISBN 979-8-4007-0772-8/23/08…$15.00
https://doi.org/10.1145/3600160.3605079

Contributions. First, we distilled a template to enable systematic analysis of consent mechanisms with respect to ePD and GDPR requirements on valid consent. Second, our study provides empirical evidence indicating a widespread lack of compliance with ePD and GDPR in terms of obtaining valid consent and enforcing user-given consent. None of the mobile apps examined in our study obtained valid consent as required by ePD and GDPR. The majority of apps violated requirements related to freely-given, specific, and revocable consent. Additionally, almost half of the apps continued to engage with third-party trackers even after users declined consent, indicating a failure to adhere appropriately to user-given consent. Third, our study confirms the prevalence of third-party trackers on both Android and iOS platforms, with Android apps mainly utilizing analytics and fingerprinting services, while iOS apps were connected to advertising services.

Outline. The remainder of the paper is organized as follows. The next section presents the legal requirements on valid consent that cookie banners should satisfy, and Section 3 discusses related work. Section 4 presents the methodology adopted in our study, and Section 5 reports the results and discuss the limitations of the study. Section 6 discusses the main findings and provides directions for future research.

2 LEGAL REQUIREMENTS ON COOKIE BANNERS

Cookie banners are the predominant consent mechanism used by mobile app developers. In order for the consent given through the banners to be valid within the EU, their design should comply with the requirements imposed by the ePrivacy Directive 2002/58/EC amended by Directive 2009/136/EC and the General Data Protection Regulation. An overview of the main requirements that cookie banners should satisfy to collect valid consent is presented in Table 1.

According to Article 5(3) of the ePD, it is required to inform users about the reasons for processing their personal data and obtain their consent before any data collected to monitor their online activities is stored or accessed on their devices. This requirement is violated when a cookie banner is not presented to the users before tracking technologies are deployed. The GDPR complements the ePD by imposing specific requirements on valid consent (GDPR Art. 4(11) and Art. 7). Art. 4(11) establishes that consent is valid when is *freely given*, *informed*, *unambiguous* and *specific* to each different purpose of the processing. The term freely given implies that a user should be able to provide consent without experiencing any form of coercion or undue influence in persuading them to give their consent. Thus, cookie banners that obstruct access to the mobile app for users who have not granted consent and only present the option to accept all cookies would not be compliant.

For consent to be unambiguous, the user must provide consent through clear and affirmative action like clicking on a button or checking a box. Therefore, cookie banners that use pre-ticked boxes or pre-selected sliders to opt in do not lead to valid consent. Moreover, denying consent should be as easy as giving it. A cookie banner that places the "Reject All" button in the 'configuration settings' section or on a third-party page would not be compliant. Similarly, cookie banners that emphasize the "Accept All" button over the "Reject All" button using contrast and colors are not compliant because they influence the users toward the "Accept All" button. An additional non-compliant approach is incorporating the concept of legitimate interest for subsequent processing in the "deepest layers of the banner", which can be misleading for users as they may mistakenly believe they have to decline consent twice.

Table 1: Legal requirements for valid consent

Requirement	Description
Prior	A user should give their consent before their personal data can be collected and processed.
Informed	A user should be informed about how her data are processed before consent is collected.
Freely given	A user should be presented with a genuine choice and should be able to refuse or withdraw their consent at any time.
Specific	A user should be able to give consent for each specific purpose of the data processing.
Unambiguous	It must be evident, e.g., through an active motion or declaration, that a user wanted to give their consent.
Revocable	A user should be able to revoke consent at any time. The way consent is withdrawn should mirror the way it is given.

Consent is specific when the cookie banner allows the user to give consent for independent and specific purposes of the processing. A cookie banner that offers the user the option to give consent on a vendor or category basis, would be in violation of the requirement for specific consent.

Informed consent entails providing the user with clear and comprehensive information regarding the processed data, as well as the purposes and methods of expressing their consent. This ensures that the user understands the implications of any consent they may give. The first layer of the cookie banner must provide a minimal information notice that informs the users of the use of cookies or other tracking tools and the purposes of the processing, e.g., sending advertisements and/or customizing services and a link to the privacy policy or cookie policy that should be compliant with Art. 13 of GDPR. This article outlines the specific details that must be given to users when collecting data, including the identity and contact details of the data controller, the processing objectives, the recipients of personal data, the duration of data retention, and the user's rights to access information related to the processing. Hence, a cookie banner that fails to clearly state the processing purpose and lacks a link to the comprehensive privacy policy is in violation of the informed consent requirement.

Additionally, Art.7 states that data controllers should be able to demonstrate that the user has consented to the processing of personal data. The user should also be able to *withdraw consent* at any given time, and *withdrawing* consent should be as *easy* as giving it. This means that the cookie banner should allow users to return to the 'cookie settings' page where they can withdraw consent by a means of small hovering and permanently visible icon or a link placed in a visible and standard place.

