"We Can't Live Without Them!" App Developers' Adoption of Ad Networks and Their Considerations of Consumer Risks

Abraham H. Mhaidli, Yixin Zou, and Florian Schaub,
University of Michigan School of Information

https://www.usenix.org/conference/soups2019/presentation/mhaidli

"We Can't Live Without Them!" App Developers' Adoption of Ad Networks and Their Considerations of Consumer Risks

Abraham H. Mhaidli, Yixin Zou, Florian Schaub
University of Michigan School of Information
{mhaidli, yixinz, fschaub}@umich.edu

Abstract

Mobile ads pose privacy and security risks to consumers, including behavior tracking, malware, and inappropriate or biased content. Advertising networks connect mobile app developers with advertisers, enabling in-app advertising. We conducted a mixed-methods study with mobile app developers, consisting of survey and semi-structured interviews, to better understand why and how they partner with advertising networks, and their considerations of consumer risks in those interactions. Our findings focus on app developers who work independently or in smaller companies. We find that developers use advertising because they see it as the only viable way to monetize their app. Developers mostly choose an advertising network based on perceptions of which ad networks are popular rather than a holistic assessment. Despite claims of optimizing for profitability or consumer well-being, developers largely keep ad networks' default configurations. Developers are resigned to ad-related consumer risks, seeing themselves as unable to and not responsible for addressing the risks. Based on our findings, we discuss recommendations for mitigating consumer risks of mobile advertising.

1 Introduction

Many mobile apps use advertising to generate income [43]. Apps typically utilize *advertising networks* (e.g, Google AdMob, One by AOL, or Smaato [25]), which act as mediators between apps that are able to show ads and advertisers with ads to display. Ad networks provide revenue for apps; moreover, with ads apps can be offered free of charge, making

them more broadly accessible.

However, ad networks are not without problems. In order to deliver relevant ads to users, ad networks use targeted advertising, for which they collect data about users through the apps or other means (e.g., online and app behavior, interests, geolocation, age, and gender) [65]. This pervasive data collection raises privacy concerns about access to this data, and whether it can be abused to manipulate or harm users [17]. Ad networks have been found to deliver offensive ads (which can emotionally harm users [65]) and discriminatory ads (e.g., promoting high paying jobs only to men or associating "black-identifying names" with prison sentences [20, 68]). Other ads have redirected users to malicious URLs that install malware onto users' devices [6, 51]. While issues with ads have been studied widely, we know little about how mobile app developers choose an ad network and to what extent they consider potential risks for their users in that decision.

Prior work on mobile developers' privacy and security behaviors found that developers want to choose 'good' third-party libraries, but may not be able to effectively evaluate them, e.g., because respective privacy policies are confusing [8]. Sources used to learn coding practices (e.g., Google vs. Stack Overflow) have also been shown to affect the security of resulting apps [1]. However, so far there has been no in-depth analysis of mobile ad network selection from the developers' perspective. Yet, understanding how app developers interact with and use ad networks is important for effectively tackling the consumer risks posed by ad networks. App developers have a crucial role in the in-app advertising ecosystem, as they decide whether and how they use in-app advertising.

To better understand app developer behaviors with ad networks, we investigated the following research questions: (1) Why do developers choose to monetize their apps through ads? (2) How and why do developers decide which ad network to use? (3) How do developers configure the ad networks they use? (4) How do developers manage the consumer risks posed by ad networks?

We conducted a mixed-methods study with mobile app developers, the majority of whom were independent app de-

velopers. We surveyed 49 developers who have worked with in-app advertising and interviewed 10. We find that developers choose to use advertising out of a belief that it is the only viable way to monetize an app; most choose ad networks based on information in forums or a vague notion of which ad networks are used the most. Regarding their ad network configurations, developers claimed to optimize profit or ensure consumer well-being – however, we find that developers largely stuck to ad networks' default settings. While most developers were aware of consumer risks posed by ads, they were resigned about them. Most developers saw the responsibility to address those issues with ad networks, and viewed themselves as having little ability to effect change.

Our findings provide new insights on how app developers navigate the realm of in-app advertising. We conclude by discussing our findings' implications for intervention efforts to reduce the consumer risks of targeted ads and ad networks, including potential public policy directions and methods for better supporting developers in considering the implications of their ad network choices.

2 How Ad Networks Work

Advertising accounts for over half of mobile app revenue [43]. An advertising network connects *publishers* (i.e., app developers) and *advertisers* [50, 69]. Publishers offer ad networks space in their apps for advertising, e.g., a banner ad. The ad network pays the publisher a fee for this space, e.g., X dollars for every Y users who click an ad. The ad network then charges advertisers a slightly higher fee [50, 69]. The most commonly adopted ad network is Google AdMob [74], used by over 90% of apps that show ads [67]. Other popular ad networks include Facebook Audiences (9.86%), StartApp (8.82%), and Unity Ads (7.32%) [67].

2.1 Targeted Advertising

Ad networks often engage in *targeted advertising* [65], i.e., individual users are shown ads that are presumably relevant to their interests, e.g., someone who likes soccer might be shown an ad for tickets to a soccer match nearby [80]. The expectation is that since users are shown ads relevant to them, they are more likely to engage with the ad and buy the advertised product. Advertisers can select what groups of people should see their ads based on interest-profile selectors. This increases advertisers' revenue, and reduces resources spent on inefficient ads shown to consumers who are unlikely to engage with them [10]. Targeted advertising can benefit publishers as well: having ads that users are more likely to click increases the ad click rate and thus revenue [10]. Arguably, targeted advertising also benefits consumers, since consumers are not subjected to irrelevant ads [52].

However, targeted advertising also presents substantial risks for consumers. A necessity of ad targeting is the ex-

tensive gathering of information about individual consumers. This might include a consumer's online and app activities, age, gender, occupation, location, and other information inferred from individual behavior. This data is used to create a profile for a given individual. Ad networks infer what profiles are amenable to what sort of advertisements by monitoring who opens what kind of ads [52]. Information for ad targeting is often collected directly by ads displayed in an app and tracking code. For instance, when a user opens an app with an ad, the ad network code used to load the ad can (potentially) access the location information of the device, and so determine where the user is. The ad network can leverage this information to update the user's advertising profile and show the user more relevant ads (e.g., only showing ads for events near the user).

2.2 Ad Network Options for Publishers

To better understand how developers interact with ad networks, we analyzed the websites, terms of use, and documentation of five prominent ad networks [24]: Google AdMob, One by AOL, InMobi, Smaato, and StartApp. Overall we find that their services, functionalities, and even interfaces are very similar, with some minor differences.

To use an ad network to host ads in their app, developers apply for an account, and after review their account is approved or rejected. Once approved, developers have access to an online dashboard. Although dashboards differ among ad networks, they typically allow developers to view their revenue earned and the apps they have registered with the ad network. After registering an app, developers get access to the necessary code and IDs to integrate ads into their app. Integrating the ad code is fairly straightforward. Ad networks provide software development kits (SDKs) with which developers place ad display code in their app. The SDK typically allows developers to configure the type of ad to display (e.g., banner ad, video ad, etc.), its size, and where/when it appears in the app. Thus, while the ad network determines what ads get shown, the developer determines how ads are displayed.

Through the online dashboard, developers can further filter what ad categories may appear in their apps. Potential categories may include dating, cars, health, etc., and may differ by ad networks. By default, almost all categories are enabled. Google AdMob, though, has 'restricted ads' (for alcohol and gambling) that require publishers to opt-in to show them. Others (e.g., InMobi) have these same categories enabled by default. Developers can further block specific advertisers.

In addition, developers can choose (to some degree) what user data the ad network collects through a specific app by requesting certain mobile permissions for the app. Some permissions are required by the ad network (e.g., Internet connection, operating system, device type, network status); other permissions are not (e.g., precise geolocation). Developers can choose whether to provide this information to the ad net-

work. Other information developers can choose to send to the ad network include a user's age and gender, depending on what ad display code is used in the app. Developers have a financial incentive to share more information with ad networks: the more information is shared, the more relevant ads are delivered to users, and so, in theory, the developer's revenue will be greater. Lastly, targeted ads (as opposed to non-targeted ads) are the default option for all five ad networks studied, but developers can choose to display non-targeted ads.

3 Related Work

Prior research relevant to our work has focused on ad networks and developer behaviors regarding information seeking, tool selection, and privacy and security.

3.1 Consumer Risks of Ad Networks

Documented consumer risks posed by ad networks include (1) insensitive or offensive content [3]; (2) discriminating ads (e.g., ads for high paying jobs only shown to men, or ads that associate "black-identifying names" with criminal sentences and offer felony checks for individuals [20, 68]); (3) targeting based on sensitive content (e.g., religion) despite regulation against it [12]; and (4) excessive resource draining (such as battery and data) by ads [36, 57, 74]. Two prominent concerns are users' privacy and security.

Regarding users' privacy, ad networks collect information about users to target ads. This raises concerns over the vast quantities of information being collected, who has access to it, and for what purposes it is being used beyond advertising. Studies have found that ad networks collect extensive personal information, over-privilege apps to collect more information than needed, and that current protections are not effective at safeguarding user privacy [34, 46, 58]. A user's profile and data could be exposed, not only to an ad network and its advertisers, but to anyone who could access the ads seen by the user [14, 71]. Proposed solutions aim to protect consumer privacy while providing benefits of targeted ads [35, 38, 70], e.g., by performing targeting locally in the user's browser [70]. However, it is unclear how widely such solutions have been adopted.

Regarding users' security, a prominent risk is that of fraudulent ads that redirect users towards installing malware [27, 66], also known as madware [73]. Despite proposed solutions, such as improving malware classifiers using semantic features [15], it is still a prevalent problem. In 2017, Google AdMob purged over a billion ads, due to malware, phishing, and other consumer risks [63]. Additionally, there is the risk of sensitive ads being shown to users that can cause emotional discomfort or harm [65].

3.2 Developer Behaviors

To understand how app developers choose and engage with ad networks, it is important to know their information seeking behaviors. Social environment, especially information from colleagues and close friends, is highly influential in determining what tools developers adopt [39, 60, 79]. For instance, the adoption of security tools is heavily shaped by whether peers are utilizing that tool [56, 59, 78]. However, while peers are an important and useful resource for adopting new tools, they get used infrequently [55, 56].

Developers also use online forums and communities to find information and evaluate issues or complicated topics, such as code-related ethics, privacy risks, or the appropriateness of code contributions to a project [64, 72]. Trust and ease of access are major factors in determining what information sources developers use [39]. Contextual factors, such as familiarity with subject matter, stage of project, and client characteristics further impact information seeking behavior [28].

