Mohammad Tahaei*, Kopo M. Ramokapane, Tianshi Li, Jason I. Hong, and Awais Rashid

Charting App Developers' Journey Through Privacy Regulation Features in Ad Networks

Abstract: Mobile apps enable ad networks to collect and track users. App developers are given "configurations" on these platforms to limit data collection and adhere to privacy regulations; however, the prevalence of apps that violate privacy regulations because of third parties, including ad networks, begs the question of how developers work through these configurations and how easy they are to utilize. We study privacy regulations-related interfaces on three widely used ad networks using two empirical studies, an expert review and think-aloud sessions with eleven developers, to shed light on how ad networks present privacy regulations and how usable the provided configurations are for developers.

We find that information about privacy regulations is scattered in several pages, buried under multiple layers, and uses terms and language developers do not understand. While ad networks put the burden of complying with the regulations on developers, our participants, on the other hand, see ad networks responsible for ensuring compliance with regulations. To assist developers in building privacy regulations-compliant apps, we suggest dedicating a section to privacy, offering easily accessible configurations (both in graphical and code level), building testing systems for privacy regulations, and creating multimedia materials such as videos to promote privacy values in the ad networks' documentation.

Keywords: usable privacy, software developers, ad networks, privacy regulations, CCPA, COPPA, GDPR

DOI Editor to enter DOI

Received ..; revised ..; accepted ...

***Corresponding Author: Mohammad Tahaei:** University of Bristol, E-mail: mohammad.tahaei@bristol.ac.uk

Kopo M. Ramokapane: University of Bristol, E-mail: marvin.ramokapane@bristol.ac.uk

Tianshi Li: Carnegie Mellon University, E-mail: tianshil@cs.cmu.edu

Jason I. Hong: Carnegie Mellon University, E-mail: jasonh@cs.cmu.edu

Awais Rashid: University of Bristol, E-mail: awais.rashid@bristol.ac.uk

1 Introduction

Showing ads to users is a widely adopted app monetization method; on Android, about 77% of free apps contain an ad library [32, 35]. This broad adoption enables ad networks to collect data from users and track their behavior in all types of apps such as in free and paid apps, children-directed apps, as well as health-tracking apps [10, 30, 64, 68, 89]. With the recent introduction of privacy regulations such as the California Consumer Privacy Act (CCPA) [61], the Children's Online Privacy Protection Rule (COPPA) [16], and the General Data Protection Regulation (GDPR) [63], ad networks have started to give app developers "configurations" in the form of graphical and code configurations on the ad networks to make their libraries compliant with the regulations (e.g., by restricting data collection for European and Californian users).

Developers may have two potential motivations to use these configurations, first to follow the regulations to avoid fines (several software companies got fined in the past few years because of privacy violations [42]), and second, they may have privacy concerns for users as some developers expressed such opinions in developer forums [45, 76]. However, developers often stick to the default privacy-unfriendly configurations [52] which begs the question of how developers work through these configurations and how easy they are to utilize.

When looking at the ad networks' interfaces with privacy configurations, they may contain dark patterns (i.e., "tricks used in websites and apps that make you [users] do things that you [they] didn't mean to" [13]) making it challenging for developers to discover the configurations, understand what they do, and implement them [74]. The defaults are also often not in favor of users and are set to maximize data collection [52, 74]. Developers may as well leave the defaults as they are, which in turn means building privacy-unfriendly apps for users [52]. Examples include defaults that are set to show personalized ads and not limit data processing [74]. The inconsistencies in the privacy configurations may also result in violating privacy regulations. In the example of COPPA non-compliant apps, developers use the required configurations (e.g.,

CC BY-NC-ND

app_limit_tracking, opt_out, and COPPA) inconsistently causing apps to violate children's privacy [64].

While prior research shows that ad networks' privacy interfaces may contain dark patterns and may be challenging to use for developers, it lacks an empirical study to understand how developers find these platforms when trying to integrate a privacy regulations-compliant ad. We contribute to the evolving body of work in supporting developers in performing privacy tasks by investigating configurations and information presented to developers about privacy regulations in ad networks to pinpoint design issues. Our research questions (RQs) are developed to extend the body of research in this area:

RQ1: How do ad networks present information about privacy regulations in their documentation?

RQ2: How do developers find ad networks' support for complying with privacy regulations?

RQ3: How can ad networks improve their privacy regulations support for developers?

We conducted two studies on three widely used ad networks (i.e., Facebook Audience Network, Google AdMob, and Twitter MoPub) to answer our research questions: (1) an expert review to find all the privacy regulations information available on the ad networks, and (2) think-aloud sessions with eleven developers to uncover their challenges while trying to integrate an ad and comply with privacy regulations.

We find that information about privacy regulations is scattered in various places on the studied ad networks, making it difficult for developers to know what to do to comply with privacy regulations. Participants were frustrated with the amount of documentation they had to read, terms and abbreviations that they did not understand, and highlighted the need for a central place for all the information about privacy regulations. One of the strategies that they would apply to make their app compliant with regulations was to follow the documentation as it is, highlighting the importance of having privacy-friendly defaults on the documentation.

We recommend improving the documentation design by dedicating a section to privacy, unifying the terms and language used to explain privacy, eliminating the dark patterns, and integrating the privacy features in the developers' workflow. We further discuss future research avenues to support developers in performing privacy tasks, for example, by building test systems to assist developers in complying with privacy regulations (and also knowing when they are or are not compliant) and improving developers' mental models about ad networks to go beyond the concept of notice-and-consent, which is potentially rooted in the ad networks' language. Such improvements may make developers aware of privacy-invasive business models of ad networks as well as the detrimental privacy consequences of data collection by ad networks on users.

2 Related Work

Our work contributes to the privacy literature that focuses on understanding developers' needs for integrating privacy and building usable tools for software developers to empower them to create privacy-friendly apps for their users [3, 6, 29, 38, 44–46, 66, 67, 74, 76, 77, 80, 85].

2.1 Privacy Regulations

The three major privacy regulations that we discuss in this paper are: the California Consumer Privacy Act (CCPA, covers Californian users) which "gives consumers more control over the personal information that businesses collect about them," [61] the Children's Online Privacy Protection Rule (COPPA, covers users in the United States) which "imposes certain requirements on operators of websites or online services directed to children under 13 years of age," [16] and the General Data Protection Regulation (GDPR, covers European users) which is for "the protection of natural persons with regard to the processing of personal data and on the free movement of such data." [63]

Privacy regulations manifest themselves in the software design often as the notice-and-consent concept [86]. However, the effectiveness of these consent forms is under question as many of them do not provide a "reject all" button [58] making it difficult for users to make an informed choice [82].

Privacy policies, as another example of privacy regulations implications, are notoriously hard to read and understand for users, and a majority of users do not read them [59, 81]. While all studies about the impact of privacy regulations focus on the implications and design changes for end-users, our study aims to look at how these regulations manifest themselves in software development documentation used by developers who build apps adopted by hundreds or millions of users.

2.2 Online Advertising Networks

One way to monetize apps is to show ads to users. Over half of Android apps use ads to generate revenue [7, 8], which in turn often enables users to use the app without paying, but the price comes with seeing ads.