3 RELATED WORK

In this section, we review the works that investigated tracking in mobile apps and the compliance of cookie banners with data protection laws.

Tracking in Mobile Apps. A large body of literature has investigated the prevalence of trackers in mobile applications. Existing works mainly differ in the approach adopted to detect tracking in mobile apps: *static analysis* and *dynamic analysis*. Static analysis focuses on scrutinizing the code of an app to identify trackers, whereas dynamic analysis involves examining network traffic to extract the third-party tracker domains with which the apps interact. Binns et al. [4] used static analysis of the app code to identify references to third-party hosts related to tracking companies in one million Android apps. They found that news and games apps were amongst the worst in terms of the number of tracker hosts. Kollnig et al. [12] adopted a similar methodology to study the presence of tracking in two million Android apps from before and after GDPR came into effect. Their analysis showed that there has been limited change in tracking practices of mobile apps after the introduction of GDPR. The works in [13, 17], instead, used dynamic analysis to detect tracking domains in iOS apps [17] and Android apps [13]. They found that the most commonly contacted domains belong to Alphabet, the parent company of Google. The study reported in [15] combined the strengths of both analyses to detect trackers in 24k Android and iOS apps. Their results show that both Android and iOS apps widely communicate with domains categorized as third-party trackers related to Alphabet. Similar to the studies reported in [13, 17] we adopted dynamic analysis to identify the most prevalent third-party tracker domains. Nevertheless, the studies mentioned earlier identify tracker domains without directly considering the consent mechanism employed by mobile apps. It is important to note that accepting or rejecting consent can potentially influence the set of third-party tracker domains that mobile apps interact with. Therefore, in our study, we detect the top third-party tracker domains both when users provide affirmative and negative consent to being tracked. This approach minimizes the risk of overlooking third-party tracker domains that are contacted exclusively when positive consent is granted.

Studies on Cookies Banners Compliance. Numerous studies have concentrated on detecting potential legal infringements in the implementation of websites' cookie banners and the enforcement of user consent. A significant number of studies [10, 23, 24] have specifically targeted the identification of *dark patterns* in the design of cookie banner interfaces, which subtly influence users to accept tracking. Additionally, research has been conducted to assess the impact of these dark patterns on users' consent decisions [11, 18]. However, the analysis of legal violations in mobile apps' cookie banner design has received limited attention. The only work we are aware of is the one from Kollnig et al. [13] that investigated the extent to which consent is implemented in Android mobile apps. They analyze the network traffic generated by mobile apps before and after consent is given to identify the apps that lack consent mechanisms to legitimize third-party tracking. The researchers found that a small percentage of Android apps requested user consent, and the majority of these apps employed tactics that coerced users into granting consent. In contrast, our study not only seeks to examine whether mobile apps solicit user consent but also assesses the legal compliance of the apps' consent mechanisms in relation to the requirements for valid consent outlined in the ePD and GDPR.

4 METHODOLOGY

The aim of our study is to investigate the use of third-party tracking technologies in mobile applications in relation to valid consent. In particular, we investigate the following research questions:

RQ1 *Do mobile apps' cookie banners comply with the ePrivacy Directive and GDPR's requirements on valid consent?*

RQ2 *Do mobile apps ensure that user consent for tracking is enforced?*

RQ3 *What are the most prevalent third-party tracker domains contacted by mobile apps?*

In this section, we discuss the methodology used for our study. This includes how we selected the mobile apps to be analyzed, what data we collected about the apps, and how we performed data analysis.

4.1 App Selection

The study was conducted from March to December 2022. The first step was constructing a corpus of mobile applications that meet the following criteria: (1) the application must be popular, i.e., it has a high number of downloads (2) it must be downloadable in the EU; (3) it must be available both for Android and iOS; and (4) it must be free of charge. We imposed the first criterion because we wanted to consider mobile apps that have an impact on a large scale. The second criterion restricts our analysis of mobile applications that have to comply with the ePD and GDPR requirements on valid consent. We impose the third criterion because, similarly to other studies [7, 15], we wanted to analyze applications that exist on both platforms. The last criterion was imposed to simplify the interaction with the applications.

To search for candidate applications, we used the Google Play scraper [2] to download information about the first 400 most installed free Android mobile apps available for download within the EU between April and June 2022. For each app, the scraper returns several information including the app's name, a short description, the developer, the app category, the number of downloads, and the link to the privacy policy. Then, for each Android mobile app returned by the scraper, we manually investigated if there was a version of the app for iOS and if the app had a high number of downloads. The final dataset contained a total of 400 mobile cross-platform apps: 200 Android apps and their corresponding version for iOS.