A common theme in studies of app developers' privacy and security behaviors is that developers often want to adhere to 'good' privacy and security practices (e.g., create secure code, respect user privacy), but fail to do so for a variety of reasons, such as lack of resources or expertise [5, 8, 32], faulty information sources [1], or insufficient documentation [26]. Balebako et al. found that app developers struggled to navigate complex privacy policies of third-party libraries, and were generally unaware of the data collected by such tools [8]. Egele et al. found that app developers often make mistakes when using cryptographic APIs [23]. Some app developers ask for more permissions than necessary, potentially for financial incentives [26, 46, 58]. However, Gorski et al. showed that API-integrated security advice can support developers in improving code security [32].

Despite the recognized privacy and security risks, very few studies have looked specifically at how developers choose ad networks. Some studies touch tangentially on this subject (e.g., Balebako et al. [8]) as part of more general investigations into developers' selection and use of tools. In contrast, our study provides deeper insights into both *how* and *why* app developers interact with ad networks, as well as to what extent and how they consider consumer risks in those interactions.

4 Study Design

To study mobile developers' behavior, practices, and attitudes regarding ad networks, we conducted a mixed-methods study involving a survey and semi-structured interviews. Our study was approved by the University of Michigan's IRB.

4.1 Survey

We first conducted an online survey to understand developers' attitudes and behaviors regarding ad networks (see Appendix

A). We asked about participants' experience developing apps and working with advertising networks. To gain more insights about particular experiences, we next asked participants to focus on one app for which they were involved in choosing and/or integrating ad network code. We asked what resources were used to choose an ad network, and had them rate which factors they valued when choosing an ad network. The survey concluded with demographic questions.

The survey was hosted on Qualtrics. Participants were given the option to enter a raffle for eight $20 Amazon gift cards. The median response time was 12.5 minutes.

4.2 Semi-structured Interviews

We conducted semi-structured interviews with some survey participants to gain deeper insights into mobile developers' views, behaviors, and attitudes towards ad networks (see Appendix B). We first asked participants about their background and experience with developing apps. Second, we asked which ad networks they had used and their respective experiences. Third, we asked how an ad network was chosen and how ads were configured in their app. Fourth, we asked about issues, problems, and consumer risks they had seen, heard of, or experienced with ad networks. Lastly, we asked broader questions to elicit their general thoughts regarding ad networks. Interview participants received a $15 Amazon Gift Card. Interviews lasted 27 to 42 minutes (median: 32 min.).

Interviews were transcribed and then analyzed with descriptive coding [53]. Two of the authors developed an initial codebook by jointly reading the transcripts and identifying emergent themes. They then iteratively refined the codebook by separately coding an interview, determining inter-rater reliability, revising the codebook as needed, and repeating with a separate interview. This procedure was repeated for 5 interviews until high inter-rater reliability was reached (Cohen's κ=.75) [53]. One of the authors then re-coded all interviews with the final codebook.

4.3 Recruitment

Our target population was app developers who have used ad networks in some capacity. Thus, our recruitment message asked for participants who had worked with ad networks, but did not mention privacy, security or risks.

We leveraged multiple channels to recruit participants, including posting in online forums aimed at app developers (e.g., the subreddit /r/AndroidDev) and technical Facebook groups; advertising through Craigslist; handing out flyers at local app developer meetups; reaching developers through personal contacts; and directly contacting developers based on contact information in the app store and LinkedIn.

The recruitment message advertised both the survey and interview component of the study, encouraging (but not requiring) participation in both. We conducted the survey and

interviews in Summer and Fall 2018.

5 Findings

Our results show four key findings: (1) developers use advertising due to a belief that it is the only viable way to monetize an app; (2) when choosing an ad network, developers rely on online forums and ad networks' official websites, and do not spend much effort exploring which ad network to use; (3) developers often stick to ad networks' default configurations instead of optimizing for revenue or consumer safety; (4) developers do not view themselves as being able to or responsible for addressing consumer risks, believing that the responsibility lies with ad networks. We first discuss participant demographics, before presenting our findings in detail. We group findings by theme, combining findings from the survey and interviews, given that they address similar topics and complement each other nicely (quantitative information from the survey and rich qualitative insights from the interviews).

5.1 Participant Demographics

In total, 49 participants completed our survey. Their median age was 24 years (range: 18-47 years), which is relatively young compared to app developers' estimated average age (34 years) [45]. 37 participants were male, 3 female, 1 identified as non-binary, and the rest did not disclose their gender. This is reflective of the male-dominated app development field, e.g., over 90% of UK app developers are male [75].

Mobile app development experience varied: 8 participants had less than one year, 12 had 1-2 years, 9 had 2-3 years, 10 had 3-4 years, and 10 had more than 4 years of experience developing mobile apps. The median numbers of apps participants had worked on over the past three years was 6 (range: 1 to 100). Most (38) developed Android apps, 23 for iOS, and 13 for both; 1 developed for Windows Phone.

All participants provided the app's name and/or a link to its app store page. We analyzed each app's download and review numbers. As of May 2019, 26 apps were available in the Google Play store, with download numbers ranging from 10+ to 10,000,000+ (median: 10,000+), and review numbers ranging from 1 to >504k (median: 157). 12 apps were not available in the Google Play Store, but via APKPure, an alternative Android app market. 9 apps were in the iOS App Store, which only provides review numbers (range: 6-519k, median: 118). This snapshot shows that most participants' apps had a smaller audience, but other apps were highly popular.

About half of our participants (26) worked in small companies (four employees or less), and most (38) worked in small development teams (see Figure 1). This might be due to our recruitment strategies (e.g., directly contacting app developers via app store contact information), which were more likely to reach developers in small companies. However, it is reasonable to expect that developers in small companies/teams have
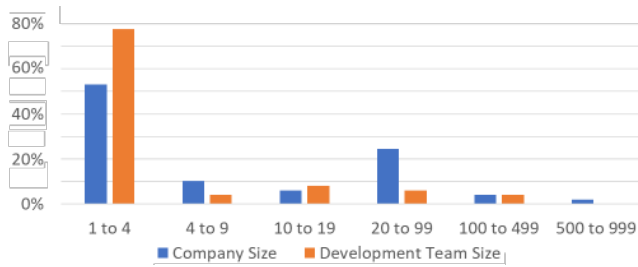
Figure 1: Company size (*blue*) and development team size (*orange*) of survey participants (n=49).

	Age	Years Experience	Ad Networks Used	Company Size (employees)
P1	21	3–4	Admob, StartApp, Flurry	1–4
P2	29	> 5	AdColony	1–4
P3	24	2–3	Admob, StartApp, InMobi, Unity Ads	10–19
P4	22	1–2	AdMob, ONE by AOL, Unity Ads	1–4
P5	39	1–2	AdMob	1–4
P6	23	> 5	AdMob, StartApp, Unity Ads, Facebook Ads, Vungle	20–99
P7	19	3–4	AdMob	1–4
P8	26	< 1	AdMob	1–4
P9	24	> 5	Admob, Facebook Ads, Vungle, App-O-Deal	1–4
P10	24	3–4	AdMob, InMobi, Unity Ads	1–4

Table 1: Interview participant demographics (n=10).

more say in how ad networks are chosen and used. Most (44) participants had worked as developers or software engineers; 23 as project managers; 16 as testers; 15 in upper management; 12 in marketing and 12 in user support (participants could select multiple roles).

9 survey participants were also interviewed. An additional interview participant (P9) did not fill out the survey, but contacted the researchers to participate in the interview directly. Table 1 provides their demographics. All interviewees were male; their median age was 24 years (range: 19–39 years). 8 participants were app developers working alone or in small teams (< 5 employees); P3 worked for a slightly larger company and P6 worked in upper management of a larger company that develops several apps.

5.2 Considerations in Adopting Advertising

Most participants used ads out of a resignation that ads are the only way to make money (despite general dissatisfaction with ad revenue), and after a careful evaluation of the type of app being developed. We first characterize ad network use before discussing why developers decided to use ads.

5.2.1 Ad Network Use Is Common

Ad networks were commonly used in the mobile apps developed by both survey and interview participants. 60% of the mobile apps developed by survey participants in the past three years used an ad network. 20 survey participants reported that advertising was the only monetization model they used. The most used ad network was Google AdMob (91% used it at least once), followed by Unity Ads (34%), inMobi (22%), and StartApp (20%). Others included Flurry (16%), Smaato (12%), One by AOL (12%), and LeadBolt (8%). This reflects a market dominated by Google AdMob, echoing prior work [74]. 16 survey participants and 6 interviewees had worked with three or more ad networks.

5.2.2 Resignation to ads as monetization model

When asked why advertising was chosen, 7 interview participants expressed a resignation towards advertising, saying it was the only viable way to monetize an app. They noted that because most apps are free (and monetized through ads), the only realistic way for an app to be competitive is to make it free as well. P10 said: *"I [knew] that many people wouldn't consider purchasing my app, so the only other viable option at the point seemed to include ads."* P9 was explicit: *"If it wasn't for advertising, almost all the independent developers would basically just die."* P6 mentioned a 'race to the bottom': when apps first came out they were expensive, but over time, app developers competed with one another, driving prices down and eventually forcing many apps to be free.

Despite a resignation towards ads, both survey and interview participants expressed dissatisfaction with ad revenue. In the survey, we asked participants whether and why they had changed ad networks in the past. All 10 survey participants who had changed ad networks indicated that higher revenue was a very/extremely important factor for changing – suggesting that their current revenue levels might be low or at least could be improved from their perspective. Moreover, 8 interview participants directly complained about the low revenue share they receive from ad networks. P7 stated: *"Google [AdMob] takes quite a big cuts of ad revenue obviously themselves, so you as the developer don't always see a lot of returns."* P2 similarly said: *"It's tough because the advertising dollars are so low, you need to have a large-scale viewership. You can't just have 1,000 people playing and watching."* While also disappointed with ad revenue, P10 had a different motivation for using ads: annoy users and encourage them to pay for the app's ad-free premium version.

5.2.3 Type of app matters for ad adoption

Alongside resignation with ads, all interview participants considered the type of app they were developing in their monetization choice. They would consider the app's genre, expected audience, and how often people would use the app and for

how long. Interviewees noted that for an app targeted toward a niche market, an app developer could charge users while still profit and gain traction. However, for a 'general' app with a wider audience, or an app that people would use infrequently, advertising was considered the only option for monetization.

