"Developers are Responsible": What Ad Networks Tell Developers About Privacy

"Developers Are Responsible": What Ad Networks Tell Developers About Privacy

Mohammad Tahaei
mohammad.tahaei@ed.ac.uk
School of Informatics
University of Edinburgh

Kami Vaniea
kami.vaniea@ed.ac.uk
School of Informatics
University of Edinburgh

ABSTRACT

Advertising networks enable developers to create revenue, but using them potentially impacts user privacy and requires developers to make legal decisions. To understand what privacy information ad networks give developers, we did a walkthrough of four popular ad network guidance pages with a senior Android developer by looking at the privacy-related information presented to developers. We found that information is focused on complying with legal regulations, and puts the responsibility for such decisions on the developer. Also, sample code and settings often have privacy-unfriendly defaults laced with dark patterns to nudge developers' decisions towards privacy-unfriendly options such as sharing sensitive data to increase revenue. We conclude by discussing future research around empowering developers and minimising the negative impacts of dark patterns.

CCS CONCEPTS

• **Security and privacy** → **Human and societal aspects of security and privacy**; • **Software and its engineering** → *Software creation and management*; • **Information systems** → **Online advertising**.

KEYWORDS

software developers, usable privacy, ad networks

ACM Reference Format:
Mohammad Tahaei and Kami Vaniea. 2021. "Developers Are Responsible": What Ad Networks Tell Developers About Privacy. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts (CHI '21 Extended Abstracts), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3411763.3451805

1 INTRODUCTION

Mobile ads are one of the most popular models of monetising apps [2, 3, 18, 25, 43], about 77% of free Android apps contain an ad library [19, 22]. With about 3 million apps in the Google Play Store alone [42], ad networks collect massive amounts of data about users on a daily basis. Developers who build these apps may be able to decide what to include or exclude in their apps, but these decisions are not always fully informed, and developers tend to pick the default options provided by the ad networks ("status quo bias") potentially endangering user privacy [30].

Developers may have privacy concerns for users and look for options that can protect user privacy [11, 45, 48, 50]. For example, when given the option, developers chose coarse over fine grain location information [21]; suggesting that developers do consider privacy. Other developers, though, may just use "industry standard" content provided by large companies which may not be in the best interest of users [11]. Ad networks' documentation is also one of the primary resources of developers when choosing an ad network [30], making presented information particularly important. To understand the default ad networks' configurations and what privacy-related information they provide to developers which can effect developers' choices and consequently user privacy, we conducted a study with a usable security and privacy researcher and a senior Android developer who reviewed the quick start guides and linked information, of four popular ad networks. We find that most of the privacy information presented is framed around legal compliance, casting developers as the responsible entity—which contradicts developers' view that ad networks are responsible for user privacy [30]. The information is also provided in a variety of places sometimes on the main path or included in the libraries by default and sometimes linked from hard-to-notice places which makes finding the information highly inconsistent between ad networks.

2 BACKGROUND

Although developers acknowledge the value of user privacy, they find it difficult to understand what information is collected and how it is addressed by platforms [11]. Furthermore, developers' user privacy attitudes and actions may contradict; while they may say that they care about user privacy, their decisions and final app may not be privacy favourable [30]. Developer concerns about privacy are reflected in questions they ask on Stack Overflow [48], and given the options, they pick more privacy-preserving alternatives [21]. Developers tend to follow guidelines and requirements provided by the platforms [38, 48]. Our study primarily focuses on the available privacy guidelines for developers in ad networks, as one of the main resources for choosing an ad network [30].

Android developers must request for permissions from the operating system, and sometimes the user, to access certain resources. These permissions are defined by the developer in a manifest file `AndroidManifest.xml` [8]. Permissions could be "normal permissions" like "time zone" that do not require user consent, or "dangerous permissions" such as access to contacts, location, and read/write messages that requires explicit user consent [9, 41]. Permissions requested by the app are shared within the project, and libraries

CHI '21 Extended Abstracts, May 8–13, 2021, Yokohama, Japan

ACM ISBN 978-1-4503-8095-9/21/05…$15.00
https://doi.org/10.1145/3411763.3451805

do not need to ask for second permission from the user or the developer to access shared resources [36, 40]. Third-party libraries not only collect data in free apps but also from paid apps [4, 18], opening up the question of why developers make such choices? Our study expands ad network literature by studying developer-facing privacy information and options in ad networks.

Dark patterns are "instances where designers use their knowledge of human behavior (e.g., psychology) and the desires of users to implement deceptive functionality that is not in the user's best interest" [17, p. 1]. Some common dark patterns are (1) *nagging*: when an interface interrupts user workflow consistently and asks for a certain action from them, (2) *preselection*: values set to defaults that are in the best interest of the provider prior to user interaction, (3) *aesthetic manipulation*: graphical elements used to deceive the user into taking an action that may be in favour of service provider rather than the user, (4) *forced action*: users are given only one option to follow even if that is not what they prefer to do, (5) *toying with emotion*: elements, colours, or language to provoke user's emotion to get user make a decision that is in favour of the service provider, and (6) *false hierarchy*: options that are in the best interest of the service provider are in higher positions [17]. As such patterns become prevalent in the digital world [5, 6, 10, 12, 13, 17, 27, 31, 32, 51], we are keen to explore the presence of them in tools and libraries that developers use, specifically, in ad networks.

3 METHOD

We conducted a walkthrough with two reviewers (similar to a pair-programming activity) of four highly popular Android ad networks [1]: *Google AdMob (GAM)*, *Amazon Mobile ad network (AMN)*, *Facebook Audience Network (FAN)*, and *Twitter MoPub (TMP)*. Reviewers started by searching for "[ad library's name] Android." on Google which is one of the primary tools developers use to find information [29]. Doing so produced the official guidance on how to integrate the library into an app for all four ad networks. This guidance was then accessed and followed to integrate interstitial ads into a hypothetical app, including creating an account. While stepping through the guidance, the reviewers noted any material provided that related to privacy as well as any links to other materials that might be privacy-related which were then visited later. The two reviewers discussed all material as they went through it and agreed on the observations. All websites were visited on a Firefox v79.0 with a UK-based IP address in August 2020. In total, we spent 15.5 hours on the four ad networks; 6 hours on GAM, 3 hours on AMN, 2.5 hours on FAN, and 4 hours on TMP. GAM took most of the time since it had the most materials.

Privacy. In advance of the review, the researcher reviewed prior work on how developers think about privacy on Stack Overflow [48], an ad networks study with developers [30], and in the privacy by design framework [20]. Developers tend to associate privacy with permissions, data collection and management, information disclosure, privacy policies, and laws and regulations associated with privacy such as the General Data Protection Regulation (GDPR) [35], California Consumer Privacy Act (CCPA) [34], and Children's Online Privacy Protection Act (COPPA) [7].

Reviewers. A *researcher* with four years of experience in usable security and privacy research and four years of experience in software engineering, and a senior software engineer who we will call *Abi* who has a computer science degree and 11 years of experience in Android development, went through all the content. Abi has written over 40 apps for corporations that have users from hundreds to millions, creates online Android programming video tutorials, and is fluent in Java. Because he develops apps for corporations, he had not previously worked with ad networks and was, therefore, able to look at the pages with experienced, but fresh, eyes.