4.2 Data Collection

To download the selected apps, we created three accounts: a Google account and an Outlook account for downloading apps from the Google Play Store, and an Apple ID for downloading iOS apps. Apps were installed and run one at a time for a few minutes. Android apps were run on an Oppo X3 Lite running Color OS 12.1 and iOS apps on an iPhone 8 with iOS 15.5.

To determine whether the apps obtain valid consent before tracking users, we took screenshots of the cookie banner displayed by the app when run for the first time. Then, we performed *dynamic*

Table 2: Cookie banner Analysis Questionnaire

	Requirements	Questions
1	Prior	Q_1: Is a cookie banner shown to the user when the app is run for the first time?
2	Informed	Q_2: Does the short information notice on the first layer of the banner mention the app uses cookies or other tracking tools? Q_3: Does the short information notice on the first layer of the banner specify the purposes of the processing? Q_4: Does the short information notice on the first layer of the banner contain a link to the privacy policy and/or to the cookie policy?
3	Freely given	Q_5: Does the cookie banner interface only give the option to accept all cookies? Q_6: Does the banner force the user to give consent to use the app?
4	Specific	Q_7: Does the banner allow to give consent for a specific purpose? Q_8: Does the banner have a customization setting page on the second layer? Q_9: Does the customization settings page allow to give consent only on a third-party or cookie category basis or both?
5	Unambiguous	Q_{10}: Is denying the use of all tracking tools as easy as accepting all? Q_{11}: Is the "Accept all" option emphasized with respect to the "Reject all" option? Q_{12}: Does the second layer of the banner use pre-selected sliders or pre-ticked boxes? Q_{13}: Are the boxes or sliders labeled with accept/deny? Q_{14}: Does the second layer of the banner use legitimate interest as the legal basis for tracking?
6	Revocable	Q_{15}: Does the banner contain a link to revoke the consent on the first layer? Q_{16}: Is revoking consent as easy as giving it?

analysis, which involves capturing the network traffic generated by the apps while in use and identifying the third-party tracking domains contacted by the apps. Then, based on the contacted domains, we determined whether the user's consent was violated. To this end, we first captured the network traffic after manually granting consent on the cookie banner, and after we denied the consent through the application settings. To record the network traffic, we used a different approach on Android and iOS.

Dynamic Analysis on Android. On Android, we used Tracker Control [14], a mobile app that reports the third-party tracking domains contacted by an app and the associated company. To detect third-party tracking domains, TrackerControl relies upon the Disconnect List [1] distributed with Firefox, the X-Ray dataset [4], and Steven Black's Blocklist [5]. We first run Tracker Control, and then we launched the app we wanted to analyze for five minutes and then we exported the report of the contacted third-party tracking domains.

Dynamic Analysis on iOS. Since Tracker Control is only available for Android, we had to resort to a different approach to capture the network traffic of iOS apps and identify the contacted third-party tracking domains. We used Ettercap [3] to redirect the network traffic generated by the iPhone 8 to a Dell Inspiron 15 with Intel core i5, 16GB of RAM, and 500GB of disk space. Once redirect the traffic, we relied on Wireshark [21] to capture the iPhone 8's network traffic. We recorded the network traffic after granting consent, and then after denying the consent through the app settings. In both cases, the network traffic was saved in a pcap file. Then, for each pcap file we filtered the Client Hello packets related to the start of the handshake phase of the TLS protocol where the source IP address was equal to the one of the iPhone 8. From the Client Hello packets we extracted the Server Name Indication field that specifies the hostname the phone tries to communicate with. Since not all contacted domains are third-party tracking domains, for each of them, we manually checked if it was included in the same dataset used by Tracker Control.

4.3 Data Analysis

In this section we describe the type of analysis we performed on the cookie banners and the third-party tracking domains.

Valid Consent. As discussed in [22], violations of the requirements on valid consent can only be detected via a manual analysis of the cookie banners. Therefore, to perform a systematic analysis of the cookie banner's screenshots concerning the ePD and GDPR requirements on valid consent, we developed an analysis template. For each requirement in Table 1, the template includes a set of questions that captures the cases of violation of the requirements that were discussed in Section 2. The questions have been formulated based on the study of the literature on valid consent. In particular, our analysis template consider the ePD's Article 5(3), Articles 4(11), 7(2), 7(3), 7(4) of the GDPR, EDPB guidelines 05/2020 on valid consent [6], DPA guidelines [20], and other research papers [19, 22, 24] that have analyzed cookie banners' legal compliance. The full list of questions is reported in Table 2. All questions are binary, which means the only possible answers are "yes" or "no". A violation occurs when the answer to at least one of the questions Q_5, Q_6, Q_{11}, Q_{12}, Q_{14} is positive ("yes"), or when the answer to one of the remaining questions is negative ("no"). A mobile app violates a requirement when the answer to at least one of the corresponding questions represents a violation.