5.2.4 Showing ads to users considered fair

3 interviewees considered ads ultimately a fair way to monetize apps for both users and developers: for users, viewing ads may be annoying and inconvenient, but less so than paying for an app. P7, who used advertising in their app, said this is because the app offered a *"pretty basic service [which isn't] worth that much necessarily,"* and considered it unfair to charge users for it. Similarly, on comparing ads to charging for in-app purchases, P2 said *"I felt better about asking people to watch an ad rather than pay for a feature."* Another perspective emerging from the interviews is that ads were a fair compensation for the free app users were getting: if the app developer had spent significant time and energy creating an app, it was fair that users 'pay' the cost of seeing ads to compensate the developer.

Furthermore, 4 interviewees considered ads to have low impact on the user experience (less so than charging money). P1 justified his use of ads because *"[users] could always just shut off the ads and get rid of them,"* i.e., noting that it is up to the user whether they see ads or pay for the premium version.

5.3 Choosing an Ad Network

We asked both survey and interview participants how they selected the specific ad network for their app. In summary, participants either looked for information in online forums or acted on preconceived notions of what ad networks exist. This would lead them to a couple of ad networks, for which they would examine the ad network's website, and use it if it looked trustworthy. They typically kept using an ad network until it presented severe problems.

5.3.1 Resources used to choose ad networks

Prior work suggests that developers often rely on friends and colleagues in tool selection [39, 60]. Our survey provided a different picture. Although 32% of survey participants rated friends as very/extremely important when choosing an ad network, the ad network's website (58%) and online discussion forums (45%) were rated as more important (see Figure 2).

The interviews revealed a more nuanced selection process. 8 interviewees reported choosing a particular ad network based on a vague awareness that other developers were using it with good experiences. P4 said: *"[What ad network to use] wasn't really a thing that we researched too heavily. It was more when we decided to kind of go that route, you're already kinda familiar with other people doing it; they seemed to have*
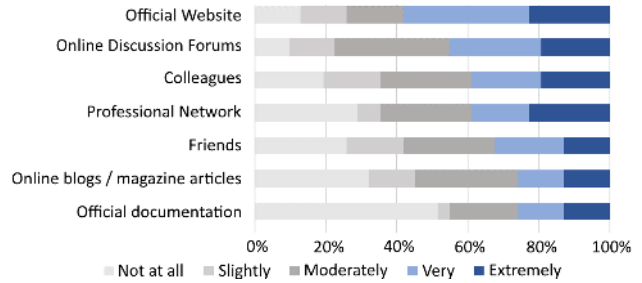

Figure 2: Survey responses to "How important were the following resources in deciding what advertising partner / advertising network to choose for APP NAME?"

success with it, it didn't seem too difficult to add in." For others, their ad network choice was based on what they had read in online forums, a vague awareness that a company existed, or even convenience (e.g., the ad network was supported by the SDK they were using to develop the app). 5 interviewees used rough heuristics to select an ad network. For example, 3 chose Google AdMob due to trust in its reliability, given that it is a large company. P5 chose AdMob because they believed it would work better on Android, given that Google develops Android. He said: *"Basically because it's Android, and as a Google product it seemed like the natural choice at the time because I trust them more. So I was like, 'Alright, I'll go with that.' And I've heard a lot about them so it made most sense."*

6 interviewees reported they would then visit an ad network's website, and use the ad network if it looked trustworthy. Only 2 interviewees reported a conscious effort to compare and contrast different ad networks before choosing one.

5.3.2 Sticking with a chosen ad network

Once they chose an ad network, most participants reported sticking with it. Only 20% (10) of survey participants had switched ad networks. "Competitor offering more revenue" was the most popular factor in this decision (3 rated 'very important;' 7 'extremely important'). Most interview participants (7) also stuck with their choice despite minor issues (e.g., low revenue), unless it posed severe problems or became unusable. Those who used ads in multiple apps typically used the same ad network for all apps, due to familiarity with the service and having all their revenue in one place.

5.3.3 Exceptions for choosing ad networks

Among the 10 interviewees, P3 and P6, who both worked for larger companies with 20 or more employees, displayed unique patterns in ad networks selection. P3 was instructed by his company to use Google AdMob. Although he had no definite knowledge as to why Google AdMob was chosen, he
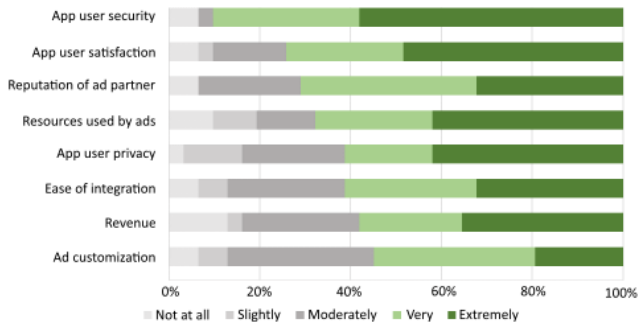
Figure 3: Survey answers to "In choosing an advertising partner / advertising network for APP NAME, what factors were considered, and how important were they in making the final decision?"

hypothesized that it was because past apps had used AdMob and the company had experience with it.

P6, as CEO of his company, would frequently switch ad networks so as to optimize revenue. In his words: *"What we would actually do is do an A/B test. [...] We would just write a particular logic method where when you first download an app [...] There would be two different [ad] networks integrated into the application, and randomly you would be assigned to one of them. We would get all the quantitative data. How often the ad shows, how often it fills, was it clicked? Was it annoying? Did the person delete it? What was the overall experience? What's the actual monetary vCPM [viewable cost-per-thousand impressions]?"* Yet, P6 noted that there were overall few changes in the set of 4–5 ad networks used, with AdMob being used the most.

5.3.4 Factors considered in ad network selection

63% (31) of survey participants reported having been involved in ad network selection. Participants considered different factors in that decision (see Figure 3): 90% of participants considered the security of their users a very/extremely important factor. Similarly, 74% considered user satisfaction as very/extremely important. By contrast, revenue or ease of integration were valued less highly (58% and 61%, respectively). Least important were ad customization options.

However, revenue was the most popular decision factor for switching ad networks. 20% (10) of survey participants switched ad networks for an app, and for all revenue was a very/extremely important reason for switching. For half of them, revenue had been an equally important factor in their initial ad network choice. For the other half, revenue was more important in switching ad networks than initial selection.

The survey findings contrasted with the interview findings: 7 interviewees valued ease of integration the most, even if the ad network may have other shortcomings, such as revenue. P1 noted: *"[StartApp]'s definitely not the best, but it's just an*

ease to implement." Considering that most interviewees were independent app developers, they might lack the resources to deal with complicated code, similar to previous findings that developers might lack the time to navigate complex privacy policies [8]. As P1 says *"I just don't have enough free time and I'd rather work on my app."* We note that for the interviewees who also took the survey, there were slight disparities between survey and interview responses in this respect. 2 participants who in the interview claimed that ease of integration was most important did not rate ease of integration as very/extremely important in the survey. Moreover, all who rated ease of integration as very/extremely important in the survey also rated at least one other factor (e.g., revenue) as extremely important in the survey, suggesting that ease of integration was on par with other factors.

The contrasting findings from the survey (where user satisfaction was valued highly in ad network choice, and revenue when switching) and the interviews (where ease of integration was valued highly in ad network choice) might be explained by social desirability bias. However, there were subtle indications in the interviews that the expressed care towards users is genuine, such as *"I don't want the app to be unfair to users"* (P7), or *"I felt better about not being intrusive to users"* (P5). Cognitive dissonance seems a more likely explanation: app developers want an ad network that does not harm their users, but integration and revenue take priority in practice, as they are factors directly experienced by the developers.

5.4 Sticking with Default Configurations

Despite claims of valuing certain factors over others, most interviewees (8) used ad networks' default ad settings and code options, *regardless* of the financial incentives. For instance, when using an ad network, developers can increase the amount of user data collected by the ad network by asking for additional mobile permissions, which in theory improves the relevance of ads shown to the user, and thus might enhance engagement and revenue. In contrast to past work finding that developers may add additional permissions for profit reasons [46], 9 interview participants claimed they used an ad network's default permissions or the bare minimum (only P9 added more permissions than necessary).

When asked if they used targeted or non-targeted advertising, 9 interviewees said they used targeted ads (the default), and 4 had not explored the possibility of non-targeted ads. The main reasons for using targeted ads were not only revenue increase (4), but also to provide a more enjoyable user experience (4), since users are not bothered by irrelevant ads. P7 said: *"I think [targeted ads are] more useful: for the developers, you end up making more money from them; and for the users seeing the ads, it's definitely more useful information."*

Moreover, most ad networks allow developers to customize what ad categories are shown in an app – by default all categories are enabled by most ad networks. 8 interviewees had

not changed the defaults; the other 2 restricted certain ad categories for apps aimed at children, or blocked a specific advertiser after a bad experience with them.

While developers explain configuration decisions with optimizing revenue or user experience, their configurations are often not consistent with the stated goals. For example, most interviewees rationalized targeted ads with improved revenue and user experience, yet they did not ask for additional permissions, which could further increase the accuracy of ad targeting (as well as increase privacy risks). Thus, rather than engaging in fully rational optimization, developers seem to be subject to status quo bias [62], even despite financial incentives to make adjustments.

5.4.1 Projection onto app users as decision rationale

One interesting way developers rationalized their ad network configuration was to imagine themselves as the users. 4 interviewees would project themselves onto their users to decide what settings to use, using a logic of 'I don't like it when an app does X, so I will not do X to my users.' P5, in explaining why he chose to use banner ads, said *"I hate the ones that pop up and make you watch a video for thirty seconds because that breaks the flow of your app. I don't want them to interrupt, I just want to have extra content so banners made the most sense."* Similarly, P2 explained why he used a minimalistic banner ad in his app: *"If [users] don't want to, they can avoid it, and I think that's what is important to me personally as a player."* This again suggests that developers cared for and desired a good experience for their users. This care, though, is nuanced, in that it might have a financial aspect to it: an app that is harmful towards its users may lead to a decline in use. Thus, care is also important so as to maximize revenue.