Limitations. Both Abi and the researcher have extensive experience in their respective fields, reducing the chances of missing the relevant information. However, we note that the results are not generalisable to all developers and ad networks. We focused on the developer-facing information and did not go through the legal documents, terms of services, and privacy policies. We are not aware of studies on developers behaviour when dealing with a privacy policy, but the general public's attitude towards privacy policies is to skip or spend less than 90 seconds reading them [33]. Notably, we conducted the study during COVID-19 pandemic when many businesses were either closed or doing remote work which may have impacted the resources that ad network companies spend on their documentation, websites, and guidelines.

4 FINDINGS

This section includes the information that was found in *guides*, linked-to content (*supplemental documentation*), and in the developer's *dashboard*. Section 4.5 consists of dark patterns that the research team found during discussions after reviewing the screenshots taken during the review procedure. Table 1 in the Appendix provides an overview of the available privacy information and where they are located, Appendix A shows the screenshots.

4.1 Google AdMob (GAM)

GAM provides developers with a clear step-by-step guide and also a consistently-visible sidebar with many links to other materials ranging from how to handle custom events to CCPA. We found the documentation easy to navigate with an everything-in-one-place tone to the user interface.

Guide. A step-by-step guide is included in *Get Started* page with videos, sample code, and some minimal explanation text. Privacy wise, it has a warning under initialising mobile ads about obtaining consent "from users in the European Economic Area (EEA)" and directs the developer to set request-specific flags such as "tagForChildDirectedTreatment" or take other actions before initialising the SDK because it may preload ads. None of the terms in the warning were linked (Figure 1).

Supplemental Documentation. GAM provides a fair amount of extra privacy-related information, most of which is linked directly off the sidebar. *CCPA Preparation* appears just below the "Get Started" and "Test Ads" items on the sidebar, so it is relatively prominent. It starts with a link to another set of instructions that explains CCPA and provides guidance on how to restrict data processing via the developer's account page. The CCPA Preparation page itself provides code examples of how to restrict data processing in code via either the Google RDP signal or the IAB ("consortium charged

with producing and helping companies implement global industry technical standards" [24]) signal. Notably, the Google option defaults to restricting data processing, but the IAB code example has only a placeholder and requires the developer to open IAB specifications to construct the parameter string. The in-code setting also overrides any setting in the developer's account page, which may be confusing to some.

The *EU Consent* option takes the user to the User Messaging Platform SDK which causes all the AdMob branding and sidebar to vanish. The page provides step-by-step instructions on how to use the SDK with many code examples. Notably, the SDK appears to handle user-facing messaging itself so developers cannot easily change it. The example code also puts user consent in a loop so if the user dismisses the popup, it just reloads (Figure 2). A comment in the code states: "Handle dismissal by reloading form." The *Precise Location Data Policy* page first links to *Google Publisher Policies* and notes that there are "notice and consent requirements for publishers who pass users' precise location data to Google, for ads-related purposes." Then provides sample code which asks the user for consent to use their location. There are several points about this code sample (Figure 3). First, Abi immediately spotted the "we may use your location . . . for the purposes of personalized advertising" which is misleading because the location data is definitely being used for this purpose. Second, the popup only provides an "OK" option. Third, the text provides a URL to "our" privacy policy that leads to a Chinese Android app market page. Presumably, the developer is meant to link to their own privacy policy which will explain how GAM will use location information. Though, we were unable to find any guidance about what a developer should write into such a policy. Fourth, Abi further pointed out that showing multiple popups that do not even belong to his app will annoy users and is the last thing he would do while building an app.

The sidebar also contains several pages on *Mediation* which is a GAM service that lets developers load ads from other ad networks through GAM. None of the sidebar options are obviously about privacy. However, information about GDPR and other regulations does appear in the instructions under "Optional steps" for some ad network partners. For example, the guidance for *Facebook Audience Network* discusses GDPR and CCPA but provides no example code. The guidance for both *AdColony* and *AdLovin* tells the developer that they are obliged to get user consent and then provides sample code that indicates that the user has given consent.

Dashboard. During account and app creation procedures, GAM encourages developers to share data with other Google services like Google Analytics and Firebase to "optimize your app's user experience and your ad revenue." These items are also preselected to maximum data sharing (Figures 4, 5, and 6). "Blocking controls" provides several privacy options such as sensitive categories, ad content rating, CCPA, EU user consent, and ad networks (Figure 8). Sensitive categories are all allowed by default using grey toggle switches (e.g. "References to Sex" and "Religion") except for "Gambling & Betting (18+)" which is blocked using a blue toggle switch. On the content rating page (Figure 7), the setting is set to "Mature Audiences" with a bar that allows developers to change the audiences to "Teens", "Parental Guidance," and "General Audiences." When trying to lower the setting, it provides a red box saying: "Est. impact of changing MA to PG: -29 to -57% impressions, -31 to -64% revenue . . ." Developers further can limit ads personalisation for California and European users (Figure 9). Defaults for these pages are set to "Don't restrict data processing," "Personalised ads," and use all common advertising partners. Under the ad networks page (Figure 10), a list of partners is shown with over 5,000 partners that GAM shares data with; they are all set to "allowed" with grey looking toggle switches. The only option that is set to on is "Automatically allow new Google-certified ad networks" with a blue toggle switch that does not have an "allowed" or "blocked" text like others. The funding choices, a service provide by GAM to assist developers in building a consent popup, includes two choice, the first choice does not include a "Do not consent" button, while the second nearly-identical choice does (Figures 11 and 12).

4.2 Amazon Mobile Ad Network (AMN)

AMN's top search result contained no step-by-step page and instead directed us to their main *Mobile Ads* page which had a "getting started" section of links. Going through the process of integrating the library involved pages that were filled with links to other pages, which in turn also contained many links. The number of pages necessary could easily be overwhelming to a developer.

Guide. We treat the "Get started" section on the *Mobile Ads* page as the guide. It contained four pages: download SDK, FAQ, account sign up, and publishing apps. To add ads to an app, all the pages except FAQ would need to be gone through, so technically FAQ could be skipped. However, the FAQ was the first thing Abi wanted to read in the hope that it will contain some useful information. He found all the provided links confusing and not related to "how to add an ad." Unlike the GAM pages, the AMN pages were very text-heavy and had no clear set of steps for developers to follow. Only the *FAQ* page contained any privacy-related information. The FAQ page had questions on CCPA, GDPR, monetizing EU traffic, managing what ads appear, geolocation from EU, and users' ability to opt-out of tailored ads. COPPA was also briefly mentioned in an answer. AMN does have a *Quick Start Guide* linked off of the FAQ page. However, its omission from the main Mobile Ads page and its low position on Google search make it unclear if AMN considers the page a primary entry point for developers. The page is a step-by-step guide to incorporating the API. It also contains information about how to optionally set up both coarse and fine grain location permissions to enable "relevant targeted ads" and points out that doing so will likely result in higher revenue (Figure 13).

Supplemental Documentation. AMN locates nearly all their privacy information on the FAQ page and directs developers elsewhere to find general information on the CCPA transparency framework and to find specifics about IAB standards and targeting options. The questions for CCPA says that "you can pass us the user choice signal via the instructions below so that we can honor that choice" and then provides a sample code that sets `us_privacy` to `1---` and says in the comment "example privacy string value." When we looked at the linked IAB documentation (Figure 14) we realised that "-" means "Not Applicable." The sample code also sets the location tracking on by `enableGeoLocation(true)` (Figure 15). The GDPR question only asks to set two flags for GDPR purposes without providing any other materials.