To facilitate the recording of the answers, we implemented the analysis template in Google Forms. The analysis of the cookie banner provided by each selected app was performed by two of the authors independently. Any disagreement in the analysis was reconciled using a discussion among the authors who collaboratively decided how to revise the answers. Once completed the analysis, for each case of violation of the requirements in Table 2, we computed the percentage of Android and iOS apps that presented the violation.

Enforcing User Consent. To assess whether a mobile app enforces the consent given by the users, we analyzed the network traffic generated by the apps. We considered a violation of user consent when a mobile app contacts third-party tracking domains after consent to

Table 3: Percentage (%) of Android and iOS apps that violate requirements on valid consent

Requirement	Android	iOS	Android & iOS	Total
Prior	50.5%	40.0%	32.5%	45.25%
Informed	32.0%	45.5%	25.5%	38.75%
Freely Given	48.5%	60.0%	42.0%	54.25%
Specific	49.5%	60.0%	42.0%	54.75%
Unambiguous	44.0%	36.0%	32.0%	40.00%
Revocable	54.0%	64.5%	48.0%	59.25%
Total	100%	100%	100%	100%

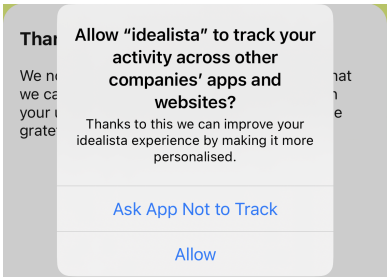

Figure 1: Apple Tracking Transparency Authorization banner

be tracked was denied. We computed the percentage of Android and iOS apps that do not respect the choice of the user to not be tracked.

Prevalent Third-party Tracker Domains. Based on the network traffic generated by the mobile apps, we identified the top third-party tracking domains contacted by mobile apps *both* after the consent to be tracked was granted and after the consent was withdrawn. We considered top domains the ones that were present in at least 5% of mobile apps' network traffic. For each third-party tracking domain, we determined the company behind that domain using the X-Ray dataset. We also computed the average number of third-party tracking domains contacted by Android and iOS mobile apps.

5 RESULTS

In this section, we discuss the results we obtained for each of our research questions.

5.1 Valid Consent

Table 3 reports the results on the compliance of the selected mobile apps' cookie banners with the requirements on valid consent imposed by ePD and GDPR. In particular, the first column (*Android*) reports the percentage of non-compliant Android apps, and the second column (*iOS*) the percentage of non-compliant iOS apps. The third column (*Android & iOS*) reports the percentage of apps for which both the Android and iOS version of the app is not compliant with the requirements. The last column (*Total*) reports the percentage of the selected apps that are not compliant. The last row reports the percentage of apps that violate at least one of the requirements for valid consent. We can observe that every app on Android and iOS apps fails to meet at least one requirement, indicating that none of the analyzed apps fully comply with privacy regulations on valid consent. Specifically, a significant number of apps do not comply with the requirements regarding revocable, specific, and freely given consent. Notably, the percentage of iOS apps that violate these requirements is higher than the one of Android apps.

Prior Consent. We found that 45.25% of the considered apps violate the prior consent requirement because they do not present a cookie banner that informs users about the use of tracking technologies and allows them to grant or deny consent to be tracked. The requirement is violated slightly more by Android apps (50%) than by iOS apps (40%). Regarding iOS apps, we found that 55% of the non-compliant apps adopted the Apple Tracking Transparency (ATT) feature (see Fig. 1), which prompts the user with an authorization request to track user activity for the purposes of advertising or sharing with data brokers. In the event that the user opts out of tracking, the app developer is unable to obtain access to the system advertising identifier (IDFA), commonly utilized for tracking purposes. Moreover, the app is prohibited from tracking user activities using other identifiable information such as email addresses. We also observed that 31.6% of the iOS apps that are compliant with the prior consent requirement presented users with both the ATT's authorization request and a cookie banner to request consent to track user activities across apps and websites.

Informed Consent. Our analysis shows that 38.75% of the considered apps violated the informed consent requirement with more iOS apps (45.5%) than Android apps (32%) not complying with this requirement. The main violation we found is that the cookie banners do not provide a link to the apps' privacy policy and/or cookie policy (56,5% of total apps, 38% of iOS apps, and 18.5% of Android apps).

Freely Given Consent. More than half of apps (54.25%) do not comply with the freely given consent requirement. Specifically, 60% of iOS apps and 48.5% of Android apps violate this requirement. The primary reason for the violation is that apps use a cookie wall, whereby consent is a prerequisite to use the apps. Indeed, 58.5% of apps on iOS and 47% of Android apps require users to give consent in order to use the apps. The second reason is that half of the apps (23%) have a cookie banner interface of type "Only Accept", which does not provide a "Reject All" option.