5.5 Awareness of Consumer Risks

We asked survey participants to rate how true or false certain statements were, in order to assess their awareness of consumer risks posed by ad networks (see Figure 4). Overall, survey participants had mixed awareness of risks associated with ad networks. Ad networks have been found to sometimes collect user data without explicit consent [22]. When asked whether ad networks collect user data without users' permission, 41% of survey participants considered it probably/definitely true, but 20% false. Responses are skewed towards 'false' for ad networks' showing malicious ads (17 probably/definitely false; 5 probably/definitely true) or explicit and graphic ads (21 probably/definitely false; 10 probably/definitely true). Interviewees, on the other hand, were generally aware of ad networks' consumer risks, including malicious or graphic ads, privacy and data collection concerns, and excessive resource draining (battery and data).
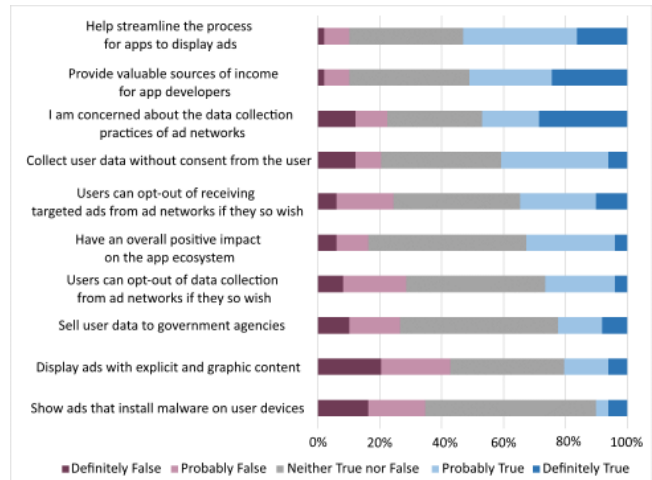

Figure 4: Survey participant answers to question "How much do you agree with the following statement: Advertising networks..."

5.5.1 Awareness of risk does not lead to concern

Both survey and interview participants expressed mixed opinions about whether certain consumer risks were concerning. For instance, when asked if they were concerned about ad networks' data collection practices, 23 survey participants said definitely/probably true; 11 said definitely/probably false.

Interviewees' responses on what constitutes main consumer risks varied substantially. When asked what risks they were aware of broadly, 4 mentioned privacy concerns; P5 highlighted how ads used a lot of battery. We then probed interview participants about four specific types of risks: excessive data collection and tracking; graphic and inappropriate ads; malicious ads; and excessive resource draining. All interviewees claimed to have heard of these risks, but they had different opinions about how much they mattered. 6 interviewees described excessive resource draining as a minor risk, whereas the other four said it deserved attention, and one of them further described steps they had taken to mitigate this issue. Similarly, privacy was a big concern for some (4), but for the rest, such as P10, it was a minor issue: *"I don't view [privacy] as so much of a problem because it's not just the ad networks gathering it, it's almost all the major vendors and smartphones do that anyway to optimize their own services, so I think it's gonna happen either way."*

5.5.2 Positive impression of ad networks despite issues

Despite acknowledging issues with ad networks, both survey and interview participants generally had a positive impression of them. 33% (16) of survey participants said it was probably/definitely true that ad networks had a positive impact on the mobile app ecosystem, as opposed to only 7 for proba-

bly/definitely false. Similarly, half (25) of survey participants said it was probably/definitely true that ad networks provide valuable sources of income for app developers. Interviewees were also generally favorable toward ad networks, commenting on how they help *"monetize an app that's not necessarily monetizable"* (P10), and on the ease and convenience they offer developers.

5.6 Managing Consumer Risks

Most survey and interview participants considered it the ad network's responsibility to manage and address consumer risks. They did not view themselves as having the agency to effect change in this regard.

5.6.1 Ad networks responsible for mitigating risks

Both survey and interview participants considered the ad networks responsible for managing and mitigating advertising-related consumer risks. Almost half (22) of survey participants said the ad network should be 'completely responsible' for removing bad ads found on ad networks; whereas only 2 survey participants considered app developers responsible, and 4 pointed at government regulatory entities. Similarly, all interviewees thought the ad network should be mostly, if not exclusively, responsible for addressing such problems, given the lack of control app developers have over what ads are shown in their apps.

Additionally, interviewees expressed resignation toward these risks and that app developers could do little to address them. When asked about issues with ad networks collecting excessive data, P10 talked about his inability to do anything about it: *"There is not much else I can do about it except not use the advertising service, but that's not really a solution. I don't even know what I could do to counter it."* Some interview participants further expressed an inherent trust in ad networks, in that these companies had the tools, willpower, and capability to filter out 'bad' ads, and thus there was little to worry on behalf of the app developers.

5.6.2 Little monitoring of ads

We asked interviewees whether they monitored the ads in their apps. P3 and P6's companies checked their apps frequently, by having dedicated employees or even a team systematically use the app to ensure the ads that appear are not malicious or explicit. However, most interviewees (8) did not make much effort to check if the ads in their apps were problematic. 3 explicitly stated that they did not monitor the ads in their app. For the 5 who did monitor the ads in their apps, they did so in a fairly informal way, such as using the app on a friend's device and seeing what ads appeared. This was similar to how P3 and P6 monitored their apps, but done in a much less frequent, structured and systematic manner.

3 interviewees explained this lack of monitoring with a fear of getting banned from an ad network. Most ad networks have measures in place to prevent automated or falsified clicks, i.e., 'clickfraud.' App developers found engaging in clickfraud may face penalties. Therefore, it is difficult for developers to check the ads in their apps without risking being reprimanded. P5 explained: *"I haven't personally [monitored my ads] because there are really strict rules, with AdMob, about triggering your own ads, because if you do that then it's kind of like trying to make your own money which is a problem."*

2 interviewees pointed out that it would be difficult to monitor malicious ads appearing in an app, given that ad selection is targeted to individual users. When talking about the possibility of viewers being exposed to overly graphic or explicit ads, P2 said *"If a person is targeted with ads that are more graphic in nature, the user would like it because [...] it's based on their viewing history."* This demonstrates strong trust in the accuracy of ad targeting and a disregard for the possibility of misuse or algorithmic bias.

6 Discussion

Our findings provide insights on (1) how developers choose ad networks, (2) how developers use and configure ad networks, and (3) how developers manage consumer risks posed by ad networks. When choosing an ad network, most participants feel resigned to the use of ads, viewing it as the only viable way to monetize an app. When configuring ad network settings, most participants used default settings *regardless* of the financial advantages or disadvantages of that choice. With respect to managing the consumer risks posed by ads, app developers are generally aware of the risks, but consider ad networks responsible for addressing them.

We first discuss limitations of our study, followed by opportunities for future research and intervention design that can better support developers in choosing and using ad networks, in ways that monetize their apps while mitigate consumer risks.

6.1 Limitations

Our study's sample consisted largely of developers working independently or for small companies (< 5 employees). This population constitutes an important faction of the app development ecosystem. For example, in France and Germany over 30% of app development companies had fewer than 5 employees, and in the UK, it is above 50% [76]. The differences in our interviews between small independent developers and one developer working for a larger company indicate that our findings are likely specific to small independent developers. Differences in ad network use between small and large app development companies should be studied in more detail in future research. Studying developers for small apps alone still provides a useful perspective though, given that most apps in

the market come from relatively new developers, and we need insight into the perspectives on ad-based monetization (and monetization more generally) from these individuals who just entered the field. Research with computer science students could also provide valuable insights in this regard.

Due to the specificity of our target population (app developers who had experience working with ad networks), our sample size is seemingly small (49 survey participants, 10 interviewees). However, our sample size is comparable to other studies examining software developer behaviors [9, 11, 16, 29, 30], due to general difficulties in recruiting participants who are professionals. Our study still provides rich insights into how small independent app developers manage ad networks and reason about associated consumer risks.

A common limitation in survey and interview studies relates to how participants may self-report behavior. Participants may not remember all details accurately, or may try to present a better self-image due to social desirability bias. We designed our survey and interview protocols in ways that avoid biasing participants. We also discussed potential indicators of social desirability bias in our findings.

6.2 Supporting Developers in Choosing App Monetization Models

Our findings suggest that many small app developers use ad networks out of resignation that advertising is the only way to make money from their app. Meanwhile, many participants complained that ad revenue was often low. It is questionable whether this resignation is well-founded: there are apps that exist without ads, and there seems to be little evidence to suggest that advertising is the only or most profitable way to monetize an app. Factors such as app category or what platform the app is on can influence how successful different monetization models are [7, 37, 61]. For instance, Roma et al. find that in Apple's App Store, paid and freemium monetization models generated higher revenues than free models, but they did not find significant differences between monetization models in the Google Play store [61]. Vratonjic et al. suggest that instead of adopting a blanket monetization approach, companies should strategically apply different funding approaches for individual users to maximize profits (e.g., using models to predict different users needs and wants, and serving ad-financed or fee-financed apps to different users) [77].

Given that our participants displayed limited knowledge of monetization models, we suggest a possible intervention: **presenting developers with more accurate information about what monetization models are available and optimal for an app under what circumstances, as well as associated risks or benefits for consumers**. This could increase developers' awareness of potential monetization models beyond the dominant reliance on advertising, and could encourage developers to adopt monetization models that increase revenue and pose fewer risks to consumers.

To accomplish this, more research is needed to (1) characterize and understand what monetization models are optimal for mobile apps under what circumstances; (2) analyze the impact of different monetization models on consumers, e.g., risks associated with each model and how consumers perceive them; and ambitiously, (3) explore new monetization models for apps that go beyond advertising and paid models, which ideally retain the low barrier to entry that free apps have, but do not pose the same consumer risks as targeted advertising.

One alternative way to finance apps is through crowdfunding, which has been an effective way to raise funds for projects related to games and journalism [4, 47]. This funding model could change the dynamic between app developer and consumer, creating a closer relationship and encouraging developers to act more responsibly towards their consumers [4, 13]. Another option for monetizing apps could lie in virtual currencies. For example, the social media platform Steemit rewards users who generate appreciated content with its own cryptocurrency: user accounts on Steemit are able to upvote posts and comments, and authors who get upvoted are rewarded with cryptocurrency tokens [18, 48]. Other platforms that adopt similar blockchain-based monetization models include Brave, SoMee.Social, Minds.com, and Presearch.org [2]. Moreover, certain subscription services (such as Youtube Premium) [31] work by having users pay a monthly flat fee, which gives users access to all content on their platform: the total money from these fees is distributed to the creators based on how much users interact with them (more interaction = larger share of the total money). Applying this to the context of mobile apps, one can imagine apps being monetized and valued based on the amount of downloads or users they have.

Once it is better understood which monetization models work best under what circumstances, as well as their respective benefits and disadvantages for both developers and consumers, a system (e.g. a website) could be constructed to aid developers with choosing a suitable monetization model for their app: after developers enter the characteristics of the app, such as the app's category and expected audience, the system would then recommend monetization models and show comparisons along multiple dimensions (e.g., revenue, user signup/conversion rate, public perception, and consumer risks). This system could be a standalone website or be offered by mobile platforms as part of their developer resources. It could also be integrated into online app development tutorials and courses (e.g., as a module on "financing your app"), as well as into integrated development environments (IDEs).