Mobile apps, as one of the enablers of ad networks, collect and track users in free and paid apps, children-directed apps, and health-tracking apps [10, 30, 64, 68, 89]. Targeted ads can influence the masses by analyzing human behavior and tailoring materials to individuals (e.g., shifting political views [20, 22, 88] and purchasing behaviors [15, 43]). There is a split between users' view of targeted ads, some finding them useful while others finding them intrusive, invasive, and creepy [47, 51, 60]. However, overall, users expect ad networks to provide transparency and control to them [22].

From a software development viewpoint, integrating an ad network into an app is straightforward. Developers usually only need to add a library to their project, and the library handles the rest. This light procedure could also enable ad networks to collect information about users, such as location information and identifiers they may share with their partners. It is also notable that all permissions in an Android app are shared within the project. Sharing permissions means that if a developer asks for fine location permission from the users for their app, other libraries can use the same level of permission without asking for permission from the user [69]. Unnecessary permissions (e.g., access to data storage, location, and camera) are not only prevalent in free apps but also visible in paid apps [10, 30], giving third parties such as ad networks access to users' sensitive data including contacts list and location [30], which highlights the prevalence of data collection from users in the app ecosystem by third parties.

Besides, there are "configurations" given to developers both as graphical and code-level configurations to limit the data collection by ad networks and to comply with privacy regulations [74]. However, it is yet not clear how usable are these configurations. We contribute to the ad networks body of work by studying how privacy regulations are presented to developers in ad networks.

2.3 Privacy Studies With Developers

After recognition of the human factor as one of the main elements of secure systems in the early 2000s [1, 87], in the 2010s, researchers started to study security and privacy interfaces directed at developers. Early work found that security libraries and tools can be unusable and counterintuitive (e.g., cryptographic libraries and static analysis tools), resulting in developers not being able to fully benefit from these tools or sometimes making mistakes that can lead to security vulnerabilities [21, 24, 28, 73, 79]. Moving to the privacy domain, privacy is often overloaded with legal language, which makes it difficult for developers first to understand it and second to transfer it to technical requirements [11, 77]. Developers find it difficult to work with permissions on mobile apps and write a privacy policy which is required by app stores [45, 76]. Another barrier for privacy is to use a security language in software teams to cover privacy requirements which undermine the value of privacy and limits its coverage [29, 77].

Ad networks, as a software development platform, use privacy-unfriendly defaults [74] and developers often stick with the defaults [52] which in turn would result in ad networks collecting more data from users. For example, a sample code that asks for user consent would appear continuously on the user side asking for consent, and it stops appearing only when the user consents to ads personalization [74]. Developer-facing privacy interfaces on ad networks also contain dark patterns that may nudge developers into making privacy-unfriendly decisions [74]. An example is to have personalized ads turned on by default. However, nudging them into making a privacy-friendly decision is possible by making privacy salient and integrating the privacy consequence of their choices within the interfaces [78]. We expand this body of work by looking at the three widely used ad networks in mobile apps to understand whether developers can find information about privacy regulations and how they would understand this information. Our study includes think-aloud sessions with developers and highlights usability issues, while others focused on developers' adoption of ad networks [52] or did an expert review of privacy pages to find dark patterns [74].

3 Method

We conducted two studies to answer our RQs: (1) an **expert review:** two researchers searched for interfaces related to privacy regulations in ad networks; we searched extensively to find all the possible routes to privacy-related information on the three chosen ad networks (RQ1 and RQ3); (2) a **think-aloud study**: we recruited eleven developers for a think-aloud study to understand developers' challenges and understandings of

interfaces related to privacy regulations in ad networks (RQ2 and RQ3). We analyzed three widely used ad networks in mobile apps [4, 36, 83]: Facebook Audience Network, Google AdMob, and Twitter MoPub (In October 2021, "AppLovin has agreed to acquire MoPub from Twitter for approximately $1 billion in cash." [23] At the time of writing this paper, MoPub is still branded under Twitter) to answer our RQs. Sample screenshots of pages related to privacy regulations are included in Appendix C. Our study was approved by the ethics committee of our organization.

3.1 Expert Review: Searching for Privacy Regulations Interfaces

To answer RQ1 and RQ3, two authors with software engineering and usable privacy backgrounds, independently built diagrams that covered pages related to privacy regulations in the three studied ad networks. Our main effort in this part was to be exhaustive, search for as many pages as possible, and find all the related information to our selected regulations. We played the role of a savvy privacy developer and made all the effort to find the available information about privacy regulations. The activity was similar to an expert review where experts critically look for usability issues in a system [31].

We built a workflow diagram of the steps that a developer would need to take to get to all the information about privacy regulations from the documentation. The goal was to understand the extent of privacy information and where developers need to find such information. We started with the "Get Started" page on each ad network and studied the linked pages (in September-October 2021). We continued going to the linked pages until we reached an external link, and it no longer sent us to an internal page. We logged in to the ad network and ran the same procedure to find related pages in the developer's account pages. We recorded the text, hyperlinks, and the title of the target page. We also flagged pages with any graphical and code configurations because we were interested in knowing what configurations are given to developers for privacy regulations.

To reduce the complexity of diagrams, we decided to focus on Android-specific pages as Android is the most common mobile operating system [72]. The researchers then merged their findings and resolved disagreements through discussions. Section 4.1 is based on the findings of this analysis. The diagrams are included in Appendix D to show the depth and complexity; however, they require zooming to see all the details.

3.2 Think-Aloud Study

To answer RQ2 and RQ3, we conducted a think-aloud study [57] with eleven participants to understand developers' challenges in using ad networks' documentation to integrate a privacy regulations-compliant ad. The think-aloud method is one of the classic methods for evaluating the usability of a system [57]. It is also recommended for evaluating software development tools [55].

3.2.1 Screening Survey

We first sent out a screening survey with questions about experiences with software, mobile, Android, and iOS development, as well as knowledge of privacy regulations and general demographics questions (see Appendix A). We then invited candidates with at least two years of experience in either Android or iOS app development. On average, the survey took 4.7 minutes to complete ($SD = 2.3$ minutes) for most participants (10/11); one participant took the survey in 19.1 hours.

3.2.2 Recruitment

We recruited participants from four channels: Freelancer.com, CS student mailing list, Prolific, and social media. These channels have been used to recruit participants for studies with developers [73, 79, 84].

Freelancer.com. We posted our project on Freelancer.com for developers to bid on. We then messaged 40 freelancers to fill out the screening survey. We invited eight candidates to the main study, out of which three agreed to participate.

CS student mailing list. We sent out our recruitment ad to two CS student mailing lists (both included undergraduate and postgraduate students) in two research universities in Europe with the screening survey link. We got two participants from this channel.

Prolific. We sent out the screening survey to 150 Prolific users who stated that they had programming skills, were fluent in English, were not a student, were full-time employed, had an approval rate of over 90%, and were willing to participate in a video call interview. Survey takers received $0.40, in line with minimum wage in our university's home country. We invited 30 candidates, sending them the study details, out of which three attended the study. We used the first participant as our pilot; therefore, two were included in the main findings.

Social media. We posted the recruitment ad on our personal Twitter and Linkedin accounts, posted on eight Linkedin software development-related groups, and sent direct messages to 57 Linkedin users with mobile development titles. We got one participant from our tweets and two participants from Linkedin. Another participant said they found us on a Slack channel where other people posted about our study.