Specific Consent. Our analysis reveals that 54.75% of the examined apps do not comply with the specific consent requirement. Notably, a larger number of iOS apps (60%) violate the requirement compared to Android apps (49.5%). The primary reason behind this discrepancy is the presence of a "Cookie Settings" page within the cookie banner interface that allows users to make a granular choice but not for specific purposes of the processing. In fact, 49% of iOS apps and 48.5% of Android apps feature a "Cookie Settings" page that allows users to give consent on a vendor or category basis (see Fig. 2).

Unambiguous Consent. A considerable proportion of applications (42% of total apps, 47% of Android apps, and 37% of iOS apps) fail to comply with the unambiguous consent requirement. This non-compliance stems from the use of one or more dark patterns within the apps' cookie banner interface, which exerts undue influence on users to provide affirmative consent. The most prevalent dark pattern observed is that in cases where the cookie banner interface incorporates sliders to enable user consent, the sides of the sliders

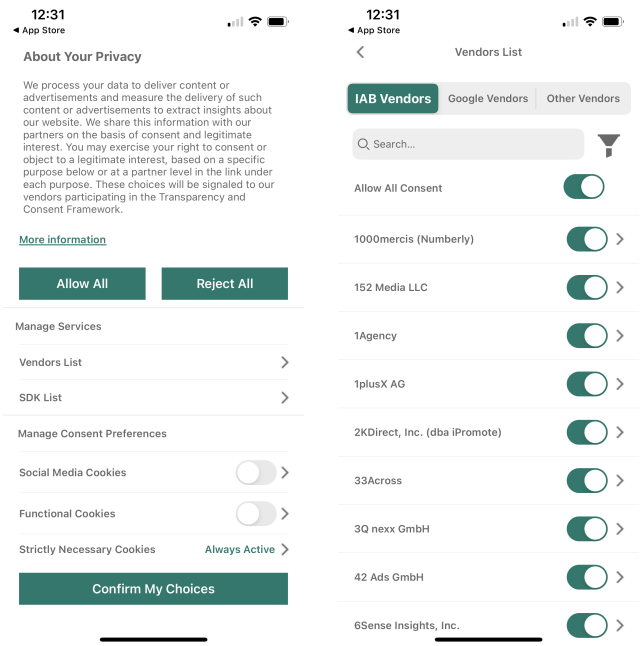

Figure 2: Example of cookie banner not compliant with specific and unambiguous consent requirements

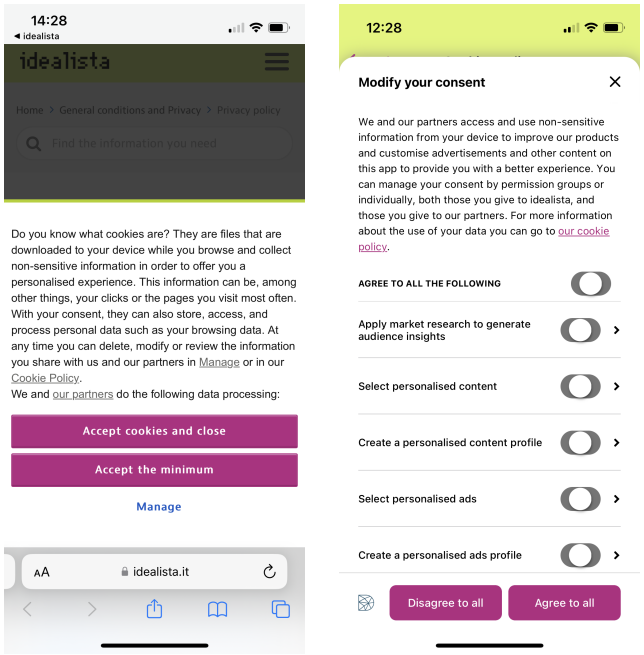

Figure 3: Example of cookie banner not compliant with unambiguous consent requirement

are not appropriately labeled with terms such as "accept/on/active" and "reject/off/inactive". Another commonly observed pattern is that granting consent is typically easier than refusing it. This holds for both Android and iOS platforms, where the average number of clicks needed to reject all cookies is 2. In other words, the option to "Reject All" cookies is typically found within the cookie settings page of the banner. An illustrative example of such an interface can be seen in Fig. 3, showcasing the interface of the "idealista" app. We also observed that the "Accept All" option is emphasized over the "Reject All" option. All these patterns are slightly more prevalent in Android apps than in iOS apps.