We argue that aiding developers with information grounded in research and data, as opposed to intuition or heuristics, could benefit both developers and consumers by highlighting less well-known monetization models with fewer consumer risks than advertising. The potential for success of this approach is supported by our finding that developers already engage in a deliberation process regarding their app's monetization model, but often in an unstructured manner. This

indicates that developers may be amenable to and benefit from more systematic information on monetization models.

6.3 Rethinking Ad Network Defaults

Participants in our study exhibited status quo bias [62]: they tended to stick to ad networks' default settings, regardless of the financial incentives involved. This implies that if harmful content appears in an app (e.g., sensitive products are being advertised), this is more likely due to the ad network's default setting, rather than any initiative by the developer. However, previous research has found that app developers sometimes ask for more permissions than necessary in their apps for financial reasons [46].

We thus propose that one way to limit consumer risks posed by ad networks could be **encouraging or mandating ad networks to change what the default settings are**. This approach has been used successfully in other contexts, such as healthy meal selection [41]. In the context of in-app advertising, the specific default settings to be regulated could relate to what permissions are set, whether targeted (or non-targeted) ads are used by default, and what categories of ads are permissible.

For instance, the default permissions required by an ad network could be reduced to the minimum necessary for the ad network to function. This would limit what data about consumers is collected and used for advertising purposes, and would also correspond to the GDPR's "data protection by default" principle. Additionally, in order to address privacy concerns of targeted advertising [80], the default could be set to 'non-targeted' rather than 'targeted' ads. Alternatively, it could be mandated that apps have to ask users for explicit consent to engage in targeted advertising (and if a user does not consent, show non-targeted ads). Consequently, fewer apps may engage in targeted advertising, perhaps alleviating some of the associated concerns. Moreover, currently it is common practice for most or all ad categories to be enabled by default. This should be changed so that certain sensitive ads, such as those for harmful products like tobacco or alcohol, political ads, or predatory ads (e.g., 'Get Rich Quick' ads that prey on vulnerable populations), are blocked by default. This could reduce the instances of such ads appearing and causing negative consequences, such as discomfort for consumers [3], the manipulation of people's voting behavior [42], and the sale of respective harmful products.

Of course, ad networks may be resistant to our proposed changes. There are financial incentives for maintaining the current defaults. Targeted ads may increase profit for the ad network, and greater data tracking may allow better (and so more profitable) targeted advertising [10]. Aside from the profitability of the ads themselves, more data might also hold better value for sale to third parties, such as data brokers. It is unlikely that ad networks will simply change their behavior due to these competing incentives, especially given that the advertising industry is mostly self-regulated through entities like the Digital Advertising Alliance.

We suggest regulators need to hold ad networks accountable by prescribing how defaults should be set up when self-regulatory approaches are ineffective. Consumer concerns about privacy risks are high [21], indicating that there may be political will to enact legislation. For instance, a recent report by the U.S. Government Accountability Office recommended that U.S. Congress should enact legislation to better protect consumers [19]. Other legislative efforts to regulate data tracking, such as the GDPR and the California Consumer Privacy Act (CCPA), have already been ratified and are being implemented. It is conceivable that future privacy legislation, such as the European ePrivacy Regulation or possibly a U.S. federal consumer privacy law, could stipulate more consumer-friendly default practices by ad networks.

App developers could also potentially drive ad networks to change defaults. App developers may desire to protect users, as directly suggested by our findings. Therefore, a collective call from app developers may exert pressure on ad networks. For instance, app developers could advocate that current app store requirements should be modified to avoid harmful content and prevent excessive data collection by default.

Finally, we should not neglect the possibility that ad networks may display goodwill. Faced with increasing concern and scrutiny surrounding data tracking practices, ad networks might want to regain consumer trust. Ad networks could set defaults that safeguard consumers to portray themselves as taking consumer safety and privacy seriously, while also providing a more explicit value proposition of targeted ads to consumers.

6.4 Encourage Developer Responsibility

Our findings indicate that developers care about the well-being of their users, e.g., most of our survey participants ranked app user security and satisfaction as very/extremely important in choosing an ad network. This aligns with Balebako et al.'s findings, suggesting developers want to create secure code that respects user privacy, but fail to do so for a variety of reasons such as struggling with complex privacy policies [8]. Our results reveal two main reasons why developers fail to mitigate ad-related consumer risks: (1) a belief that even though problems exist with ad networks, there is nothing app developers can do; and (2) a resignation that advertising is the only way to monetize an app.

Given this, we propose two opportunities for intervention. The first is to **correct the belief that developers cannot effect change**. At first glance, app developers may seem small when compared to ad networks, but they are still a crucial part of the advertising ecosystem. As such, they can effect change: both by simple actions such as configuring ads in certain ways (e.g., blocking ads for sensitive products), or more involved actions such as voicing complaints and concerns

over ad network practices, or boycotting certain ad networks. Second and more importantly, as a prerequisite of encouraging action, it is important to **make app developers realize that safeguarding app users from ad-related risks is not only the responsibility of ad networks, but also theirs**.

To encourage developers to take on responsibility, the focus of responsibility should be switched from blaming to collective action. Usually responsibility is talked about in terms of blame – if someone is responsible for consumer safety and the consumer is harmed, then that entity is blamed. Interpreting responsibility this way might be counter-productive, since it could alienate developers by painting them as 'guilty culprits.' Additionally, this interpretation does not show an accurate picture of the realities of in-app advertising. Loui and Miller discuss moral responsibility (as opposed to legal or causal responsibility) as a form of responsibility that, rather than seeking one actor or entity to blame for a system's problems, encourages all responsible actors to think critically about their role in the problem, and what they could do to mitigate the problem [49]. Similarly, Gotterbarn brings up 'positive responsibility,' a concept that does not seek to hold one party accountable or to blame for a system's problems, but rather motivates developers to think about the consequences of their actions on others [33].

Applying the positive responsibility framing to the context of in-app advertising, developers should not be blamed for the consumer risks of advertising. Rather, it emphasizes that in-app advertising is an ecosystem with multiple actors and stakeholders (advertisers, ad networks, app developers, and consumers). All members of the ecosystem do their part in allowing it to work, for good and for bad. The actions of those within the ecosystem influences how it will function – and so, it is on all the system's actors to make in-app advertising work better for everyone.

Given that developers seem to generally care about their users, as evidenced by our study and prior work [8], this suggests that developers might be amenable to taking actions that would mitigate consumer risks and protect their users. To achieve this, we suggest that it is important to show developers the power they have and the actions they can take. There are many places where this message could be promoted. One way is to target app development tutorials, courses, and online forums that developers visit frequently: creating new content that discusses positive responsibility and specific actions developers can take to mitigate consumer risks. This is in line with Mozilla's recent efforts to incorporate ethics into computer science curricula [54].

However, we acknowledge that encouraging developers to take responsibilities for consumer risks can be challenging. Not all developers would be willing to put in the effort needed to take on positive responsibility. Some might be in dire financial situations that make it difficult to properly care about their users. To address these barriers, material incentives should be created to encourage positive responsibility –

perhaps a badge, token, or icon awarded to developers who proactively attempt to mitigate consumer risks of ad networks (e.g., a "fair trade" label for ads). Such a badge could be displayed to consumers as part of app descriptions, and help consumers identify responsibly designed apps. This would hopefully lead to more consumers using such apps, increasing their revenue, thus serving as an incentive for developers to earn this certification.

Even with these incentives, there are still challenges that positive responsibility faces. Further avenues of research could examine what factors could encourage the adoption of positive responsibility in developers, similar to research on encouraging other prosocial behavior (e.g., examining how economic incentives encourage blood donations or how technology can be used to increase empathy [40, 44]).

7   Conclusion

We conducted a mixed-methods study to better understand how and why developers choose and use ad networks, and how they manage consumer risks. We find that most developers feel resigned to use advertising, seeing it as the only viable way to profit from their apps. Developers mostly choose an ad network based on factors like which ad networks they perceive to be popular rather than a holistic assessment. Most developers use ad networks' default configurations *regardless* of the financial implications of that choice. Almost all developers believe the responsibility to mitigate the consumer risks of in-app advertising lies with ad networks.

We discuss several proposals for better supporting developers in mitigating consumer risks, such as presenting information on alternate monetization models for apps to developers, and enacting policy to make the default configurations of ad networks more consumer-friendly. Future work is needed to further explore these proposals, including both their effectiveness at overcoming consumer risks posed by in-app advertising, as well as challenges that we may face in getting developers to notice any provided guidance and support.

Acknowledgments

References

[1] Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L. Mazurek, and Christian Stransky. You Get Where You're Looking for: The Impact of Informa-

tion Sources on Code Security. In *IEEE Symposium on Security and Privacy*, 2016.

[2] Activist Post. BRAVE: The Future Of Content Creation, Curation And PRIVATE Internet Browsing: Review. activistpost.com/2019/04/brave-the-future-of-content-creation-curation-and-private-internet-browsing.html, 2019. Retrieved 5/22/19.

[3] Lalit Agarwal, Nisheeth Shrivastava, Sharad Jaiswal, and Saurabh Panjwani. Do not embarrass: Re-examining user concerns for online tracking and advertising. In *Proc. of the 9th Symposium on Usable Privacy and Security*, pages 8:1–8:13, 2013.

[4] Tanja Aitamurto. The Impact of Crowdfunding on Journalism. *Journalism Practice*, 2011.

[5] Amirhossein Aleyasen, Oleksii Starov, Alyssa Phung Au, Allan Schiffman, and Jeff Shrager. On the privacy practices of just plain sites. In *Proc. of the 14th Workshop on Privacy in the Electronic Society*. ACM, 2015.

[6] Chaitrali Amrutkar, Kapil Singh, Arunabh Verma, and Patrick Traynor. Vulnerableme: Measuring systemic weaknesses in mobile browser security. In *International Conf. on Info. Systems Security*. Springer, 2012.

[7] Gil Appel, Barak Libai, Eitan Muller, and Ron Shachar. Retention and the Monetization of Apps. 2015.

[8] Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason Hong, and Lorrie Faith Cranor. The Privacy and Security Behaviors of Smartphone App Developers. In *Proc. of the Workshop on Usable Security*, 2014.

[9] Olga Baysal, Reid Holmes, and Michael W Godfrey. Developer dashboards: The need for qualitative analytics. *IEEE Software*, 30(4):46–52, 2013.

[10] Howard Beales. The Value of Behavioral Targeting. *Network Advertising Initiative*, 2010.

[11] Birgitta Bergvall-Kåreborn and Debra Howcroft. 'The future's bright, the future's mobile': A study of Apple and Google mobile application developers. *Work, Employment and Society*, 2013.