Dashboard. AMN provides a minimal set of privacy settings in the account page allowing developers to "Block Product Categories" where all the items are set to on by default (Figure 16). It also includes an option to "Include Ads From 3rd Party Networks" with a "Yes/No" radio button (default is set to "Yes") without giving a list of partners. These settings are located in a tab bar next to "My account," "Tax Identity," and "Company Profile."

4.3 Facebook Audience Network (FAN)

FAN's guidance was very prescribed with clear step-by-step instructions, lots of screenshots, and example code. Similar to GAM they had a consistent sidebar, but with a deep auto-collapsed hierarchy. So a developer can easily see where they are but might have to expand several times to find specific content.

Guide. FAN provides a *Get Started with Android* guide to developers along with a guide to adding interstitial ads. Neither guide provides any privacy information.

Supplemental Documentation. The FAN sidebar has no privacy-related terms visible at the default expansion. The "Guides" sidebar option opens to show options for pages about COPPA and CCPA but not GDPR. The *COPPA* page provides guidance on what "child directed" means and what flags to set, though when we looked up the stated flags, they did not exist in the linked API's documentation. The *CCPA* page provides code to use for both manual and library-detected setting of location.

Dashboard. "Blocking" is on the sidebar of "Monetisation Manager" next to pricing and performance. It provides options to block ad categories in sensitive and general categories (Figure 17) that are all unchecked (allowed) by default (e.g. "Associated with violence," "Gambling," and "Mature apps"). It also provides an option to limit data use but it is set to off by default (Figure 18).

4.4 Twitter MoPub (TMP)

Get Started with MoPub provides step-by-step instructions, many of which require a visit another page to complete the step. However, all the pages appear with the same sidebar, and the UI shows where the developer is in the site organisation as well as providing a clear "Get Started" link at the top of the sidebar so they can easily return to the main guide page. Each step also ends with encouraging statements like "Terrific: you've completed Step 4 of 7."

Guide. The TMP guide *Get Started with MoPub* has seven steps each of which contain a mix of text and links to other necessary guides, such as guides for integrating MoPub into Android, iOS, and Unity. Many of these are clearly on the critical path for a developer trying to integrate ads, but the guide text also contains recommended steps to do things like "refer to our best practices" with links. The *Integrate the MoPub SDK for Android* warns developers at the top that if they are upgrading they may have to do extra steps for GDPR and links to GDPR guidance which is also linked off the sidebar. The current SDK's behaviour is to auto-detect the user's coarse location using the truncated IP address and then automatically asks for consent from EU users without the developer needing to take action, hence the primary guidance does not directly cover GDPR. The sample code provides optional permissions with fine location data collection (Figure 19).

Supplemental Documentation. The first line in the *GDPR* page, described above, tells developers to read another page first; making it difficult to follow the instructions: "Do not start this article until you read our *GDPR Publisher Integration Guide* to understand the flow of events that you will implement below." Otherwise, TMP provided no other privacy guidance, and terms like CCPA and COPPA are not mentioned in guide pages.

Dashboard. The app application process requires developers to agree to a statement that their app does not target children younger than 13 years old. When clicking on our account name up in the right corner, content blocking shows up next to account settings, and log out. Some items are blocked by default (e.g. "Spyware/Malware," "Hate Content," and "Extreme Graphic/Explicit Violence") and cannot be unblocked (Figure 20).

4.5 Defaults Laced With Dark Patterns

While ad networks make it clear that it is developers' responsibility to make choices and be compliant with the regulations, ad networks make use of range of known dark patterns to nudge developers to make choices that are in the best interest of ad networks.

Developer-Facing Dark Patterns. Ad networks use *toying with emotion* by hinting that developers get higher revenue or better analytics by sharing more data with ad networks and enabling options like higher content ratings (e.g. mature audiences). *Preselection* used by all ad networks: regulation defaults are set to off, data collection is not limited, personalised ads are allowed, user consent is by default set to `true` in sample code, and content categories are all set to on (except for TMP that has a few categories set to off by default). GAM uses *aesthetic manipulation* in the content categories UI by having a blue toggle represent blocked items and a grey one for allowed items; TMP also uses a similar pattern with blue for blocked items. GAM uses *false hierarchy* by making the first option on the consent popup builder not include a "Do not consent" option, while the second nearly-identical choice does. Moreover, privacy information is hard to find in all the ad networks, representing the *hidden information* dark pattern. Abi pointed out that if privacy requirements are buried under sub-pages, advanced options, FAQs, or called "optional," it is not realistic to expect developers to fulfil those requirements. Privacy options should be part of the workflow, included in the step-by-step ad building guides like the other steps.

User-Facing Dark Patterns. Dark patterns in ad networks also target users. Sample code provided by GAM continues to ask for user consent even if they decline it, which is a clear example of *nagging* behaviour. Other examples in GAM include notifying the user about using location without giving them any options to refuse, or providing consent popups that do not have a "I do not consent" button; both of these instances represent a *forced action* dark pattern that could end up in developers' apps.

5 DISCUSSION AND FUTURE WORK

Drivers of Privacy. The need to comply with *legal requirements* like GDPR and CCPA drove much of the privacy-related content presented by ad networks. The need for *users* to consent to permission usage was also a large driver. Most mobile *operating systems* require user consent before apps can access specific data and resources, like location. This requirement seems to have compelled

ad networks to provide instructions around enabling the permissions and getting the user to consent to their usage. Prior work on privacy-related questions developers ask on Stack Overflow [48] observed developers rarely asking regulation-related privacy questions. However, a fairly large number of questions were related to construction and consequences of accessing resources in privacy policies. The overlap between the two works suggests that ad networks are interested in following regulations by providing flags, settings, and consent examples to developers, while developers are looking for advice on how to write privacy policies that properly express the impacts of including third-party content; information that ad networks do not currently provide.

A potential solution for the challenging privacy tasks may be providing tools to developers which can assist them in making more privacy-friendly decisions by making easy-to-use options available to them [21]. But there are few tools that help developers write things like user-friendly consent popups and accurate privacy policies, and even fewer that take into account both regulations and the current behaviours of common third-party APIs [44, 46], like ad networks. A line of future research would be to look into the practicalities of creating such a tool, potentially learning from usability studies in security APIs [16, 23] and notifications [47]. Ad networks also implied that making the more privacy-friendly choices would negatively impact developers' ability to make money from the ads. Since the only real benefit of adding an ad network to an app is financial, these comments may have an impact on developer decisions. Future research is called to look at the impact of choice framing and *nudging* on developers' decisions, and also the financial impact of such choices. Such studies, if presented in developer-friendly language, would have the potential to allow developers to make more informed trade-off decisions.