Revocable Consent. This is the requirement most commonly violated by the apps in our dataset (59.25%). In particular, fewer iOS apps (64.5%) comply with this requirement compared to Android apps (54%). The primary violation we identified is the absence of a link or a button that allows users to reopen the banner and revoke their consent using the same interface they initially used to give consent. As a consequence, withdrawing consent is not as easy as giving consent. In fact, the average number of clicks to withdraw consent is 4. This means that a user to withdraw consent must first click on the user's profile tab of the app, then on app settings, on the cookie settings tab, and lastly on the button to deny consent.

5.2 Enforcing Users' Consent

The analysis of the network traffic shows that almost half of the analyzed apps did not properly enforce the consent given by the user. Specifically, 45.75% of the apps contacted third-party tracker domains when the user has not given consent to be tracked. A breakdown per platform shows that the violation occurred in 47% of the Android apps and 44.5% of the iOS apps. In the next section, we investigate the most common tracker domains.

5.3 Prevalent Third-party Tracker Domains

Fig. 4 shows the most common tracker domains the analyzed apps on Android and iOS communicated with when the user has given consent to be tracked. The most popular domain on Android was `content-autofill.googleapis.com`, which is related to the Autofill service of Google.[1] In particular, this domain was contacted by 63% of Android apps. Other common domains on Android were `firebaseinstallations.googleapis.com` (contacted by 51% of the apps) and `graph.facebook.com` (contacted by 38.5% of the apps). On the other hand, the most popular domain on iOS was `inappcheck.itunes.apple.com`, which was contacted by 35.5% of iOS apps. This domain is unique to iOS. The second most contacted domains were `app.measurement.com` (22%), which is related to Alphabet's analytics services, and `graph.facebook.com` (19%), which is related to the Facebook social network. In general, we noticed that on Android, the majority of popular domains were associated with Alphabet analytics and fingerprinting services, whereas on iOS, the majority of popular domains were associated with advertising services provided by AppsFlyer. When analyzing the average number of tracker domains that apps on both platforms communicate with, Android apps were observed to interact with an average of 13.54 domains, while iOS apps communicated with an average of 8.14 domains. This means that the average app on Android contacts more third-party tracker domains than the average app on iOS.

[1]The Autofill service of Google automatically fills in usernames and passwords to facilitate app access.

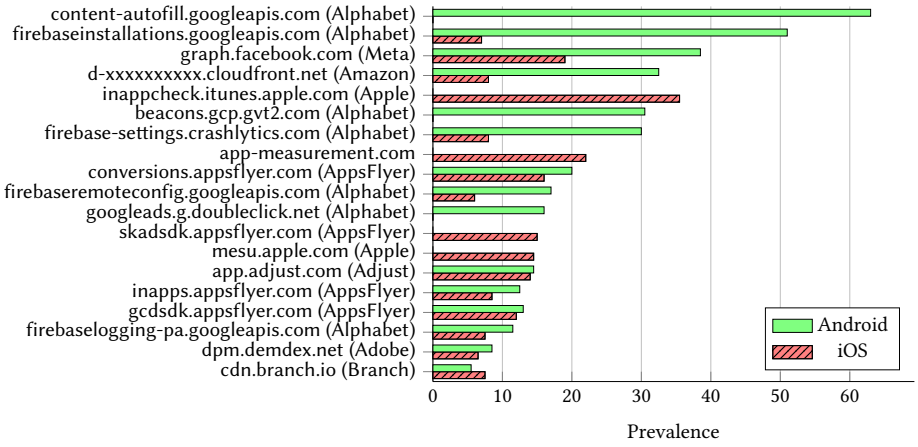

Figure 4: Prevalent Third-Party Tracker Domains After Consent is Granted

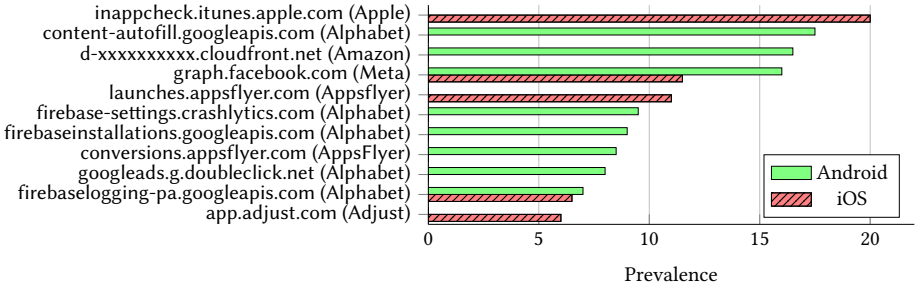

Figure 5: Top Third-Party Tracker Domains After Consent is Denied

As noted in Section 5.2, almost half of the analyzed apps on both platforms still contact third-party tracker domains even after users have explicitly denied consent for tracking. Upon analyzing the network traffic generated by the apps when consent was denied, it was observed that the group of third-party tracking domains contacted remained similar to the set of domains contacted when consent was granted. As shown in Fig. 5, the most contacted tracker domain on Android (17.5% of the apps) is still `content-autofil.googleapis.com`. Similarly, the most popular domain on iOS (20% of the apps) is `in-appcheck.itunes.apple.com`. The average number of third-party tracker domains contacted on both platforms slightly decreased (Android is 8.64 compared to 5.52 on iOS) with respect to when consent was granted.