In total, we received 67 complete survey responses from Freelancer.com, CS student mailing lists, and social media, sent invitations to 29 candidates, out of which nine agreed to participate in our study. As mentioned above, we also recruited two participants from Prolific, giving us in total eleven participants.

3.2.3 Participants' Demographics

Table 3 in the Appendix shows a summary of participants' demographics. Ten participants worked in a software development role in their most recent job; P11 is a bioinformatics researcher who also builds apps; two are students, five focus on Android, five focus on iOS, and one focuses on Unity; on average, they have 6.5 years of experience in software development ($SD = 4$), 4.5 years of experience in mobile development ($SD = 2.7$), 3.1 years of experience in Android development ($SD = 1.7$), and five years of experience in iOS development ($SD = 3$); seven are currently in Europe, and four are currently in Asia; nine identify as male, and two identify as female. Except for two participants, they all had worked with at least one ad network in the past three years, Google AdMob was the most commonly used ad network (8/11), Facebook Audience Network, Unity Ads, and Flurry were some of the other used ad networks.

When asked about their knowledge of regulations regarding GDPR, four were very knowledgeable, two were moderately knowledgeable, four were slightly knowledgeable, and one did not have any knowledge; about CCPA, one said moderately knowledgeable, and the rest were not knowledgeable at all (perhaps because they live in Asia and Europe); regarding COPPA, one was very knowledgeable, three were moderately knowledgeable, three were slightly knowledgeable, and four were not knowledgeable at all.

3.2.4 Study Procedure

Participants were sent the consent form and participant information sheet before the study. At the start of the sessions, we also briefly gave a summary of the study to participants and then read aloud the consent form for verbal informed consent. Then, we asked them questions about their job and apps, knowledge of privacy regulations, if they have used any ad networks and why (not), and what kinds of data their apps collect from users.

The study continued by giving participants example videos of think-aloud studies [9, 56] and explaining to them what they need to do with a simple practice round. The interviewer then sent the link to the "Get Started" page of the ad network and read the task for the participant: "Integrate a banner ad in the provided app that is compliant with CCPA, COPPA, and GDPR." We had already created an account on the ad networks to minimize time spent on unrelated tasks and sent this to the participant if they wanted to log in.

After each ad network, we asked questions about their experience, easy-to-understand parts, challenging sections, how they would check for the compliance of their app, and design suggestions for making the privacy regulations interfaces usable for them.

We used a Latin square design [70] to assign an order of ad networks to each participant. We audio-recorded the calls, and participants shared their screens with us when they were doing the tasks. We decided not to record the screen because of privacy concerns. The interviewer took notes during the call.

To reduce participants' cognitive load, we capped all sessions to two hours, resulting in some participants not having enough time to see all the ad networks. All ad networks were seen by nine participants.

We used our organization's Zoom service to run the study. The calls took 90 minutes on average, based on the transcripts time, which excludes 5-10 minutes introduction and consent reading in the beginning and 5-10 minutes break. Participants received an equivalent of $53 for their time.

3.2.5 Qualitative Analysis

We transcribed the think-aloud sessions using professional GDPR-compliant services. Two authors then analyzed the transcripts using thematic qualitative coding in Nvivo [34]. First, they independently read one script and built a codebook using an inductive approach with open codes [53, 65]. As the think-aloud sessions covered materials unrelated to privacy regulations, we decided to focus on the parts in line with our research questions (i.e., the privacy parts). Then, they merged their codebooks, discussed their findings,

and resolved conflicts. They followed this procedure for seven scripts while modifying and updating the codebook, meeting regularly to resolve conflicts, and communicating their findings with two other authors for further input and feedback. Recruitment was an ongoing process during this period. After the seventh round, they did not observe new themes coming up, suggesting that they reached saturation; therefore, we stopped recruiting participants. Though, we already had recruited eleven participants at this stage.

Two authors then independently re-coded all the eleven think-aloud sessions with the final codebook (codes are not mutually exclusive, and a quote may appear in multiple codes). Their overall inter-rater Cohen's kappa agreement was .56, which is considered as moderate agreement [40, 41]. The think-aloud sessions resulted in unstructured data because participants were speaking their thoughts while doing a cognitive task which is different from an interview where people have time to think and speak. Therefore, we believe the agreement rate between coders is overall good. Also, one of the coders observed participants during the study, and the other coder did not, giving them an advantage for observations. To resolve disagreements, the coders had long discussions (32 hours) and further discussed their findings with two other authors, who were not directly involved in the coding. The findings in Section 4.2 are based on the final codebook.

3.3 Limitations

Although in searching for privacy interfaces, we did try to be exhaustive, we cannot claim that we covered all the sections and available information. Having two authors independently going through the pages reduced the chances of missing related information; however, we might have missed parts.

To diversify our sample, we made an effort to prioritize invitations to candidates based on their gender and location. After our fifth participant, we first invited participants that were non-male and located outside Asia and Europe. Despite this, our sample is predominately male (consistent with the gender-biased software development profession, over 90% of software developers are male [71]) from Asia and Europe.

In addition, recruiting developers remains a challenging task [75], perhaps due to the relatively low compensation as compared to their hourly wages and the complexities of the study tasks. Future research may want to design more effective developer recruitment mechanisms and conduct further analysis with a larger and more diverse sample. We also acknowledge that our sample is small and our results may not be generalizable to a larger population of developers.

Our method does not provide data about how developers would behave and work in a real-world scenario. We primed our participants with privacy and directly tasked them to find information about privacy regulations because our research questions were centered around privacy. Such a scenario may not be representative of how developers work (functionality is often the primary task compared to privacy and security requirements [73]). However, we consider our method a necessary first step to understanding developers' approaches in performing privacy tasks. Our study shows the usability issues and the challenges a developer might face while working with privacy-related interfaces on ad networks. Our expert review also sheds light on the vast number of pages and interfaces developers need to build a privacy-compliant app. Future research may measure developers' ability in building apps that are compliant with privacy regulations (e.g., by taking an ad network as an example library) by asking developers to write code, follow the documentation, and see if they can build a functional app considering all privacy regulations.

Although it may be helpful to analyze the resulting configurations from the study and see how often developers configure things correctly or not, we did not record participants' screens for privacy reasons and therefore do not have the data for this analysis. Future research may further investigate the developers' actual behaviors when dealing with these types of tasks and explore techniques that can help developers better navigate the complicated interfaces. Additionally, to know whether a mental model is correct, we needed extensive knowledge about how the ad networks handle the network-level data, which our research does not cover. Future research may check the consequences of a configuration in reality (perhaps by checking transmitted data) and whether developers' understanding is correct about it.

4 Findings

We first present the results from our expert review (Section 4.1) and then move on to what our participants discussed in the think-aloud sessions (Section 4.2). Table 1 shows an overview of our findings emerging from each.

Table 1. Overview of our findings from the two studies.