"Developers Are Responsible": Following Regulations Is a Developer Choice and Responsibility. The ad networks' language implied that following regulations was the *developer's responsibility*, not the ad networks', which is in contradiction with what developers think: it is ad networks' responsibility to protect user privacy [30]. While some ad networks provide code samples of how to handle legal requirements, they also take care to emphasise that it is the developer's responsibility to make sure they are complying with regulations appropriately. Abi was continuously confused and frustrated with these requirements as he (the developer) was the one who would be blamed for things like permission requests, even though they were being requested by the ad networks. For example, AMN provides brief documentation for CCPA and says: "We realize that you will determine what the CCPA means for your Amazon Mobile Ads integration" making the developer responsible but not providing an adequate guide. When Abi saw that he had to set flags (e.g. *Google's RDP* and `IABUSPrivacy_String`) in his app's `SharedPreferences` and not in the SDK, he was not sure how these changes might impact his liability, because typically he sets flags in the libraries and not in his app's shared space and it was odd that the regulation-related flags were located in a different place than the other API flags.

Here Be Dragons: Each Ad Network Has Its Own Unknowns. Ad networks present privacy information in a different location, use different language and options, and have different ways to control privacy options. They also explain how to handle legal requirements differently as well as differing on who is responsible (developer vs ad network) to do checks. For example, GAM provides consent popups but asks the developer to present it to the user, as opposed to TMP's consent that is handled by TMP. The result for developers is that each ad network is effectively its own uncharted area, requiring a fair bit of time to go through and understand how it handles privacy issues, often also requiring the developer to search beyond what is presented in the quick start guide.

Privacy Run Around. IAB is being used to standardise privacy requirements. However, it is also being used as an information black hole; developers are sent to IAB to find documentation on settings and flags that does not exist. AMN page contained information on CCPA, including links to IAB's guidance, relevant flags, and a sample code that shows how to set IAB flags by setting CCPA as not applicable and turning on location tracking. The FAQ question on GDPR provides several concrete flags that the developer can set but does not link to documentation on the setting options. We tried looking for guidance on the "consent string" called `IABTCF_TCString` but could not find its correct formatting on AMN or IAB. The FAQ page makes it clear that the IAB consent must be used if the developer wants to make money from EU traffic. GAM also asks developers to use IAB flags, but does not say how. Other black holes that ad networks send developers to visit are main regulation pages under the government sites or privacy policy pages of the parent corporations. Abi was not sure about the usefulness of such links for developers who do not have a legal background and said that he needs a lawyer to understand all these acronyms, terms, and conditions. Future research is needed to build and evaluate a usable framework for presenting privacy information to developers.

Can Developers Make Informed Choices? We find that ad networks use dark patterns to nudge developers to choose personalised ads and share more data, much like users resulting in a "*control theatre*" rather than giving developers a chance to make informed choices. We hypothesise that the low rate of GDPR-compliant consent popups in websites [15, 28, 49] and the abundance of non-compliant Android apps [26, 37, 39, 54] may partially be because developers are not making *informed decisions* and are either not aware of the consequences of their choices on users or not aware of how to do a better job than the defaults suggest; hence, not because of their ignorance for user privacy. Opinions about dark patterns are mixed; they are viewed as an ethical issue or a violation of law [51, 52]. A recent study by Norwegian Consumer Council shows that instances of data sharing in ad networks (e.g. TMP) appear to be illegal under GDPR [14]. Future research could look at ways to, at minimum, inform developers about these patterns, and regulators could work towards enforcing regulations beyond satisfying requirements like having a privacy policy or terms of service that only a few people may pay attention to.

ACKNOWLEDGMENTS

We thank Yashar PourMohammad for doing the walkthrough with us, and everyone associated with the TULiPS-Lab at the University of Edinburgh for helpful discussions and feedback. This work was sponsored in part by Microsoft Research through its PhD Scholarship Program and a Google Research Award.

REFERENCES

[1] Md Ahasanuzzaman, Safwat Hassan, Cor-Paul Bezemer, and Ahmed E. Hassan. 2020. A longitudinal study of popular ad libraries in the Google Play Store. *Empirical Software Engineering* 25, 1 (Jan. 2020), 824–858. https://doi.org/10.1007/s10664-019-09766-x

[2] App Annie. 2020. The State of Mobile in 2020. Retrieved August 2020 from https://www.appannie.com/en/insights/market-data/state-of-mobile-2020/

[3] AppBrain. 2020. Android Ad Network statistics and market share. Retrieved August 2020 from https://www.appbrain.com/stats/libraries/ad-networks

[4] Kenneth A Bamberger, Serge Egelman, Catherine Han, Amit Elazari Bar On, and Irwin Reyes. 2020. Can You Pay For Privacy? Consumer Expectations and the Behavior of Free and Paid Apps. *Berkeley Technology Law Journal* 35 (2020), 40 pages. https://doi.org/10.15779/Z38XP6V40J

[5] Harry Brignull. 2020. Dark Patterns. Retrieved August 2020 from https://darkpatterns.org

[6] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. *Proceedings on Privacy Enhancing Technologies* 2016, 4 (2016), 237–254. https://doi.org/10.1515/popets-2016-0038

[7] Federal Trade Commission. 1998. Children's Online Privacy Protection Rule (COPPA). Retrieved September 2020 from https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[8] Google Developers. 2019. Application Fundamentals | Android Developers. Retrieved August 2020 from https://developer.android.com/guide/components/fundamentals

[9] Google Developers. 2020. Permissions overview | Android Developers. Retrieved August 2020 from https://developer.android.com/guide/topics/permissions/overview

[10] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, and Alberto Bacchelli. 2020. UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376600

[11] Anirudh Ekambaranathan, Jun Zhao, and Max Van Kleek. 2020. Understanding Value and Design Choices Made by Android Family App Developers. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–10. https://doi.org/10.1145/3334480.3383064

[12] Dan Fitton and Janet C. Read. 2019. Creating a Framework to Support the Critical Consideration of Dark Design Aspects in Free-to-Play Apps. In *Proceedings of the 18th ACM International Conference on Interaction Design and Children* (Boise, ID, USA) *(IDC '19)*. Association for Computing Machinery, New York, NY, USA, 407–418. https://doi.org/10.1145/3311927.3323136

[13] Forbrukerrådet. 2018. Deceived by design. Retrieved August 2020 from https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design/

[14] Forbrukerrådet. 2020. Out of Control - How consumers are exploited by the online advertising industry. Retrieved August 2020 from https://fil.forbrukerradet.no/wp-content/uploads/2020/01/2020-01-14-out-of-control-final-version.pdf

[15] Imane Fouad, Cristiana Santos, Feras Al Kassar, Nataliia Bielova, and Stefano Calzavara. 2020. On Compliance of Cookie Purposes with the Purpose Specification Principle. In *IWPE 2020 - International Workshop on Privacy Engineering*. Genova, Italy, 1–8. https://hal.inria.fr/hal-02567022

[16] Martin Georgiev, Subodh Iyengar, Suman Jana, Rishita Anubhai, Dan Boneh, and Vitaly Shmatikov. 2012. The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security* (Raleigh, North Carolina, USA) *(CCS '12)*. Association for Computing Machinery, New York, NY, USA, 38–49. https://doi.org/10.1145/2382196.2382204

[17] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. 2018. The Dark (Patterns) Side of UX Design. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3174108

[18] Catherine Han, Irwin Reyes, Álvaro Feal, Joel Reardon, Primal Wijesekera, Amit Elazari, Kenneth A Bamberger, and Serge Egelman. 2020. The Price is (Not) Right: Comparing Privacy in Free and Paid Apps. In *Privacy Enhancing Technologies Symposium (PETS 2020)*. 21. https://doi.org/10.2478/popets-2020-0050