[12] Juan Miguel Carrascosa, Jakub Mikians, Ruben Cuevas, Vijay Erramilli, and Nikolaos Laoutaris. I always feel like somebody's watching me: Measuring online behavioural advertising. In *Proc. of the 11th Conf. on Emerging Networking Experiments and Technologies*, pages 13:1–13:13. ACM, 2015.

[13] Miguel Carvajal, José A. García-Avilés, and José L. González. Crowdfunding and Non-Profit media: The emergence of new models for public interest journalism. *Journalism Practice*, 2012.

[14] Claude Castelluccia, Mohamed-Ali Kaafar, and Minh-Dung Tran. Betrayed by your ads! In *Privacy Enhancing Technologies Symposium*. Springer, 2012.

[15] Wei Chen, David Aspinall, Andrew D. Gordon, Charles Sutton, and Igor Muttik. More semantics more robust: Improving android malware classifiers. In *Proc. of the 9th ACM Conf. on Security & Privacy in Wireless and Mobile Networks*, pages 147–158. ACM, 2016.

[16] Mauro Cherubini, Gina Venolia, Rob Deline, and Andrew J Ko. Let's Go to the Whiteboard: How and Why Software Developers Use Drawings. In *Proc. of the SIGCHI Conf. on Human Factors in Computing Systems*. ACM, 2007.

[17] Jeff Chester. Cookie wars: How new data profiling and targeting techniques threaten citizens and consumers in the "big data" era. In *European Data Protection: In Good Health?* 2012.

[18] Usman W Chohan. The concept and criticisms of steemit. *SSRN 3129410*, 2018.

[19] Catalin Cimpanu. Gao gives congress go-ahead for a gdpr-like privacy legislation. zdnet.com/article/gao-gives-congress-go-ahead-for-a-gdpr-like-privacy-legislation/, 2019. Retrieved 2/27/19.

[20] Amit Datta, Michael Carl Tschantz, and Anupam Datta. Automated experiments on ad privacy settings. *Proc. of Privacy Enhancing Technologies*, (1):92 – 112, 2015.

[21] Gary Davis. Key findings from our survey on identity theft, family safety and home network security. 2018.

[22] Soteris Demetriou, Whitney Merrill, Wei Yang, Aston Zhang, and Carl A. Gunter. Free for all! assessing user data exposure to advertising libraries on Android. In *Proc. of the Network and Distributed System Security Symposium*. Internet Society, 2016.

[23] Manuel Egele, David Brumley, Yanick Fratantonio, and Christopher Kruegel. An empirical study of cryptographic misuse in android applications. In *Proc. of the SIGSAC Conf. on Computer & Communications Security*, pages 73–84. ACM, 2013.

[24] TNS Experts. 12 popular mobile ad networks for app monetization. thenextscoop.com/mobile-ad-networks-app-monetization/. Retrieved 2/26/19.

[25] Alvaris Falcon. 20 Advertising Networks to Monetize Your Mobile App. hongkiat.com/blog/mobile-app-monetizing-networks/, 2017. Retrieved 07/24/2018.

[26] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. Android permissions demystified. In *Proc. of the 18th ACM Conf. on Computer and Communications Security*, pages 627–638. ACM, 2011.

[27] Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steve Hanna, and David Wagner. A survey of mobile malware in the wild. In *Proc. of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, pages 3–14. ACM, 2011.

[28] Luanne Freund. Contextualizing the information-seeking behavior of software engineers. *Journal of the Association for Info. Science and Technology*, 66(8):1594–1605, 2014.

[29] Thomas Fritz and Gail C Murphy. Determining relevancy: how software developers determine relevant information in feeds. In *Proc. of the SIGCHI Conf. on Human Factors in Computing Systems*, pages 1827–1830. ACM, 2011.

[30] Vahid Garousi and Tan Varma. A replicated survey of software testing practices in the Canadian province of Alberta: What has changed from 2004 to 2009? *Journal of Systems and Software*, 2010.

[31] Google. Your content & YouTube Premium. support.google.com/youtube/answer/6306276, 2019. Retrieved 06/05/2018.

[32] Peter Leo Gorski, Luigi Lo Iacono, Dominik Wermke, Christian Stransky, Sebastian Möller, Yasemin Acar, and Sascha Fahl. Developers deserve security warnings, too: On the effect of integrated security advice on cryptographic API misuse. In *Proc. of the 14th Symposium on Usable Privacy and Security*, pages 265–281. USENIX Association, 2018.

[33] Donald Gotterbarn. Informatics and Professional Responsibility. *Science and Engineering Ethics*, 2001.

[34] Michael C. Grace, Wu Zhou, Xuxian Jiang, and Ahmad-Reza Sadeghi. Unsafe exposure analysis of mobile in-app advertisements. In *Proc. of the 5th ACM Conf. on Security and Privacy in Wireless and Mobile Networks*, pages 101–112. ACM, 2012.

[35] Matthew Green, Watson Ladd, and Ian Miers. A Protocol for Privately Reporting Ad Impressions at Scale. In *Proc. of the SIGSAC Conf. on Computer and Communications Security*. ACM, 2016.

[36] Jiaping Gui, Stuart Mcilroy, Meiyappan Nagappan, and William GJ Halfond. Truth in advertising: The hidden cost of mobile ads for software developers. In *Proc. of the 37th International Conf. on Software Engineering*, volume 1, pages 100–110. IEEE, 2015.

[37] Daniel Halbheer, Florian Stahl, Oded Koenigsberg, and Donald R. Lehmann. Choosing a digital content strategy: How much should be free? *International Journal of Research in Marketing*, 2014.

[38] Michaela Hardt and Suman Nath. Privacy-aware personalization for mobile advertising. In *Proc. of the ACM Conf. on Computer and communications security*, 2012.

[39] Morten Hertzum. The importance of trust in software engineers' assessment and choice of information sources. *Information and Organization*, 12(1):1–18, 2002.

[40] Emma Nuraihan Mior Ibrahim and Chee Siang Ang. Communicating Empathy: Can Technology Intervention Promote Pro-Social Behavior?—Review and Perspectives. *Advanced Science Letters*, 2012.

[41] David R Just and Brian Wansink. Smarter Lunchrooms: Using Behavioral Economics to Improve Meal Selection. *Choices*, 24(3), 2009.

[42] Dan Keating, Kevin Schaul, and Leslie Shapiro. The facebook ads russians targeted at different groups, 2017.

[43] John Koetsier. 33% Of Mobile Revenue Now Delivered By Video Ads; Rewarded Video Is Most Effective. forbes.com/sites/johnkoetsier/2017/07/31/33-of-mobile-revenue-now-delivered-by-video-ads-rewarded-video-is-most-effective/, 2017. Retrieved 07/24/2018.

[44] Nicola Lacetera, Mario Macis, and Robert Slonim. Will there be blood? Incentives and displacement effects in pro-social behavior. *American Economic Journal: Economic Policy*, 2012.

[45] Simon Lee. 7 surprising statistics about the world of app development. thisisglance.com/7-surprising-statistics-about-the-world-of-app-development/. Retrieved 2/22/19.

[46] Ilias Leontiadis, Christos Efstratiou, Marco Picone, and Cecilia Mascolo. Don't kill my ads!: Balancing privacy in an ad-supported mobile application market. In *Proc. of the 12th Workshop on Mobile Computing Systems & Applications*, pages 2:1–2:6. ACM, 2012.

[47] Dario Lolli. 'The fate of Shenmue is in your hands now!': Kickstarter, video games and the financialization of crowdfunding. In *Convergence: The International Journal of Research into New Media Technologies*, 2018.

[48] Matthew Lopez. Steemit business model – how does steemit make money? feedough.com/steemit-business-model-how-does-steemit-make-money/, 2018. Retrieved 2/27/19.

[49] Michael C. Loui and Keith W. Miller. Ethics and Professional Responsibility in Computing. In *Wiley Encyclopedia of Computer Science and Engineering*. 2008.

[50] Ginny Marvin. What Is An Ad Network? martechtoday.com/martech-landscape-what-is-an-ad-network-157618, 2015. Retrieved 07/24/2018.

[51] Niels Provos Panayiotis Mavrommatis and Marf Monrose. All your iframes point to us. In *USENIX Security Symposium*. USENIX Association, 2008.

[52] Aleecia M Mcdonald and Lorrie Faith Cranor. Beliefs and Behaviors : Internet Users ' Understanding of Behavioral Advertising. *38th Research Conf. on Communication, Information and Internet Policy*, 2010.

[53] Mathew Miles, Micheal Huberman, and Johnny Saldana. *Qual. Data Analysis: A Methods Sourcebook*. 2014.

[54] Mozilla. Responsible computer science challenge. foundation.mozilla.org/en/initiatives/responsible-cs/, 2018. Retrieved 2/26/19.

[55] Emerson Murphy-Hill, Da Young Lee, Gail C. Murphy, and Joanna McGrenere. How do users discover new tools in software development and beyond? *Computer Supported Cooperative Work (CSCW)*, 24(5), Oct 2015.

[56] Emerson Murphy-Hill and Gail C. Murphy. Peer interaction effectively, yet infrequently, enables programmers to discover new tools. In *Proc. of the ACM Conf. on Computer Supported Cooperative Work*, pages 405–414. ACM, 2011.

[57] Abhinav Pathak, Y. Charlie Hu, and Ming Zhang. Where is the energy spent inside my app?: Fine grained energy accounting on smartphones with eprof. In *Proc. of the 7th ACM Euro. Conf. on Computer Systems*, pages 29–42. ACM, 2012.

[58] Paul Pearce, Adrienne Porter Felt, Gabriel Nunez, and David Wagner. Addroid: Privilege separation for applications and advertisers in android. In *Proc. of the 7th ACM Symposium on Information, Computer and Communications Security*, pages 71–72. ACM, 2012.

[59] Akond Rahman, Asif Partho, David Meder, and Laurie Williams. Which factors influence practitioners' usage of build automation tools? In *Proc. of the 3rd International Workshop on Rapid Continuous Software Engineering*, pages 20–26. IEEE Press, 2017.

[60] Mark A Robinson. An empirical analysis of engineers' information behaviors. *Journal of the American Society for Info. Science and Technology*, 61(4):640–658, 2010.

[61] Paolo Roma and Daniele Ragaglia. Revenue models, in-app purchase, and the app performance: Evidence from Apple's App Store and Google Play. *Electronic Commerce Research and Applications*, 2016.

[62] William Samuelson and Richard Zeckhauser. Status quo bias in decision making. *Journal of Risk and Uncertainty*, 1988.