Finding	Expert review (§4.1)	Think-aloud study (§4.2)
Mental models of privacy configurations		✓
Compliance check		✓
Information-seeking strategies		✓
Usability of ad networks libraries	✓	✓
Quantitative insights	✓	

4.1 Expert Review: Where Are All the Privacy Regulations?

Through the analysis of the documentation of the three ad networks (RQ1, Table 2), we identified 26, 66, and 30 unique web pages from Facebook Audience Network, Google AdMob, Twitter MoPub, respectively, that had information about the privacy regulations either by directly mentioning them or an implied mention (such as talking about protecting children's privacy but not explicitly mentioning COPPA). Among these pages, 16, 36, and 27 pages in Facebook Audience Network, Google AdMob, and Twitter MoPub, respectively, explicitly mentioned a privacy regulation. In terms of the number of times a regulation was mentioned regardless of the platform, GPDR was the most mentioned with 39 pages, CCPA was second with 23 pages, and COPPA with 17 pages suggesting that the ad networks spend more time creating materials and covering GDPR compared to the other two regulations. We note that not all these pages are required for an app, and a developer may need to go through parts of these sections to make their app compliant with specific regulations.

Besides internal privacy-related pages, ad networks gave **links to external pages** (10, 11, and 2 pages in Facebook Audience Network, Google AdMob, and Twitter MoPub, respectively) such as government legal documents, GitHub repositories, and privacy policies of the third parties. For example, one page had 1038 links to partners' privacy policies, and another page had links to five regulatory documents about cookies and tracking.

4.1.1 Potential Usability Issues

By looking at Table 2, potential usability issues can be uncovered: (1) Only a **small portion** of the privacy support pages provide sample code or a graphical configuration as an easy way to comply with the regulations. (2) The median and max depth of the pages suggest that many privacy support pages are **buried deep** and therefore hard to locate. (3) The large number of clicks required to access all privacy support pages suggests that these pages are **scattered across the documentation**. Hence, exhaustively finding (reading, understanding, and acting set aside) all privacy support pages may incur a **significant overhead**. (4) While all regulations are presented in the three ad networks, the **differences and inconsistencies** make it difficult to follow all of them. For example, the required graphical and code-level changes vary across regulations and platforms. For instance, at the platform level, in Facebook, developers mostly need to make code configurations, but one graphical configuration for CCPA is also available under the developer panel to limit data tracking for Californian users. Another example is that a configuration in Facebook does not support GDPR, though represented by five code and one graphical configuration in Google, and three code and one graphical configuration in Twitter. Overall, we find that there is **no systematic, unified, and standard approach** for presenting privacy regulations in developer-facing documentation.

4.1.2 Dark Patterns

Several design issues that we found resonate with the current discourse in the end-users research community around **dark patterns** [14, 26, 27, 48]. Using Gray et al.'s [26] categories, we matched our findings to the dark patterns literature: (1) buried and scattered information related to "hidden information", (2) "false hierarchy" occurred when two choices were given for creating a consent form, but the first choice did not include a reject button in the consent form, (3) "preselection" happened when ad personalization was set to personalized ads by default, (4) "sneaking" took place when by-products of an ad network (e.g., analytics) were offered and preselected by default while developers are agreeing with the terms and conditions, and (5) "obstruction" occurred because of the complex language and terms that are not easy to understand for developers as well as the inconsistencies across them creating a barrier for developers in integrating privacy regulations.

4.2 Think Aloud With Eleven Developers

We analyzed the eleven think-aloud sessions and constructed four overarching themes (RQ2 and RQ3): mental models (i.e., people's understanding of a domain in the world [5]) of ad networks, compliance check, information-seeking strategies, and usability. We do not intend to make specific conclusions and judgments

Table 2. Privacy regulation compliance support in the three studied ad networks. Depth is defined as the minimum clicks to reach a page. We consider the Get Started page takes one click to open and has a depth of 1. The sum of clicks shows the clicks one needs to take to access all pages from the Get Started page.

	Facebook Audience Network			Google AdMob			Twitter MoPub			Total
	CCPA	COPPA	GDPR	CCPA	COPPA	GDPR	CCPA	COPPA	GDPR	
Privacy regulations pages	6	5	5	12	6	18	5	6	16	79
Pages with a sample code	2	3	4	2	3	4	0	0	3	21
Pages with a graphical configuration	1	3	0	1	0	1	0	1	1	8
Median depth	4.5	3	4	3.5	3	5	5	4	3	-
Min depth	2	2	3	2	1	1	3	3	1	-
Max depth	5	4	5	5	4	6	5	5	5	-
Sum of clicks from Get Started	24	16	20	44	17	70	22	24	53	290

about specific platforms and regulations in reporting our findings. Therefore, we do not refer to a specific ad network or regulation as we were interested in finding developers' challenges in building privacy-friendly apps.

4.2.1 Mental Models of Privacy Configurations

We were interested in participants' understanding of privacy configurations in ad networks. We asked participants what they think would happen if they change a privacy configuration such as a code-level configuration (e.g., `forceGDPRApplies` in Twitter MoPub) or changing a graphical-level configuration (e.g., CCPA configurations in the developer panel in Google AdMob where developers can restrict processing of users data). We observed three main mental models that participants associate with such changes:

4.2.1.1 Data processing will change

A majority of participants reported that there would be some **changes on the back end**, restrictions over data processing, or how data is collected and tracked. However, we did not get an in-depth understanding of what such tracking and collection mean, and all the mentions included a general description of data processing changes: "It means that it will have consent for doing whatever data is to be tracked." (P5)

4.2.1.2 Ads' content will change

Besides back-end changes, some participants explained that the **users' front end would change** based on the changes to the configurations. Participants' thoughts were consistent with the language that the ad networks used to explain the changes to the developers. For example, by turning the ads personalization on, users will see ads that are tailored to them: "Age, location, or interest, and – based on these categories – these publishers can send ads to these people." (P2)

4.2.1.3 The user will see an interface

Similar to changes on the front end, several participants brought up an **interface popping** (e.g., a consent form, a warning, or a notification) on the user side when they make changes to the ads configurations. For example, if the GDPR configuration is set to on, then users will see a consent form: "Every time the user opens the app, they'd need to be prompted whether they can send it to advertising information." (P1)

4.2.2 Compliance Check

When asked how they would make their app compliant, all the participants expressed some challenges in making it compliant. They reported **not knowing** how to or not finding any information that could help them to comply: "It's impossible because I wanted to make sure that my app complied with CCPA and this COPPA, but they hadn't given me any kind of information, like technical information on how to do it." (P9)

4.2.2.1 Responsibility

While not part of our questions, several participants talked about responsibility when it comes to checking for compliance which is a common theme for privacy in software development teams [73, 77, 86]. Privacy is often treated like a hot potato, and finding who is responsible is not easy. Our participants saw three entities in making sure that their app is compliant with regulations:

First, themselves, **developer's responsibility**, which is not what we expected to see because prior work shows that developers think that it is the ad network's responsibility to protect users' privacy [52] but the language of the ad networks puts the burden on the developers [74]. Therefore, it seems when developers read the documentation, they realize that it is their job to ensure that their app satisfies all the requirements for users' privacy and regulations. P3, for example, sounded frustrated when he realized that it is all on him to figure out all the nuances of privacy regulations: "It is just like it's your responsibility to do this, and it's your duty to follow this and this, and there is nothing." (P3)

Developers see (or wish to see because platforms put all the responsibility on the developer [74]) the platforms as the responsible body for privacy regulations, **platform's responsibility**:

> Feels a bit lazy from Google's perspective . . . because these laws are really on Facebook and Google, and that's why they exist, because of the massive amount of data that those companies have on their users, and it shouldn't be down to the little people plugging these things into their apps to sort out the legal implications; it should be down to the people that are actually storing and collecting massive amounts of data on you. (P9)

This expectation mirrors prior works findings that developers expect software development platforms (e.g., Google) to provide support and usable documentation to developers [45, 52].