[19] Boyuan He, Haitao Xu, Ling Jin, Guanyu Guo, Yan Chen, and Guangyao Weng. 2018. An Investigation into Android In-App Ad Practice: Implications for App Developers. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*. 2465–2473. https://doi.org/10.1109/INFOCOM.2018.8486010

[20] Jaap-Henk Hoepman. 2019. *Privacy Design Strategies (The Little Blue Book)*. Radboud University. https://cs.ru.nl/~jhh/publications/pds-booklet.pdf

[21] Shubham Jain and Janne Lindqvist. 2014. Should I Protect You? Understanding Developers' Behavior to Privacy-Preserving APIs. In *Workshop on Usable Security (USEC'14)*. Internet Society, 10 pages. https://doi.org/10.14722/usec.2014.23045

[22] Ling Jin, Boyuan He, Guangyao Weng, Haitao Xu, Yan Chen, and Guanyu Guo. 2019. MAdLens: Investigating into Android In-App Ad Practice at API Granularity. *IEEE Transactions on Mobile Computing* PP, PP (2019), 1–1. https://doi.org/10.1109/TMC.2019.2953609

[23] Brittany Johnson, Yoonki Song, Emerson Murphy-Hill, and Robert Bowdidge. 2013. Why Don't Software Developers Use Static Analysis Tools to Find Bugs?. In *Proceedings of the 2013 International Conference on Software Engineering* (San Francisco, CA, USA) *(ICSE '13)*. IEEE Press, 672–681. https://doi.org/10.1109/ICSE.2013.6606613

[24] IAB Tech Lab. 2018. About IAB Tech Lab. Retrieved September 2020 from https://wiki.iabtechlab.com

[25] Ilias Leontiadis, Christos Efstratiou, Marco Picone, and Cecilia Mascolo. 2012. Don't Kill My Ads! Balancing Privacy in an Ad-Supported Mobile Application Market. In *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications* (San Diego, California) *(HotMobile '12)*. Association for Computing Machinery, New York, NY, USA, Article 2, 6 pages. https://doi.org/10.1145/2162081.2162084

[26] Ilaria Liccardi, Monica Bulger, Hal Abelson, Daniel Weitzner, and Wendy Mackay. 2014. Can apps play by the COPPA Rules?. In *2014 Twelfth Annual International Conference on Privacy, Security and Trust*. 1–9. https://doi.org/10.1109/PST.2014.6890917

[27] Arunesh Mathur, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW, Article 81 (Nov. 2019), 32 pages. https://doi.org/10.1145/3359183

[28] Celestin 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)*. 791–809. https://doi.org/10.1109/SP40000.2020.00076

[29] Michael Meng, Stephanie Steinhardt, and Andreas Schubert. 2018. Application Programming Interface Documentation: What Do Software Developers Want? *Journal of Technical Writing and Communication* 48, 3 (2018), 295–330. https://doi.org/10.1177/0047281617721853

[30] Abraham H. Mhaidli, Yixin Zou, and Florian Schaub. 2019. "We Can't Live Without Them!" App Developers' Adoption of Ad Networks and Their Considerations of Consumer Risks. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 20 pages. https://www.usenix.org/conference/soups2019/presentation/mhaidli

[31] Arvind Narayanan, Arunesh Mathur, Marshini Chetty, and Mihir Kshirsagar. 2020. Dark Patterns: Past, Present, and Future. *Queue* 18, 2 (April 2020), 67–92. https://doi.org/10.1145/3400899.3400901

[32] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376321

[33] Jonathan A. Obar and Anne Oeldorf-Hirsch. 2020. The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23, 1 (2020), 128–147. https://doi.org/10.1080/1369118X.2018.1486870

[34] State of California Department of Justice. 2018. California Consumer Privacy Act (CCPA). Retrieved September 2020 from https://oag.ca.gov/privacy/ccpa

[35] The European parliament and the council of the European union. 2018. General Data Protection Regulation (GDPR). Retrieved September 2020 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[36] Joel Reardon, Álvaro Feal, Primal Wijesekera, Amit Elazari Bar On, Narseo Vallina-Rodriguez, and Serge Egelman. 2019. 50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 603–620. https://www.usenix.org/conference/usenixsecurity19/presentation/reardon

[37] Irwin Reyes, Primal Wijesekera, Joel Reardon, Amit Elazari Bar On, Abbas Razaghpanah, Narseo Vallina-Rodriguez, and Serge Egelman. 2018. "Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale. *Proceedings on Privacy Enhancing Technologies* 2018, 3 (2018), 63–83. https://doi.org/10.1515/popets-2018-0021

[38] Katie Shilton and Daniel Greene. 2019. Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development. *Journal of Business Ethics* 155, 1 (March 2019), 131–146. https://doi.org/10.1007/s10551-017-3504-8

[39] Laura Shipp and Jorge Blasco. 2020. How private is your period?: A systematic analysis of menstrual app privacy policies. *Proceedings on Privacy Enhancing Technologies* 2020, 4 (Oct. 2020), 491–510. https://doi.org/10.2478/popets-2020-

0083
[40] Sooel Son, Daehyeok Kim, and Vitaly Shmatikov. 2016. What Mobile Ads Know About Mobile Users. In *Network and Distributed System Security Symposium (NDSS)*. 14 pages. https://doi.org/10.14722/ndss.2016.23407
[41] Chad Spensky, Jeffrey Stewart, Arkady Yerukhimovich, Richard Shay, Ari Trachtenberg, Rick Housley, and Robert K. Cunningham. 2016. SoK: Privacy on Mobile Devices – It's Complicated. *Proceedings on Privacy Enhancing Technologies* 2016, 3 (2016), 96–116. https://doi.org/10.1515/popets-2016-0018
[42] Statista. 2020. Number of available applications in the Google Play Store from December 2009 to June 2020. Retrieved August 2020 from https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/
[43] Statista. 2020. Share of global smartphone shipments by operating system from 2014 to 2023. Retrieved August 2020 from https://www.statista.com/statistics/272307/market-share-forecast-for-smartphone-operating-systems/
[44] Ruoxi Sun and Minhui Xue. 2020. Quality Assessment of Online Automated Privacy Policy Generators: An Empirical Study. In *Proceedings of the Evaluation and Assessment in Software Engineering* (Trondheim, Norway) *(EASE '20)*. Association for Computing Machinery, New York, NY, USA, 270–275. https://doi.org/10.1145/3383219.3383247
[45] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3411764.3445768
[46] Mohammad Tahaei and Kami Vaniea. 2019. A Survey on Developer-Centred Security. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 129–138. https://doi.org/10.1109/EuroSPW.2019.00021
[47] Mohammad Tahaei, Kami Vaniea, Beznosov Konstantin, and Maria K. Wolters. 2021. Security Notifications in Static Analysis Tools: Developers' Attitudes, Comprehension, and Ability to Act on Them. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, 1–17. https://doi.org/10.1145/3411764.3445616
[48] Mohammad Tahaei, Kami Vaniea, and Naomi Saphra. 2020. Understanding Privacy-Related Questions on Stack Overflow. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376768
[49] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)Informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 973–990. https://doi.org/10.1145/3319535.3354212
[50] Dirk van der Linden, Pauline Anthonysamy, Bashar Nuseibeh, Thein Than Tun, Marian Petre, Mark Levine, John Towse, and Awais Rashid. 2020. SchrödDinger's Security: Opening the Box on App Developers' Security Rationale. In *Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering* (Seoul, South Korea) *(ICSE '20)*. Association for Computing Machinery, New York, NY, USA, 149–160. https://doi.org/10.1145/3377811.3380394
[51] Ben Wagner, Krisztina Rozgonyi, Marie-Therese Sekwenz, Jennifer Cobbe, and Jatinder Singh. 2020. Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (Barcelona, Spain) *(FAT* '20)*. Association for Computing Machinery, New York, NY, USA, 261–271. https://doi.org/10.1145/3351095.3372856
[52] Ari Ezra Waldman. 2020. Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology* 31 (2020), 105–109. https://doi.org/10.1016/j.copsyc.2019.08.025
[53] John E. Williams, J. Kenneth Morland, and Walter L. Underwood. 1970. Connotations of Color Names in the United States, Europe, and Asia. *The Journal of Social Psychology* 82, 1 (1970), 3–14. https://doi.org/10.1080/00224545.1970.9919925
[54] Sebastian Zimmeck, Peter Story, Daniel Smullen, Abhilasha Ravichander, Ziqi Wang, Joel Reidenberg, N. Cameron Russell, and Norman Sadeh. 2019. MAPS: Scaling Privacy Compliance Analysis to a Million Apps. *Proceedings on Privacy Enhancing Technologies* 2019, 3 (2019), 66–86. https://doi.org/10.2478/popets-2019-0037