5.4 Limitations

In this section, we discuss the limitations of our empirical study. First, our dataset comprises 400 mobile apps available for download on Google Play Store and iOS App Store. This choice was dictated by the type of analysis that we performed. To detect whether the cookie banners of mobile apps are compliant with ePD and GDPR requirements, two researchers independently had to manually examine the cookie banner interface. Currently, due to the absence of standardized cookie banner designs, it is not feasible to fully automate the verification of these requirements. However, our analysis resulted in a smaller, and richer dataset, and allowed us to detect violations present in the implementation of cookie banners that cannot be easily automatically detected. Similarly, the dynamic analysis of the network traffic could not be fully automatized. This was necessary to avoid the risk of incorrectly attributing contacted tracker domains to a specific app, as they could have been contacted by a different app on the mobile phone. To reduce this risk, we implemented a procedure where we installed and run the app one by one. Second, we only run the apps for a few minutes where the user interaction was limited to granting or denying consent through the cookie banner interface. However, mobile apps might have contacted more tracker domains if used for a prolonged period of time. Therefore, we could have under-reported the extent of contacted third-party trackers. Another limitation concerns the ability to generalize our results beyond the study settings. We addressed this limitation by choosing mobile apps that are popular and that belong to different app categories.

6 DISCUSSION AND FUTURE WORKS

We analyzed different aspects related to the use of third-party trackers by Android and iOS apps. In particular, we detected potential violations of ePD and GDPR requirements on valid consent in the implementation of mobile apps cookie banners and violations in the enforcement of the consent given by users on being tracked. Moreover, we identified the most common third-party tracker domains contacted by mobile apps on both platforms. Our analysis shows that the use of third-party trackers is extensive on both Android and iOS platforms, although there are differences. Android apps predominantly establish connections with domains associated with analytics and fingerprinting services offered by Alphabet, the

parent company of Google. Conversely, on iOS, the most frequently contacted domains are related to advertising services provided by AppsFlyer. We also observed that Android apps contacted on average a higher number of tracker domains than iOS apps. Regarding the validity of consent obtained by mobile apps, we found that all mobile apps violated at least one requirement for valid consent with the percentage of non-compliant iOS apps being higher than the one of Android apps. The most violated requirements were the revocable, specific, and freely-given consent. The non-compliance arises from inherent flaws in the design of the cookie banner interface. These include the inability to provide consent for specific purposes, the absence of a "Reject All" option on the initial layer of the banner, and the omission of a link or a button that would allow users to reopen the banner and withdraw their consent.

A possible explanation for these widespread violations is that the responsibility of implementing cookie banners and enforcing users' consent falls into the hands of app developers who lack legal expertise and receive limited support from tracker companies on how to implement a compliant cookie banner [13].

To address the uncovered violations related to the use of third-party trackers, platform-level support should be given to standardizing the implementation of cookie banners and of the enforcement of the consent obtained through the banners. A step in this direction has been done by Apple, which since iOS version 14.5 has introduced new privacy features to increase transparency and user control over personal data that are shared with third-party trackers: the App Tracking Transparency, Privacy Nutrition labels, and Privacy Report. App Tracking Transparency enables users to grant authorization to apps for the collection of their personal data, which can then be shared with other companies for the purpose of tracking across various apps and websites. Privacy Nutrition Labels, instead, use graphical icons to make it easier for end-users to understand apps' data collection and processing practices, while Privacy Report shows users the domains that apps communicated with. However, these new additions might be misleading because they can give users a false sense of privacy [16]. For example, our analysis has shown that more than half of iOS apps being non-compliant with prior consent, prompted users with an App Tracking Transparency authorization request before engaging in third-party tracking. However, the App Tracking Transparency prompt does not in any way constitute valid consent under GDPR. Therefore, as shown by our analysis, app vendors are forced to prompt users with a second cookie banner further contributing to "Consent Fatigue".

In future work, we are planning to conduct an empirical study to analyze the effectiveness of the Privacy Report and App Tracking Transparency feature in increasing transparency over users' personal data shared with third-party trackers and enforcing users' permissions on being tracked. In particular, we want to evaluate if the Privacy Report feature gives a faithful report about the extent to which iOS apps communicate personal data with third-party trackers and whether mobile apps contact third-party trackers even when permission has been denied through the App Tracking Transparency prompt. We also want to conduct a user study to evaluate users' perception of the Privacy Report and App Tracking Transparency features and how these features impact users' choices regarding tracking.