We observed that a small set of participants thought that it is **someone else's responsibility** to sort out the regulations part, which echos the findings of prior work [73, 77, 86]. P9 sees the business side of the company in charge of sorting out privacy issues: "It's really the business people, the business side, that care about these regulations, and they're the ones who are going to be setting up the user interface." (P9) P10 saw app stores as an entity to check for privacy compliance: "Google play store when you upload it makes some checks on the code to check for privacy." (P10)

4.2.2.2 Strategies to Apply Regulations

While all the participants at some point during the session expressed **not knowing** how to comply with regulations, they suggested ways to make their apps compliant. Participants' strategies included filtering users, notice-and-consent, following the documentation, running tests, and turning off personalized ads. Others suggested regulations did not apply to their apps and, hence, did not need to take action, while some suggested the platform would take care of compliance.

All the participants suggested **filtering users** based on either age or location, which reverberates the language of ad networks and privacy regulations in general; CCPA applies in California, COPPA discusses children, and the GDPR applies to Europe: "We can pass data so if we are in U.S. or California we can pass 1 and 100 and if we are not we should just pass zero for our location." (P8)

The prevalent notice-and-consent concept in the ad networks realm prompted some participants to suggest **showing an interface to users** to apply regulations: "Make sure that the app is compliant with all these different policies . . . then the usual consent and informing all the users." (P11)

Some of the participants suggested that if they **followed the documentation** as it is (e.g., set the suggested configurations and copy-paste from sample codes), they will be compliant with the regulations: "Google has given us two keys or saving two values. I would just set those values in my app if it is children directed and I would just relax." (P4) This strategy emphasizes the value of having privacy-friendly documentation and defaults as developers put trust into what platforms offer to them.

Some participants would **write and run tests** to see if their app is compliant. These tests take the form of copy-pasting a sample code provided by the ad networks to see whether a consent form would appear, or doing some try and error with the sample code to see what would happen: "If I've integrated this I would test . . . if it's being first time opened in Europe, then if the consent pops up, then I would ensure that it's compliant." (P5)

A few participants thought that **turning off ads personalization** would make them compliant with the regulations: "Turning off personalized adverts and assuming that because I'm not doing any work with user data or personalization that I am conforming." (P1)

Some participants said that a specific regulation **does not apply to their app**. Therefore, they would not need to take any further action. Seven participants did not see their app targeting children; hence, no need for checking for COPPA: "Most of my users are above 18, so I wouldn't really be too much concerned." (P2) One participant said that the app is not directed to American users, so there was no need to check or comply with COPPA: "Will only service non-United States users of the app." (P10) And, two participants mentioned that their app does not collect any information,

so the regulations would not apply to their app: "I will probably not collect any personal information." (P10)

Similar to the does not apply to my app theme, some participants said that the **would not take any actions** because the regulation does not apply to them, the platform would take care of the issue, or the default is set in a way that does not require any further actions by them: "It says by default . . . obtains consent from a user located in European Economic Area. So I wouldn't bother reading the rest of the document." (P4)

4.2.3 Information-Seeking Strategies

Participants used multiple ways to find information about privacy regulations. All of them, at some point during the session, referred to what they have seen in other platforms or other software development places, **applying prior knowledge and expectations**. This expectation and behavior show the value of having consistent and uniform terminologies and interfaces for privacy-related information. P2 discussed the problem with an example of moving between multiple operating systems could be problematic (he has experience with an ad network but not with the one that we asked him to work with. The quote is about the latter):

> Being a Windows-user and then, suddenly, they put a Mac computer, or like a Linux computer in front of you, and you, basically, have to adapt and try to use a different side of screen or try to use some other shortcuts. This is a learning progress [to learn about various ad networks] – these things take time and, if I have time, that's okay but, if I am busy, that's really difficult to transition for me. (P2)

Participants also commonly noted the use of **online resources** such as the search on Google, use Stack Overflow, and watch videos on YouTube: "I'd head straight to Stack Overflow or somewhere else." (P1)

The **platforms' search** was a place that participants liked to use; however, in all cases, when participants used it, they could not find the right information. Thinking about the right term to search was also challenging (example tried keywords: "California," "CCPA," and "COPPA"). The other problem was with the search results. They included results from other unrelated products of the company making it difficult to find the relevant information.

A few participants used the **browser search** (Ctrl-F) to find the information they needed, potentially because some pages had long text making it difficult to find needed information (see Section 4.2.4.2 for too much detail and structured documentation).

4.2.4 Usability of Ad Network Libraries

At the end of the session with each ad network, we asked participants questions about their experience with the platforms. They also brought up usability issues during the think-aloud period, allowing us to target usability issues with these platforms and provide design recommendations to improve support for developers.

4.2.4.1 The Easy Part: Integration of an Ad

Many participants found the integration of an ad, the main functionality of an ad network, easy and straightforward, suggesting that ad networks can make usable interfaces and documentation: "So integrating those banners was fine but making the app more compliant with the rules and regulation it was impossible." (P4) It might be the case that ad networks treat privacy as a secondary or even tertiary priority, similar to how privacy is treated in software development teams [73, 77]; therefore, the documentation for these features are not well-designed compared to the parts of the documentation that is functionality-related.

4.2.4.2 Information Presentation Issues

Participants often had a problem understanding the **terms and language** of the privacy regulation pages. Several terms were hard to understand and not intuitive. They also found it challenging to understand all the terms, abbreviations, and acronyms used by ad networks: "I find it a little difficult to understand what GDPR is all about." (P5) "This is just so much information and, as a developer, it's just like legal jargon to me." (P9) The difficulties in understanding the legal language is a common problem for software developers [29, 77].

The situation is exacerbated when each ad network has its own terminology, and learning from one platform or knowing about a regulation from prior reading may not be helpful to understand privacy regulations and terms in another platform. For example, in several places, ad networks refer to IAB (Interactive Advertising Bureau, a "consortium charged with producing and helping companies implement global industry technical standards" [39]) without spelling out what it means or what it does, assuming that developers know about it:

"I still don't know what IAB is. Where's IAB? . . . it just says IAB. Doesn't tell you what IAB is." (P7)

"Funding Choices" a service that Google provides for building consent forms, is not an intuitive name for a consent building service: "Funding Choices isn't something I've done that but I imagine that's just the finance side." (P1) "Funding account linked to your AdMob account so I think this is the way you can get payments." (P6) Conversely, a section called "Policy Center" is not about privacy regulations; or RDP, restricted data processing configuration, is used multiple times without giving detail about its meaning: "The RDP signal, IAB signal don't seem to be explaining that well." (P1)

How platforms refer to privacy regulation also varies across platforms such as "EU Consent," "GDPR," "CCPA Preparation," "Child-directed apps (COPPA)," and "Targeting," making it difficult to expect and know where to find the relevant information (all participants tried to apply their prior knowledge to find information, see Section 4.2.3).