A SCREENSHOTS & SUMMARY OF PRESENTED PRIVACY-RELATED INFORMATION

Here, we provide a list of screenshots (as of Jan 2021), that have a privacy element or a dark pattern. Table 1 provides an overview of the available privacy information and where they are located.

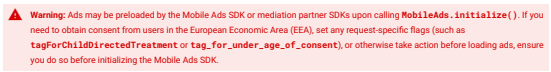

Figure 1: GAM's warning about obtaining consent from users in the European Economic Area in the *Get Started* page.

```
public void loadForm(){
    UserMessagingPlatform.loadConsentForm(
        this,
        new UserMessagingPlatform.OnConsentFormLoadSuccessListener() {
            @Override
            public void onConsentFormLoadSuccess(ConsentForm consentForm) {
                MainActivity.this.consentForm = consentForm;
                if(consentInformation.getConsentStatus() == ConsentInformation.ConsentStatus.REQUIRED) {
                    consentForm.show(
                        MainActivity.this,
                            new ConsentForm.OnConsentFormDismissedListener() {
                                @Override
                                public void onConsentFormDismissed(@Nullable FormError formError) {
                                    // Handle dismissal by reloading form.
                                    loadForm();
                                }
                            });

                }

            }
        },
        new UserMessagingPlatform.OnConsentFormLoadFailureListener() {
            @Override
            public void onConsentFormLoadFailure(FormError formError) {
                /// Handle Error.
            }
        }
    );
}
```

Figure 2: *Obtaining Consent with the User Messaging Platform* page in GAM provided a sample code for obtaining consent from users that constantly shows the popup to the user until they consent. Developers who use this sample code spread a "nagging" dark pattern in their apps.

```
protected void presentConsentOverlay(Context context) {
  new AlertDialog.Builder(context)
      .setTitle("Location data")
      .setMessage("We may use your location, " +
          "and share it with third parties, " +
          "for the purposes of personalized advertising, " +
          "analytics, and attribution. " +
          "To learn more, visit our privacy policy " +
          "at https://myapp.com/privacy.")
   .setNeutralButton("OK", new DialogInterface.OnClickListener() {
     @Override
     public void onClick(DialogInterface dialog, int which) {
       dialog.cancel();
       // TODO: replace the below log statement with code that specifies how
       // you want to handle the user's acknowledgement.
       Log.d("MyApp", "Got consent.");
     }
   })
   .show();
}

// To use the above method:
presentConsentOverlay(this);
```

Figure 3: *Precise Location Data Policy* page in GAM provided a sample code for obtaining location consent from users without providing a "I do not consent" or "No" button. Developers who use this sample code spread a "forced action" dark pattern in their applications.

Table 1: Presented privacy-related information on the ad networks' pages.

Ad Network	GDPR	CCPA	COPPA	Block Categories	Block Certain Domains	List of Vendors	Consent Popup	Location Permission	Other
GAM	Sidebar & warning in guide	Sidebar	Warning in guide	Dashboard	Dashboard	Dashboard	Customisable	Sidebar	Content rating (dashboard)
AMN	FAQ	FAQ	FAQ	Dashboard	Dashboard	-	-	Within guide	-
FAN	-	Sidebar	Sidebar	Dashboard	Dashboard	-	-	-	-
TMP	Sidebar & within guide	-	While creating an app	Dashboard	Dashboard	-	Provided	Within guide	Personal data passing (sidebar)

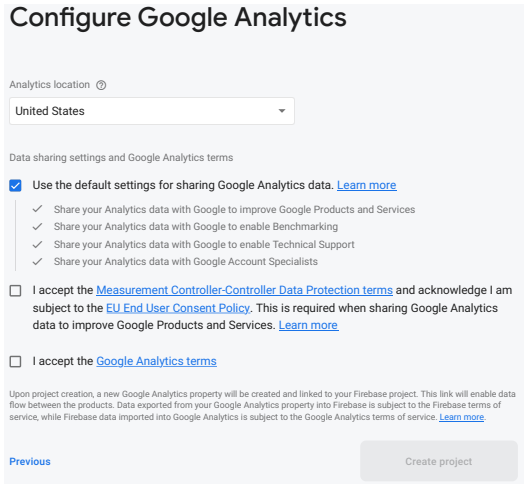

Figure 4: Google Analytics had the default option on to share our data with Google (GAM). Turning off the default option would result in seeing a list of sub by default on permissions for all the grey items (e.g. Google products, Benchmarking). "Preselection" dark patterns happens here as the default setting to share information between multiple services is not in the best interest of user privacy.

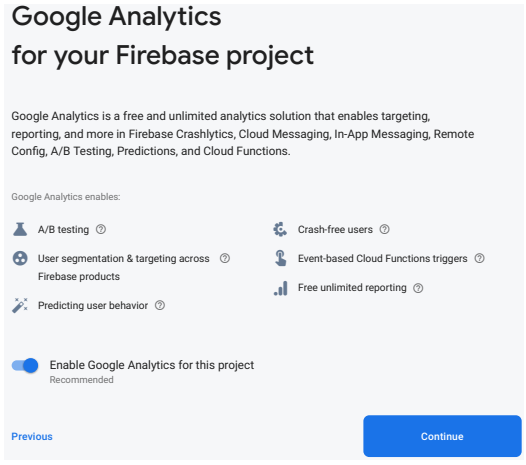

Figure 5: Google Analytics is turned on by default when creating an account on Firebase (GAM). "Preselection" dark patterns happens here as the default setting to share information between multiple services is not in the best interest of user privacy.

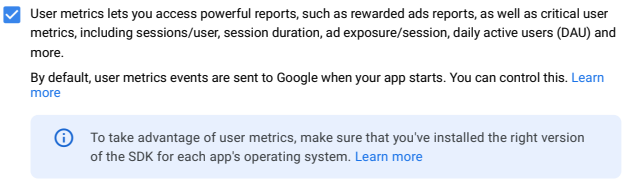

Figure 6: When creating an app on GAM, we were asked to enable users metrics for powerful reports. The box was pre-ticked. "Preselection" happens here as sharing user data with multiple services is not in favour of user privacy.