[63] Stephen Shankland. Ads are great, Google says, except for the 3.2 billion bad ones. cnet.com/news/google-removes-billions-of-bad-ads-in-2017-bans-publishers/, 2018. Online; retrieved 09/03/2018.

[64] Katie Shilton and Daniel Greene. Linking platforms, practices, and developer ethics: Levers for privacy discourse in mobile application development. *Journal of Business Ethics*, Mar 2017.

[65] Sooel Son, Daehyeok Kim, and Vitaly Shmatikov. What Mobile Ads Know About Mobile Users. In *Proc. of the Network and Distributed System Security Symposium*. Internet Society, 2016.

[66] César Soto-Valero and Mabel González. Empirical study of malware diversity in major android markets. *Journal of Cyber Security Technology*, 2(2):51–74, 2018.

[67] Statista. Most popular installed mobile monetization software development kits (sdks) across global mobile apps in 2017. statista.com/statistics/742408/leading-mobile-app-monetization-sdks/. Retrieved 2/22/19.

[68] Latanya Sweeney. Discrimination in online ad delivery. *arXiv preprint arXiv:1301.6822*, 2013.

[69] Ian Thomas. Online Ad Business 101, Part III - Ad Networks. liesdamnedlies.com/2008/07/online-ad-bus-1.html, 2008. Retrieved 07/24/2018.

[70] Vincent Toubiana, Arvind Narayanan, Dan Boneh, Helen Nissenbaum, and Solon Barocas. Adnostic: Privacy Preserving Targeted Advertising. *Proc. of the Network and Distributed System Symposium*, 2010.

[71] Minh-Dung Tran. Privacy challenges in online targeted advertising. theses.fr/2014GRENM053/document, 2014. Retrieved 06/05/2019.

[72] Jason Tsay, Laura Dabbish, and James Herbsleb. Let's talk about it: Evaluating contributions through discussion in github. In *Proc. of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering*, pages 144–154. ACM, 2014.

[73] Bartlomiej Uscilowski. Mobile adware and malware analysis. symantec.com/content/en/us/enterprise/media/security_response/whitepapers/madware_and_malware_analysis.pdf, 2013. Online; retrieved 09/03/2018.

[74] Narseo Vallina-Rodriguez, Jay Shah, Alessandro Finamore, Yan Grunenberger, Konstantina Papagiannaki, Hamed Haddadi, and Jon Crowcroft. Breaking for commercials: Characterizing mobile advertising. In *Proc. of the Internet Measurement Conf.* ACM, 2012.

[75] Vision Mobile. Distribution of mobile app developers in the United Kingdom (UK) in 2014. statista.com/statistics/320488/app-developers-by-age-and-gender-uk/. Retrieved 2/22/19.

[76] Vision Mobile. Share of mobile app development companies with fewer than five employees in the United Kingdom (UK), Germany and France in 2014. statista.com/statistics/320476/app-companies-with-fewers-than-five-employees-uk-germany-france/. Retrieved 2/25/19.

[77] Nevena Vratonjic, Mohammad Hossein Manshaei, Jens Grossklags, and Jean Pierre Hubaux. Ad-Blocking games: Monetizing online content under the threat of ad avoidance. In *The Economics of Info. Security and Privacy*. 2013.

[78] Jim Witschey, Olga Zielinska, Allaire Welk, Emerson Murphy-Hill, Chris Mayhorn, and Thomas Zimmermann. Quantifying developers' adoption of security tools. In *Proc. of the 10th Joint Meeting on Foundations of Software Engineering*, pages 260–271. ACM, 2015.

[79] Shundan Xiao, Jim Witschey, and Emerson Murphy-Hill. Social influences on secure development tool adoption: Why security tools spread. In *Proc. of the 17th ACM Conf. on Computer Supported Cooperative Work*, pages 1095–1106. ACM, 2014.

[80] Frederik Zuiderveen Borgesius. Improving Privacy Protection in the Area of Behavioural Targeting. *SSRN*, 2015.

A Survey Instruments

1. First, we would like to learn more about your experience as a mobile app developer. How many years have you worked in mobile app development?

   (a) Less than one year
   (b) Between 1 and 2 years
   (c) Between 2 and 3 years
   (d) Between 3 and 4 years
   (e) More than 5 years

2. What platforms have you developed apps for? (select all that apply):

   (a) Android
   (b) iOS
   (c) Blackberry
   (d) Windows Phone
   (e) Other (please specify)

3. How did you learn to develop mobile apps? (select all that apply):

   (a) Undergraduate major or course (e.g., BA in computer science)
   (b) Graduate major or course (e.g., masters degree in computer science)
   (c) Online course (e.g., a MOOC)
   (d) Self taught
   (e) Online tutorials
   (f) Workshop
   (g) On-the-job training
   (h) Other (please specify)

4. How many apps have you worked on in the last 3 years?

5. In the last 3 years, which role(s) have you carried out when working on mobile apps (select all that apply):

   (a) Developer, Programmer, or Software Engineer
   (b) Product or Project Manager
   (c) Tester or Quality Assurance
   (d) CEO or other high management / executive position
   (e) Sales / Marketing
   (f) User Support
   (g) Other (please specify)

6. Now we want to learn a little more about how you have integrated ads into apps. What role(s) have you played in regards to in-app advertising? Select all that apply.

   (a) I have been involved in choosing an advertising partner or advertising network for an app.
   (b) I have been involved in configuring the types of in-app ads shown in an app (e.g., where to place ads, what categories of ads to show, etc.)
   (c) I have been involved in integrating the necessary code into an app to enable in-app advertising
   (d) Other (please specify)
   (e) I have NEVER been involved in any way with regards to in-app advertising

7. Regarding mobile apps, have you used or worked with any advertising networks? if so, how often? (For each entry, participants answered to one of the following options: Have Not Used, Used in 1 app, Used in up to 3 apps, Used in up to 5 apps, Used in up to 10 apps, Used in more than 10 apps)

   (a) Google Ad Mob
   (b) ONE by Aol
   (c) InMobi
   (d) StartApp

(e) Smaato

(f) Flurry

(g) LeadBolt

(h) Unity Ads

(i) Other (please specify)

To learn more in-depth about your experience with in-app advertising, we want to ask you about a specific app you have worked in which you were especially involved with either choosing the advertising partner / advertising network to use, configuring what sort of ads are shown, or integrating the necessary code to display ads in the app.

8. Please name an app that utilizes in-app advertising and in which you were especially involved in decisions/integration regarding in-app advertising:

9. Please provide a link to this app in an app store/market (if unpublished enter N/A):

10. When did you work on the app?

11. What is the operating System for that app? Select all that apply.

    (a) Android

    (b) iOS

    (c) Blackberry

    (d) Windows Phone

    (e) Other (please specify)

12. Estimated company size for company that developed this app: (Options: 1-4, 10-19, 20-99, 100-499, 500-999, 1,000-4,999, 5,000-9,999, 10,000+)

13. Estimated development team size for team that developed this app: (Options: 1-4, 10-19, 20-99, 100-499, 500-999, 1,000+)

14. What role(s) did you have when developing this app? (select all that apply):

    (a) Developer, Programmer, or Software Engineer

    (b) Product or Project Manager

    (c) Tester or Quality Assurance

    (d) CEO or other high management / executive position

    (e) Sales / Marketing

    (f) User Support

    (g) Other (please specify)

15. How were you involved in the integration of ads into this app? (select all that apply):

    (a) I was involved in choosing the advertising partner(s) / advertising network(s) to use.

    (b) I was involved in deciding how ads are displayed in the app (e.g., where to place ads, what type of ads to show, etc.)

    (c) I was involved in integrating the ad network into the app

    (d) Other (please specify)

16. For each of the following role(s) with regards to in-app advertising, how involved were you in that role? (slider to the right = more involved)

    (a) Choosing what advertising partner / advertising network to use

    (b) Integrating the necessary code into an app to enable in-app advertising

    (c) Configuring the type of in-app ads shown (e.g., where to place ads, what categories of ads to show, etc.)

17. Revenue model of APP:

    (a) Free with In-App Advertising

    (b) Free with In-App Advertising, users can pay a fee to remove advertisements

    (c) Freemium model (app is free, certain features cost users money)

    (d) Paid download

    (e) In-App purchases (selling physical or virtual goods through the app)

    (f) Subscription (similar to Freemium, except instead of paying for extra features, users must pay for extra content)

    (g) Other (please specify):

    (h) Cannot remember

18. Who decided what revenue model to use in APP? (select all that apply):

    (a) Me

    (b) Programmer(s)

    (c) Project manager(s)

    (d) CEO and/or other upper level management

    (e) Investor(s)

    (f) Other (please specify):

    (g) I do not know who was involved in the decision process.

19. What ad formats does APP use? (select all that apply)

    (a) Banner ads (rectangular ads that occupy a portion of an app's layout; can be refreshed automatically after a period of time)

    (b) Interstitial ads (full-page ad format that appears at natural breaks and transitions, such as level completion in a game)

    (c) Native ads (advertisements presented to users via UI components that are native to the platform: for example, they can match the visual design of the app they are in)

    (d) Reward ads (Ad format that rewards users for watching ads)

    (e) Other (please specify)

    (f) Do not know / Cannot Remember

20. Who was responsible for choosing the ad formats used in APP? (select all that apply):

    (a) Me

    (b) Programmer(s) responsible for integrating the ad library code

    (c) Programmer(s) who were not responsible for integrating the ad library code

    (d) Project manager(s)

    (e) CEO and/or other upper level management

    (f) Investor(s)

    (g) Other (please specify):

    (h) I do not know who was involved in the decision process.

21. Which advertising networks, if any, were used in APP? (select all that apply):

    (a) Google Ad Mob

(b) ONE by Aol
(c) InMobi
(d) StartApp
(e) Smaato
(f) Flurry
(g) LeadBolt
(h) Unity Ads
(i) Other (please specify)
(j) No advertising network was used in this app.
(k) Cannot remember

22. Who decided what advertising partner / advertising network to use in APP? (select all that apply):

(a) Me
(b) Programmer(s)
(c) Project manager(s)
(d) CEO and/or other upper level management
(e) Investor(s)
(f) Other (please specify):
(g) I do not know who was involved in the decision process.

[If participant indicated they were involved in choosing an advertising network]

Your previous answers indicate that you were involved in selecting an advertising partner / advertising network for APP. These next questions will ask more about that process.