Another challenge was having **too much detail** in the documentation. On some pages, ad networks have a long text for privacy regulations making it a tedious task for developers to read and also know what they have to do: "A lot of times, we come across these regulations, but I'm not sure if all of us, but a lot of us do not read them in very minute detail at times." (P11) "Reading that long, long terms with so academic things were much harder to understand." (P6) On the other hand, some participants expressed **lack of detail**, often around technical and implementation detail: "Authenticity, security, privacy, dignity. It all seems very buzzwordy. It doesn't really seem like there's any real content to this. It all seems very vague, very wishy-washy." (P10) The difference between these two groups shows that platforms need to address various types of developers with diverse information needs. Also, perhaps it shows that platforms spend time creating policies and terms that developers may not read but do not provide the technical detail about the implementation of making privacy-compliant apps.

Many participants at some point during the study expressed reaching to a dead-end sate, and **not being able to find the information** or feature they were looking for: "The GDPR, I haven't seen any of them in the whole implementation of Facebook ads documentation." (P4) Participants used information-seeking strategies (Section 4.2.3) to find the needed information; however, that also did not always end up in finding the relevant information: "CCPA isn't coming up with anything, so I'm searching California, nothing. That's disappointing." (P1) On the other hand, in some places, participants did find information but expressed frustration because the information was there, but it was difficult to see or find because it was **buried and hidden**:

> [You've to] work out yourself how the dense technical documentation applies to the regulations, like with the simple set up stuff it's all spelled out for you. But if it can affect their revenue, they don't make it easy, they hide it, and they make it very difficult because a big barrier to entry is you've got to know the regulations. (P3)

One of the reasons that made it difficult for participants to find privacy information was what we call as **scattered privacy information**. Participants had no central place to find all the relevant information; instead, they had to navigate through the platforms and click on several links to hunt for the relevant information. As shown in Section 4.1, privacy information in ad networks is spread in multiple pages and layers, some with sample code, some with graphical controls, and some with textual explanations. Not having a central place to go to and find all the related information about privacy regulations might be one of the confusing causes:

> I would go with this way, but that's not what I'm looking for. This is another thing, so I'm looking for something that tells me that I'm following the CCPA. Oh, it's the same page. Okay. No, this article wasn't helpful. This is not what I was looking for. (P10)

4.2.4.3 What Developers Want? Design Wishes for Improving Support for Privacy Regulations

A majority of participants expressed a desire to see (or appreciated) **sample code**: "I'm looking for code now . . . there's no code on here." (P7) "I would add those documents and those breakdowns of the regulations in code example." (P4) While in several places, ad networks do have sample codes, having a sample code is inconsistent and sometimes hard to find (see Section 4.1 for details).

Video was another preferred material that participants would want to see: "I find these videos quite helpful as a brief overview but not really in detail just cause of the format it's presenting." (P1) At the time of writing this paper, the videos provided by platforms do not include information about privacy regulations.

Having a **step-by-step and structured documentation** is a suggestion to address the issues with too much detail, hard to find detail, hidden, and scattered information:

> You start at the top and go left to right, but more of this kind of thing, one, two, three, four. If your app is X, here are the steps to follow. If your app is directed at children under 14, here are the steps you need to follow. (P7)

The "Get Started" pages and documentation of integration of ads has a step-by-step structure, and perhaps participants are also more used to this style of documentation because of their prior experiences with other software development platforms.

Having **easily accessible configurations** both in the graphical-level and the code-level was another request that participants had to make the task of following privacy regulations easier: "We set some settings, some configuration to follow those rules." (P8) While there are some graphical-level and code-level configurations on these platforms, participants find it challenging to find them all and know how they all work together. Therefore, there is a need for having **all privacy-related information in one place**. There are multiple places in ad networks where developers have to make changes to both graphical and code configurations, and it is unclear how they are connected. Having a central place to cover all materials might clarify the ambiguities. Also, participants prefer to see more graphical simple checkboxes rather than configurations that they have to change in their code:

> Having a legislation checklist or legislation sub-page in one place that's very clear would be helpful and then leading off to these advanced topics or CCPA so they can say these are the legislation we need to do, the CCPA, the EU, and GDPR. (P1)

Similar to easily accessible configurations, some participants expressed a preference for **automatic configurations** such as using package managers (e.g., CocoaPods for iOS) and XML configurations (e.g., Maven and Gradle for Android) to set up their ads: "They've got a Pod here so I would go, and I would add this Pod to my Podfile and pod-install it." (P9) None of the provided examples in the studied ad networks had a configuration for privacy regulations. An opportunity to ease the integration of privacy regulations is to incorporate privacy regulations as a line in these configuration files.

5 Discussion and Future Work

We studied three popular ad networks for mobile apps using two studies: an expert review and think-aloud sessions with eleven developers to understand ad networks' support for developers in building privacy regulation-compliant apps. The two studies gave us in-depth views into usability issues of ad network libraries. The think-aloud sessions provided insights into mental models of privacy configurations, compliance check strategies, and information-seeking strategies. On the other hand, the expert review gave us quantitative insights into the extent of information about privacy regulations available on the studied ad networks.

We find that ad networks documentation for privacy regulations is poorly designed, and developers find it challenging to find relevant information; building and applying all the regulations might be even more complicated. We acknowledge the effort that ad networks put into expanding their libraries to include privacy regulations. Privacy regulations are ever-evolving, and following the changes and modifications requires time and effort. We suspect that one reason for all the inconsistencies we observed might be the number of changes that occur in the privacy regulations causing ad networks to add new sections without fully considering all aspects such as usability. Our results can benefit ad networks who want to use **privacy as a competitive advantage** (similar to other companies such as Brave [12], DuckDuckGo [17], and Matomo [49] that brand as a privacy-friendly alternative to large tech companies). It also gives researchers and regulators a starting point to investigate the software development documentation to improve privacy support for developers. In the following, we discuss the implications of our work and suggest avenues for future research.

5.1 Design Implications

This section uses participants' suggestions, findings from our expert review, and prior work to recommend potential directions to improve privacy support for developers in ad networks. All of the suggestions require **further research and empirical work** (e.g., using human-centered design methods for API design [54, 55]) to understand what works for developers. We also acknowledge that developers come from a range of expertise and background, meaning that one solution may not fit the needs of all developers. However, this space needs research because ad networks' interests may not align with the public's benefits. Developers play a role in giving access to users' data to ad networks, and they deserve to know about the privacy consequences of their choices before making a decision.

5.1.1 Create Multimedia Materials for Privacy

A balance between text, sample code, and video is needed, with videos and sample codes being the most popular among our participants. Some participants also like to have a well-structured text about all the details and scenarios about the regulations. For example, when seeing information about COPPA, it is beneficial to have bullet points with explicit age limits and whether a developer needs to add a Boolean flag in the configurations if their app targets a certain age range.

Future research may find ways to **promote privacy regulations within the developer communities** (e.g., Stack Overflow, Reddit, and conferences) and create materials such as videos to inform developers about privacy regulations and how to integrate them into their products. The need for building online resources around privacy is further highlighted when we look at Stack Overflow's survey in 2021 with its users. It shows that online resources are the top resource (60%) for developers to learn how to code (the second resource is at school with 54%), which shows the value of these resources to developers. On the other hand, privacy questions on Stack Overflow cover topics such as privacy policies, permissions, and access control, but rarely talk about privacy regulations [76], which in turn might mean that there may not be enough online resources for developers to learn about privacy regulations.