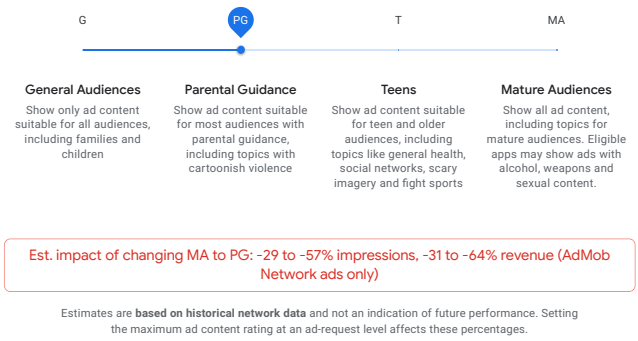

Figure 7: In the GAM account page under *Blocking controls* we could change the ad content rating. The default value was on the MA. "Toying with emotion" has been applied to encourage developers stay with the MA ratings.

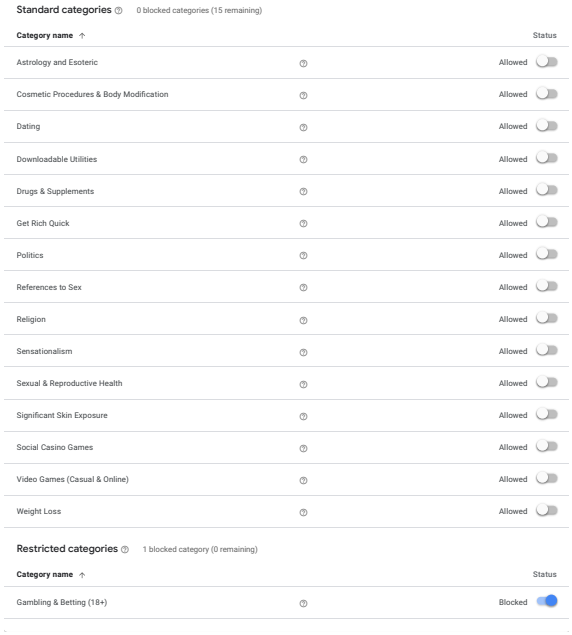

Figure 8: In the GAM account page under *Blocking controls* we could "allow" or "block" certain categories. The use of grey and blue colour to use "aesthetic manipulation" dark pattern is easily visible. Grey commonly has a passive and negative tone whereas blue is known to have a positive tone [53].

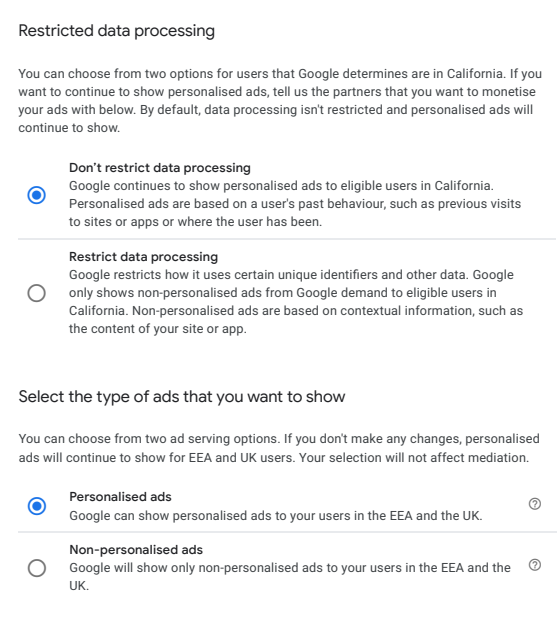

Figure 9: CCPA and GDPR sections of GAM have pre-selected items for information processing and personalised ads. "Preselection" dark pattern occurs here because GAM by default collect information and also shows personalised ads (hence collects more information as well).

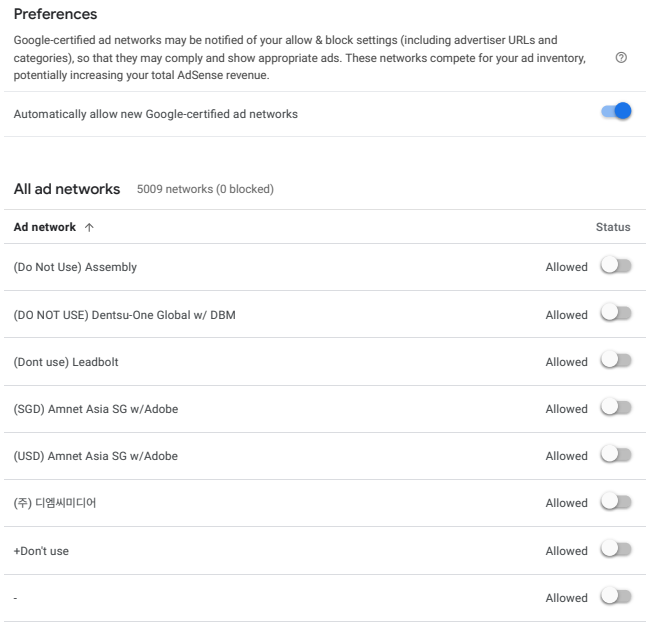

Figure 10: In the *funding choices* service we could "allow" and "block" certain ad vendors. All vendors were "Allowed" by default. GAM pre-ticked the box for automatically adding new vendors to list. 'Preselection" dark pattern spreads via this interface to end-users if developers do not make an effort to change the defaults.

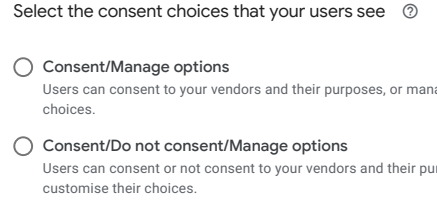

Figure 11: *Funding choices* is a service from GAM to create consent popups. It provides two ready-to-use consent pop-ups to developers, the first option does not have a "Do not consent" button.

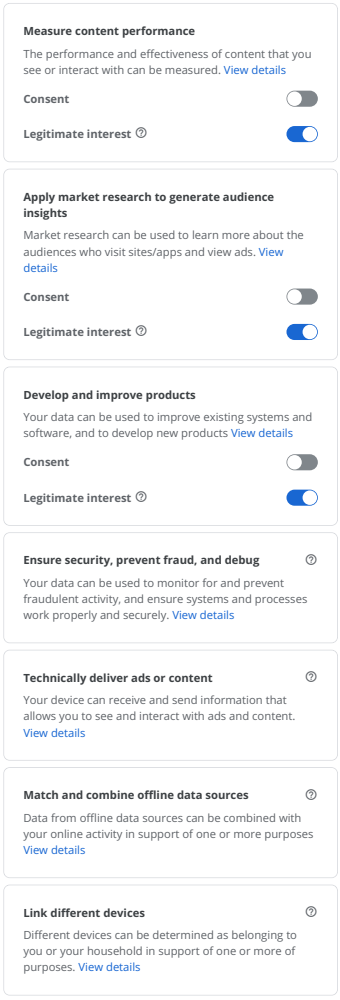

Figure 12: *Funding choices* is a service from GAM to create consent popups. Several items could be customised for users. These are some of the default values. "Preselection" dark pattern spreads via this interface to end-users if developers do not make an effort to change the defaults.

```
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
```

Figure 13: AMN in the *Quick Start Guide* page asks developers to add internet, network, wifi access, coarse and fine location for higher revenues for developers. While location permissions are called as "optional" the sample code includes both fine and coarse location permissions. "Sneak into basket" dark pattern is present here because developers may copy paste this code without fully being informed about what the sample code does.