23. How important were the following resources in deciding what advertising partner / advertising network to choose for APP? [Not at all important, slightly important, moderately important, very important, extremely important, and an additional N/A option]

(a) Friends
(b) Colleagues (fellow developers/others internal to the company)
(c) Professional Network (fellow developers/others external to the company)
(d) Official website(s) of advertising partner / advertising network
(e) Official documentation and / or documents from advertising partners / advertising networks (e.g., SDK documentation, privacy policy, Terms of Service)
(f) Online blogs / magazine articles
(g) Online discussion forums (e.g., Reddit, StackOverflow)
(h) Other (please specify)

24. In choosing an advertising partner / advertising network for APP, what factors were considered, and how important were they in making the final decision? [Not at all important, slightly important, moderately important, very important, extremely important, and an additional N/A option]

(a) Revenue provided (e.g., eCPM rate)
(b) Ease of integration
(c) App user privacy
(d) Reputation of advertising partner / network
(e) Ad customization options offered (e.g., customize ad format, ad content, types of ads shown...)
(f) App user's security (e.g., likelihood of ads serving malware)

(g) App user's satisfaction / experience
(h) Resources used by ads (e.g., battery, network data)
(i) Other (please specify)

[Shown to all participants]

25. In what ways, if any, have the ads shown in APP been configured or customized? (select all that apply)

(a) Blocked certain advertisers / URLs
(b) Blocked certain categories of ads from being shown in the app
(c) Use only non-personalized or non-targeted ads
(d) Other (please specify)
(e) The ad content of APP has not been customized in any way
(f) I do not know if any configurations were made
(g) Prefer not to say

26. If the ads shown in APP were customized, who decided what configuration to use? (select all that apply):

(a) N/A / Ads were not customized
(b) Me
(c) Programmer(s) responsible for integrating the ad library code
(d) Programmer(s) who were not responsible for integrating the ad library code
(e) Project manager(s)
(f) CEO and/or other upper level management
(g) Investor(s)
(h) Other (please specify):
(i) I do not know who was involved in the decision process.

27. If decisions were made to configure the ad content, please explain why the ads in APP were configured this way? If the answer is not known, or not applicable, please respond N/A.

28. Some advertising partners / advertising networks collect data through the advertisements inside an app. What information does the advertising partner / advertising network used in APP collect or have access to? [Does have access, Probably has access, Probably does not have access, Does not have access, unsure]

(a) Device ID
(b) Operating System Information (e.g., what OS is on the device)
(c) Coarse Location
(d) Precise Location
(e) Age of user
(f) Gender of user
(g) Name of user
(h) Contact list of users
(i) Microphone
(j) Camera

29. Some advertising partners / advertising networks allow developers to customize what data is collected through the in-app ads and sent to an advertising partner / advertising network. If such customizations were made, who was in charge of that decision? Please select all that apply.

(a) Me

(b) Programmer(s) responsible for integrating the ad library code

(c) Programmer(s) who were not responsible for integrating the ad library code

(d) Project manager

(e) CEO and/or other upper level management.

(f) Investors

(g) Other (please specify):

(h) I do not know who was involved in the decision process.

(i) N/A / No customizations were made

30. Has APP experienced any of the following issues with regards to its advertising partners / advertising networks? If so, how often? [Never, Rarely, Occassionally, A moderate amount, A great deal, and an additional Unsure option]

(a) Failure to receive payment (or received late payment) from advertising partner / advertising network

(b) Advertising network account being deleted or banned without explanation.

(c) Inappropriate or undesired ads shown in app (e.g., an advertisement that displays explicit pornographic material, graphic violence)

(d) Malicious and/or harmful ads shown in app (e.g., advertisements that install malware onto user devices)

(e) Complaints from users about the type of ads shown in your app

(f) Advertisements not displaying in app

(g) Advertising network being slow or inefficient responding or addressing issues

(h) Being misled, lied to, or otherwise deceived by advertising network's policies and guidelines.

(i) Excessive data collection by advertising network

(j) Other (please specify)

31. If any of the above issues were experienced, please briefly describe what steps, if any, were taken to address them (if no steps were taken, please write N/A):

32. Did the advertising partner for APP change in the time you worked on this app?

(a) Yes

(b) No

(c) Do not know / Unsure

[Shown only if answer to Q32 was yes]

33. What reasons prompted the change of advertising partners / networks for APP, and how important were they in making the decision to change? [Not at all important, slightly important, moderately important, very important, extremely important, and an additional N/A option]

(a) Competitor offered better revenue (e.g., higher eCPM (effective cost per one thousand impressions) rates)

(b) Competitor offered more customization options (e.g., more customizability with regards to what ads to place)

(c) Competitor offered an overall better product (e.g., offered higher quality ads)

(d) Advertising partner / advertising network displayed ads that were harmful to users of the app (e.g., the ads installed malware on user devices).

(e) Advertising partner / advertising network displayed ads that were explicit (e.g., advertisements that showed pornography, ads that showed graphic violence).

(f) Other (Please Specify)

Now we want to learn a bit more about your perception of advertising networks.

34. For each of the following statements, please indicate to what degree you think the statement is true. [Definitely false, Probably false, Neither true nor false, Probably true, Definitely true]

(a) Advertising networks provide valuable sources of income for app developers.

(b) Advertising networks collect user data without consent from the user

(c) Users can opt-out of data collection from advertising networks if they so wish.

(d) Users can opt-out of receiving targeted advertisements from advertising networks if they so wish.

(e) Advertising networks help streamline the process for apps to display ads.

(f) Advertising networks show advertisements that install malware on user devices.

(g) Advertising networks show advertisements that show explicit and graphic advertisements (e.g., pornographic material, explicit violence and gore, etc.)

(h) Advertising networks sell user data to government agencies (e.g., the FBI)

(i) Advertising networks have an overall positive impact on the app ecosystem

(j) I am concerned about the data collection practices of advertising networks

Sometimes, when an app uses an advertising network to display ads, an ad can be shown that is either harmful to users (e.g., installs malware on user devices) or otherwise illegal (e.g., displays explicit ads for terrorism or prostitution).

35. If such a thing happens, who do you think SHOULD BE responsible for fixing the issue? [Not at all responsible, Somewhat responsible, Mostly responsible, and Completely responsible]

(a) Network

(b) App

(c) Government Agency (E.g., the FTC or the FBI)

36. If such a thing happens, who is currently responsible for fixing the issue? [Not at all responsible, Somewhat responsible, Mostly responsible, and Completely responsible]

(a) Network

(b) App

(c) Government Agency (E.g., the FTC or the FBI)

Thank you for your time! We are almost done. We would like to ask you to complete some basic demographic questions:

37. Please enter current age in years, in a number format (if you'd prefer not to say, enter 0):

38. What is your gender?

(a) Male

(b) Female

(c) Non-binary

(d) Other (please specify)

(e) Prefer not to say

39. Highest level of education achieved (if currently enrolled, highest degree received.):

    (a) No schooling completed

    (b) Some high school, no diploma

    (c) High school graduate, diploma or the equivalent (for example: GED)

    (d) Some college credit, no degree

    (e) Trade/technical/vocational training

    (f) Associate degree

    (g) Bachelor's degree

    (h) Master's degree

    (i) Professional degree (e.g., J.D., M.D.)

    (j) Doctorate degree

    (k) Prefer Not To Say

40. Current employment status:

    (a) Full time employment for salary / wages

    (b) Part time employment for salary / wages

    (c) Self-employed

    (d) Unemployed

    (e) A homemaker

    (f) A student

    (g) Retired

    (h) Unable to work

    (i) Prefer Not To Say

B Interview Protocol

1. First, I'd like to learn more about your experience developing mobile apps. How did you get into mobile app development?

2. What is your current role? What role(s) have you played in the past? How has working on them been like?

3. Now I want to ask a bit more about in-app advertising. Can you describe the purpose of an ad network and how it functions to provide ads in your app?

4. What is your experience with advertising networks? Which ones have you worked with? What was this like? How long have you worked with ad networks? What role(s) have you played in working with them?

5. Now I want to talk in depth about a specific app you have worked on in which you were heavily involved in incorporating ads into your app. Describe a typical day working on APP. What was your role? How were ads used in APP? Was an ad network used? Do you remember which one? Why was it decided to use advertising in APP?

   I want to focus on your experiences with APP. But feel free to mention experiences you have had with other apps.

6. What were the reasons why advertising was used in APP? What is the business model of APP? Can you walk me through how the model was chosen? Was an alternative without advertisements considered? Why / Why not?

7. Walk me through the decision to use [AD NETWORK]. Who was involved in making that decision? What were you looking for in an ad network? I.e, what were your priorities? Why

was this particular ad network chosen? How much time was spent researching each company? Were other ad networks considered? Why was [AD NETWORK] chosen over other ad networks? Are you using other ad networks in parallel? Do you utilize mediation?

8. What resources, if any, did you use to help choose what ad network to use? Walk me through how they were used.

9. Walk me through the process of integrating the ad library code into your app. How easy or difficult was it to integrate the ad library code into your app?

10. Some ad networks allow you to customize what permissions are needed for the app to function. Do you remember what permissions were set in APP? Why were they set / not? How did you (or your team) come to this decision?

11. Some ad networks collect data about the phone that uses the app. Do you know what data the ad network collects through APP?

12. With [AD NETWORK] you can choose what data is sent to the advertiser to deliver better targeted ads. Do you know what data is sent to the ad network through APP? Why / Why not? Do you see any issues with this sharing of data?

13. Do you know if the ads shown by your ad network are targeted? Do you know if you can change this to non-targeted ads? Have you ever explored the option of non-targeted ads? Which ones do you use? Why? What are your own views on targeted advertisements?

14. With [AD NETWORK] you can configure what category of ad your app shows – for example, you can choose where apps that show clothing appear in your app, or block a certain vendor or advertiser from your app. Have you ever blocked a certain category from your app? Why or why not? Have you ever blocked a specific advertiser from your app? Why or why not?

15. Have you had any experiences with ad networks that are different from the ones you have just described?

16. What are the main benefits you see with advertisement networks?

17. What are the main issues you see with ad networks?

    Some ad networks have been known to show advertisements that are offensive or harmful to users (e.g., ads that display pornographic or offensive material, ads that download malware onto user devices...)

18. Have you ever received complaints that there have been these bad ads on one of your apps? If so, how did you deal with them?

19. Have you ever checked the ads on your ad network for these issues? If so, how?

20. Do you know your ad networks policy on these sorts of ads?

21. If a harmful ad like this is found in an app, whose responsibility is it to remove it? Why?

22. Now I will walk through series of issues that have been identified with ad networks. I want to know if your company/team were aware of these issues, and if so, if any steps were taken to mitigate them? (Issues mentioned: malware, inappropriate / offensive content, battery draining due to sharing of data, using up user's mobile data plan, companies obtaining user data without explicit permission.)