5.1.2 Unify Privacy Terms, Controls, and Language

Across the three ad networks, privacy regulations are addressed differently using various terms and language. We suggest building a unified terminology that ad networks can use consistently to talk about privacy regulations. It would also help developers learn once and apply their knowledge in another ad network reducing effort and barriers to consider privacy regulations. Future research may suggest and evaluate approaches to explain the privacy regulations that are easy to understand for the developer community. We note that compliance is a challenging term. It is non-binary, malleable, and difficult to define in certain situations as it may take different forms based on context. There is a need for metrics to measure compliance and a framework to guide developers to comply. Future research may aim to translate and disambiguate legal requirements into requirements that developers can follow and implement.

Ad networks' current approach to advocate for users' privacy is to self-regulate (e.g., through Interactive Advertising Bureau [39]). However, ads still invade users' privacy (e.g., by using users' data for malicious political campaigns [18]), suggesting that the self-regulatory approach is not sufficient. We posit that ad networks' data-exploitative business models do not bring privacy features to the forefront of their interfaces. With the help of academia, we suggest **an independent organization build an open-source library** that is easy to use, works across platforms, and provides transparency to developers and users (perhaps in the form of a not-for-profit organization). Otherwise, developers may use other off-the-shelf consent building tools (e.g., Quantcast and OneTrust), which may not put privacy first and instead may have many preselected defaults that do not favor users' privacy [50, 58]. Such efforts may help bring regulations closure to developers' understanding and language and bridge the gap between what privacy regulations require and the technical measures needed to comply with regulations.

5.1.3 Dedicate a Section to Privacy in the Documentation

A majority of participants suggested having a section dedicated to regulations which may include subsections for CCPA, COPPA, and GDPR, each with a simple checklist that developers need to follow with easy-to-click graphical configurations to make them compliant with a specific regulation. The differences between flags that need to be set in the code and graphical configurations could also be confusing. Therefore, we suggest only having graphical interfaces on the developer panels to enable developers to choose easily. We suggest having those in the same section with a simple Boolean flag only if ad networks require code configurations because of technical difficulties on their side. Developers also need to be informed about these configurations, especially if they are under developer panels that need logging in, in their workflows (e.g., in the "Get Started" as a separate step), as not all participants checked all the sections in a platform which is normal behavior because the documentation covers a wide range of topics.

5.1.4 Integrate Privacy in Developers' Workflow

In addition to participants' suggestions, we recommend adding privacy regulations in the middle of developers' workflows, such as in the Get Started pages, as a separate step. While it is helpful to have all privacy regu-

lations in one place, adding an extra step in the midst of what developers have to go through to get their ads integrated might remind them about the privacy regulations. The approach to making this integration usable and noticeable for developers requires further research because one ad network has a red box on its Get Started page that mentions GDPR and COPPA. However, few participants noticed and read it. Therefore, future research may evaluate various ways of including privacy regulations in developers' workflow.

5.1.5 Eliminate Dark Patterns From Privacy-Related Documentation

Considering the depth and spread of privacy regulation on the ad networks, it may not always be easy for developers to find all the information they need, understand it, and adjust their apps. This challenge may be exacerbated in small and medium-sized companies where teams may not have access to lawyers and dedicated privacy teams. The current ad networks' documentation puts functionality first, and privacy is a secondary or tertiary priority, resulting in a cognitive burden for developers to integrate privacy features. It may not be in the best interest of ad networks' data-hungry business models to have privacy at the forefront of their documentation. Therefore, we suggest that regulators enforce ad networks to offer usable documentation where developers can see all the available configurations without dark patterns. We also suggest that software companies include privacy, design, programming, and legal experts in the design of privacy documentation to include diverse voices in today's multi-interdisciplinary software development ecosystem, which may lift privacy features from a secondary priority to a first priority and ease the process of translating legal requirements into understandable and clear technical requirements.

Future research may study dark patterns directed at developers through the four lenses suggested by Mathur et al. [48]: (1) "individual welfare," by looking at developers' gains and losses when they make changes to configurations related to privacy regulations, with and without the presence of dark patterns, (2) "collective welfare," ad networks use a language that focuses on revenue increase [74], future research may provide empirical evidence to help developers understand the extent of financial gains when using different ad networks, (3) "regulatory objectives," while the studied interfaces are directly related to privacy regulations, there is a need to understand whether these interfaces themselves are compliant with regulations, and (4) "individual autonomy," by running studies with developers to understand their awareness of ad networks' privacy interfaces.

5.2 Make Ad Networks' Mechanisms Transparent

Developers may choose an ad network without fully understanding its detrimental privacy implications and see ad networks as the only resource for monetization [52]. Currently, it is not clear how much money developers can make from integrating ads from an independent source other than what is available on the ad networks, where they emphasize on an increase of revenue if ads are personalized [74]. We suggest expanding the Universal Ad Transparency (i.e., an effort from the research community to make ads transparent motivated by providing clarity to the funders of ad campaigns [19]), to include a field that covers the percentage of the spend that goes into the publishers' pocket (e.g., an app developer) to transparently communicate with developers about how much money an app can make if they include an ad network and use personalized ads. Then, analyze this data and make it available to the public (e.g., through visualizations) to give developers unbiased empirical evidence about the potential revenues. This data may be used to provide developers factual information about gains and losses if they include ads or use personalized ads instead of non-personalized ads.

5.3 Testing Systems for Compliance

Some participants mentioned writing and running a test to see if their app is compliant with the regulations. A classic developer behavior is to write code, run, and debug. This behavior is also typical within the startup community [25], similar to the "fail fast, fail often" idea. However, when looking at privacy regulations, it is not clear what developers need to test against. Future work may look at ways to build a privacy testing system that developers can easily drop their apps in, ideally an online system, and get results about the privacy regulations' compliance. It may map the results into a framework such as Privacy by Design [33] to improve usability using a high-level common framework. In addition to a detailed report, this system may have a checkbox that turns green when the app is compliant with a regulation. It would also reduce developers' efforts to check for third-party libraries because third parties can be one of

the reasons for privacy implications though developers are not always aware of them [64, 80].

5.4 Improve Developers' Mental Models

Waldman argues that the tech industry has put effort into reducing the discourse in privacy to the "notice-and-consent" concept [86]. In our sample, the predominant conceptualization is notice-and-consent as well. Participants talked about surface-level data analysis by the ad networks showing that their **mental models of ad networks and privacy consequences are limited**. Looking at Google AdMob's documentation [2], as an example, ads personalization uses "*user's previous search queries, activity, visits to sites or apps, demographic information, or location.*" When ads are not personalized, Google still uses "*contextual information, including coarse (such as city-level) geo-targeting based on current location, and content on the current site or app or current query terms . . . cookies or mobile ad identifiers for frequency capping, aggregated ad reporting" and developers "must obtain consent to use cookies or mobile ad identifiers for those purposes.*"

While we expected to see well-developed mental models because of the technical background of participants, it seems that having a technical background does not necessarily equate with a higher understanding of privacy implications of online technologies, similar to what prior work suggests [37]. One of the potential causes that many apps and websites are not regulation-compliant might be developers not knowing and understanding the mechanisms behind third parties (e.g., ad networks). The situation might exacerbate when developers think they know about regulations while they might not. Several participants consider themselves as "very knowledgable" about the GDPR and a few about COPPA. However, we did not observe a profound understanding or difference between these participants and others (our results are qualitative; hence, we cannot make a conclusive statement), suggesting that developers may think that they know about the regulations perhaps because they have heard about them in the news. However, in practice, their general knowledge of regulations may not be helpful to understand the documentation and build a privacy-compliant app.