Examples

The following examples provide a sample US Privacy String that represents the stated conditions. In all but the last example, a digital property has determined to use a US Privacy String and that CCPA applies to the transaction.

Example 1 meets the following conditions:

- Version 1 of the US Privacy string is being used. (1)
- The digital property has provided explicit user notice. (Y)
- The user has NOT made a choice to opt out of sale. (N)
- The digital property is not operating under the Limited Service Provider Agreement. (N)

1YNN

Example 2 meets the following conditions:

- Version 1 of the US Privacy string is being used. (1)
- The digital property has NOT provided explicit user notice. (N)
- The user has made a choice to opt out of sale. (Y)
- The digital property is not operating under the Limited Service Provider Agreement. (N)

1NYN

Example 3: Digital property ousources string creation

In this example the digital property has asked a vendor to create a US Privacy String on their behalf, knowing only whether the user has opted of sale of personal data.

- Version 1 of the US Privacy string is being used. (1)
- The status of provided explicit user notice is unknown. (-)
- The user has made a choice to opt out of sale. (Y)
- The status of operating under the Limited Service Provider Agreement is unknown. (-)

1-Y-

Example 4: CCPA does not apply

In this example, a digital property has determined to use a US Privacy String and that CCPA does not apply to the transaction.

1---

Figure 14: IAB's sample values for CCPA's *US Privacy String*.

```
final JSONObject pjObject = new JSONObject();
try {
  pjObject.put("us_privacy", "1---"); // example privacy string value
}
catch (JSONException ex)
{
  Log.e(LOGTAG, ex.getMessage());
}
final AdTargetingOptions adOptions = new AdTargetingOptions();
adOptions.enableGeoLocation(true);
adOptions.setAdvancedOption("pj", pjObject.toString());
this.adView.loadAd(adOptions);
```

Figure 15: AMN's sample code in their *FAQ* page. `enableGeoLocation` is switched on in the sample code ("sneaking" [17]). "1---" is provided as an example privacy string value. "1" means version 1 and "-" means "Not Applicable." Two dark patterns are visible here, if developers copy paste this code "sneak into basket" occurs and "preselection" also happens because the defaults are not in favour of user privacy (see Figure 14 for IAB code samples.)

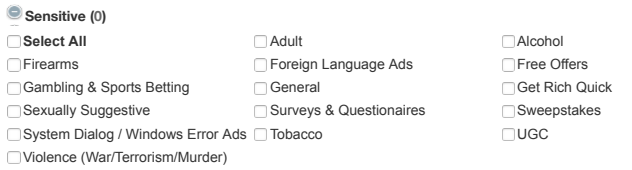

Figure 16: AMN lets developers to block ad categories. By default no categories are blocked. "Preselection" dark pattern happens here as developers may never visit this page and the defaults are not in the best interest of end-users.

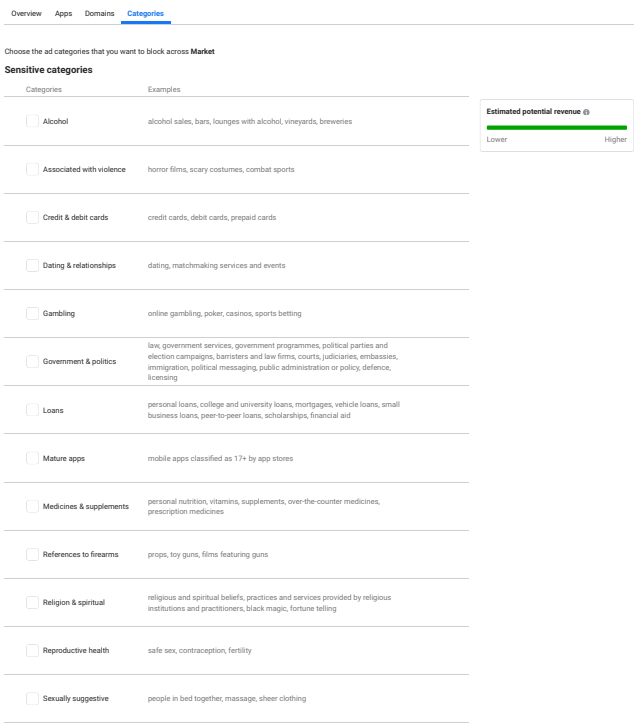

Figure 17: FAN's sensitive categories are all active by default. The two blocked options are blocked by us. "Preselection" dark pattern happens here as developers may never visit this page and the defaults are not in the best interest of end-users. The green bar on the top right corner will change as developers pick several items, hinting a loss of revenue as they block more categories.

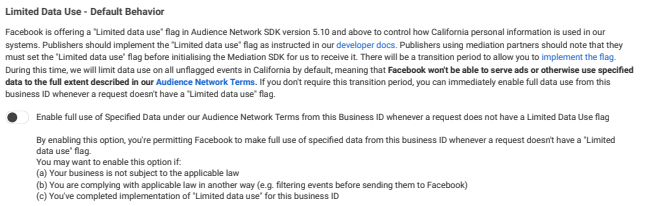

Figure 18: FAN users' data policy is under developer's setting page, next to roles and permissions and notification. It is disabled by default to no limit for data use. "Preselection" dark pattern happens here as data collection which is not in favour of user privacy is turned on by default.

```
<!-- Required permissions -->
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />

<!-- Optional permissions. Will pass Lat/Lon values when available. Choose either Coarse or Fine -->
<uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
```

Figure 19: TMP's permissions for older versions of Android in the *Integrate the MoPub SDK for Android* page.

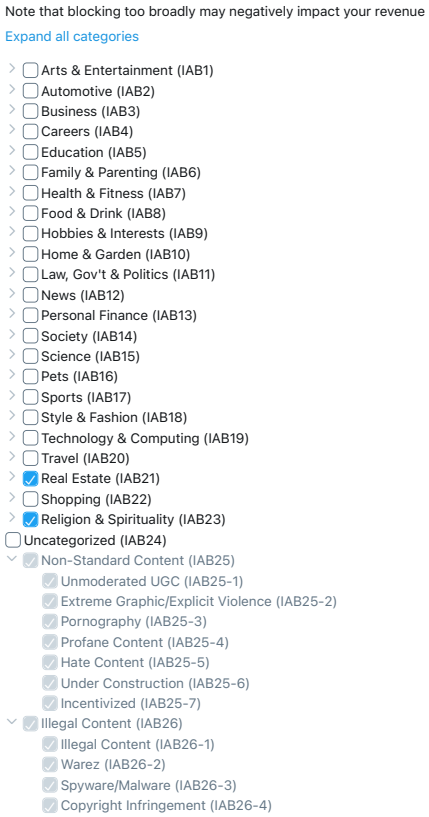

Figure 20: TMP's content categories. Default blocked categories cannot be changed and are greyed out. Blocked items by the developer are highlighted by blue.