REFERENCES

[1] 2023. Disconnet List. https://github.com/mozilla-services/shavar-prod-lists Accessed on May 30, 2023.

[2] 2023. Google Play Scraper. https://github.com/facundoolano/google-play-scraper.

[3] Emilio Escobar Alberto Ornaghi, Marco Valeri. 2023. Ettercap. https://www.ettercap-project.org/ Accessed on March 24, 2023.

[4] Reuben Binns, Ulrik Lyngs, Max Van Kleek, Jun Zhao, Timothy Libert, and Nigel Shadbolt. 2018. Third Party Tracking in the Mobile Ecosystem. In *Proceedings of the 10th ACM Conference on Web Science (WebSci '18)*. 23–31.

[5] Steven Black. [n. d.]. Steven Black's Blocklist. https://github.com/StevenBlack/hosts Accessed on May 30, 2023.

[6] European Data Protection Board. [n. d.]. Guidelines 05/2020 on consent under Regulation 2016/679. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf Accessed on March 24, 2023.

[7] Kai Chen, Xueqiang Wang, Yi Chen, Peng Wang, Yeonjoon Lee, XiaoFeng Wang, Bin Ma, Aohui Wang, Yingjun Zhang, and Wei Zou. 2016. Following Devil's Footprints: Cross-Platform Analysis of Potentially Harmful Libraries on Android and iOS. In *IEEE Symposium on Security and Privacy*. 357–376.

[8] European Commission. 2002. Directive 2002/58/EC of the European Parliament. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

[9] European Commission. 2016. Regulation (EU) 2016/679 of the European Parliament (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj

[10] Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, and Christo Wilson. 2021. A Comparative Study of Dark Patterns Across Web and Mobile Modalities. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW2 (2021).

[11] Hana Habib, Megan Li, Ellie Young, and Lorrie Cranor. 2022. "Okay, Whatever": An Evaluation of Cookie Consent Interfaces. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*.

[12] Konrad Kollnig, Reuben Binns, Max Van Kleek, Ulrik Lyngs, Jun Zhao, Claudine Tinsman, and Nigel Shadbolt. 2021. Before and after GDPR: tracking in mobile apps. *Internet Policy Review* 10, 4 (2021).

[13] Konrad Kollnig, Pierre Dewitte, Max Van Kleek, Ge Wang, Daniel Omeiza, Helena Webb, and Nigel Shadbolt. 2021. A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps. In *Symposium on Usable Privacy and Security (SOUPS 2021)*. 181–196.

[14] Konrad Kollnig and Nigel Shadbolt. 2022. TrackerControl: Transparency and Choice around App Tracking. *Journal of Open Source Software* 7, 75 (2022), 4270.

[15] Konrad Kollnig, Anastasia Shuba, Reuben Binns, Max Van Kleek, and Nigel Shadbolt. 2021. Are iPhones Really Better for Privacy? A Comparative Study of iOS and Android Apps. *Proceedings on Privacy Enhancing Technologies* 2022 (2021), 6 – 24.

[16] Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns, and Nigel Shadbolt. 2022. Goodbye Tracking? Impact of IOS App Tracking Transparency and Privacy Labels. In *2022 ACM Conference on Fairness, Accountability, and Transparency (FAccT '22)*. 508–520.

[17] Brian Krupp, Joshua Hadden, and Malik Matthews. 2021. An Analysis of Web Tracking Domains in Mobile Applications. In *Proceedings of the 13th ACM Web Science Conference 2021 (WebSci '21)*. Association for Computing Machinery, 291–298.

[18] Oksana Kulyk, Annika Hilt, Nina Gerber, and Melanie Volkamer. 2018. "This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer. In *3rd European Workshop on Usable Security (EuroUSEC)*.

[19] 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 *IEEE Symposium on Security and Privacy (SP)*.

[20] Garante Privacy. 2021. Guidelines on the use of cookies and other tracking tools. https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9677876#english Accessed on March 24, 2023.

[21] Ulf Lamping Richard Sharpe, Ed Warnicke. [n. d.]. Wireshark. https://www.wireshark.org/ Accessed on March 24, 2023.

[22] Cristiana Santos, Nataliia Bielova, and Célestin Matte. 2019. Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. *CoRR* abs/1912.07144 (2019).

[23] 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 Workshop on Privacy in the Electronic Society (WPES '21)*. 187–194.

[24] Than Htut Soe, Oda Elise Nordberg, Frode Guribye, and Marija Slavkovik. 2020. Circumvention by Design - Dark Patterns in Cookie Consent for Online News Outlets *(NordiCHI '20)*. 12 pages.