A place to improve developers' mental models and make them privacy-conscious is to **include privacy topics within the computer science curriculum** because many developers have a degree in a computer science-related field (62% of respondents to Stack Overflow's survey in 2020 [62]). Another possible avenue is to **create multimedia materials**, as explained in Section 5.1.1, to increase awareness in the technical community about privacy regulations. Future research may also focus on understanding how developers perceive data flows within the ad network ecosystem. This may be achieved by investigating the impact of showing developers the consequences of their configurations in complying with regulations and establishing a ground for developers' conceptualizations of compliance.

6 Conclusion

We analyzed three popular ad networks for mobile apps using two studies, an expert review of pages with information about CCPA, COPPA, and GDPR, and think-aloud sessions with eleven developers. We find that the current documentation does not support developers in building apps that are compliant with privacy regulations. Privacy information is often buried, hidden under multiple layers, is inconsistent across platforms, filled with legal jargon, and lacks structure. We make several suggestions to improve privacy support for developers in ad networks, such as dedicating a section to privacy, unifying terms used for explaining privacy regulations, building a privacy testing system for developers, and involving an independent player to build a usable open-source library that handles privacy regulations for developers using easy-to-use configurations. Prior work shows promise in making privacy salient, while developers make a choice with privacy implications [78], future research may extend this body of work to make privacy a first-class citizen in the software development ecosystem. Improvements in this area may help developers understand privacy configurations and regulations in today's software development ecosystem, which requires technical people to understand privacy requirements and reduce the effort developers need to put in to get their apps compliant with the privacy regulations.

Acknowledgments

This work is partly supported by EPSRC grant: Why Johnny doesn't write secure software? Secure software development by the masses (EP/P011799/2) and the National Science Foundation under Grant No. CNS-1801472. Tianshi Li is supported in part by the CMU CyLab Presidential Fellowship.

References

[1] Anne Adams and Martina Angela Sasse. Users Are Not the Enemy. *Communications of the ACM*, 42(12):40–46, December 1999. 10.1145/322796.322806.

[2] Google AdMob. AdMob & AdSense programme policies Personalized and non-personalized ads, 2021. URL https://support.google.com/admob/answer/7676680. Last accessed October 2021.

[3] Nitin Agrawal, Reuben Binns, Max Van Kleek, Kim Laine, and Nigel Shadbolt. Exploring Design and Governance Challenges in the Development of Privacy-Preserving Computation. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, New York, NY, USA, 2021. ACM. 10.1145/3411764.3445677.

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

[5] Dedre Gentner Albert L. Stevens. *Mental Models*. Taylor & Francis, first edition, 1983. 10.4324/9781315802725.

[6] Sami Alkhatib, Jenny Waycott, George Buchanan, Marthie Grobler, and Shuo Wang. Privacy by Design in Aged Care Monitoring Devices? Well, Not Quite Yet! In *32nd Australian Conference on Human-Computer Interaction*, OzCHI '20, pages 492–505, New York, NY, USA, 2020. ACM. 10.1145/3441000.3441049.

[7] App Annie. The State of Mobile in 2020, 2020. URL https://www.appannie.com/en/insights/market-data/state-of-mobile-2020/. Last accessed November 2021.

[8] AppBrain. Android Ad Network statistics and market share, 2020. URL https://www.appbrain.com/stats/libraries/ad-networks. Last accessed November 2021.

[9] Gabor Aranyi, Paul van Schaik, and Philip Barker. Think-aloud Demonstration Video, 2021. URL https://www.youtube.com/watch?v=BwpPIiBK0cA. Last accessed September 2021.

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

[11] Kathrin Bednar, Sarah Spiekermann, and Marc Langheinrich. Engineering Privacy by Design: Are engineers ready to live up to the challenge? *The Information Society*, 35(3):122–142, 2019. 10.1080/01972243.2019.1583296.

[12] Brave. Secure, Fast & Private Web Browser with Adblocker | Brave Browser, 2021. URL https://brave.com. Last accessed November 2021.

[13] Harry Brignull. Dark Patterns, 2021. URL https://darkpatterns.org. Last accessed November 2021.

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

[15] Ryan Calo. Digital Market Manipulation. *George Washington Law Review*, 82, 01 2013. 10.2139/ssrn.2309703.

[16] Federal Trade Commission. Children's Online Privacy Protection Rule (COPPA), 1998. URL https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule. Last accessed November 2021.

[17] DuckDuckGo. DuckDuckGo — Privacy, simplified., 2021. URL https://duckduckgo.com. Last accessed November 2021.

[18] Laura Edelson, Tobias Lauinger, and Damon McCoy. A Security Analysis of the Facebook Ad Library. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 661–678, 2020. 10.1109/SP40000.2020.00084.

[19] Laura Edelson, Jason Chuang, Erika Franklin Fowler, Michael Franz, and Travis N Ridout. Universal Digital Ad Transparency. 2021. 10.2139/ssrn.3898214.

[20] Laura Edelson, Minh-Kha Nguyen, Ian Goldstein, Oana Goga, Damon McCoy, and Tobias Lauinger. Understanding Engagement with U.S. (Mis)Information News Sources on Facebook. In *Proceedings of the 21st ACM Internet Measurement Conference*, IMC '21, page 444–463, New York, NY, USA, 2021. Association for Computing Machinery. 10.1145/3487552.3487859.

[21] Sascha Fahl, Marian Harbach, Henning Perl, Markus Koetter, and Matthew Smith. Rethinking SSL Development in an Appified World. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, CCS '13, pages 49–60, New York, NY, USA, 2013. Association for Computing Machinery. 10.1145/2508859.2516655.

[22] Centre for Data Ethics and Innovation. Public Attitudes Towards Online Targeting, 2020. URL https://www.gov.uk/government/publications/cdei-review-of-online-targeting. Last accessed November 2021.

[23] Adam Foroughi. AppLovin to Acquire MoPub Business From Twitter, 2021. URL https://www.applovin.com/blog/applovin-to-acquire-mopub-business-from-twitter/. Last accessed November 2021.

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

[25] Carmine Giardino, Michael Unterkalmsteiner, Nicolò Paternoster, Tony Gorschek, and Pekka Abrahamsson. What Do We Know about Software Development in Startups? *IEEE Software*, 31(5):28–32, 2014. 10.1109/MS.2014.129.

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

[27] Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, and Damian Clifford. Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2021. Association for Computing Machinery. 10.1145/3411764.3445779.

[28] Matthew Green and Matthew Smith. Developers Are Not the Enemy!: The Need for Usable Security APIs. *IEEE Security and Privacy*, 14(5):40–46, September 2016. 10.1109/MSP.2016.111.

[29] Irit Hadar, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. Privacy by designers: software developers' privacy mindset. *Empirical Software Engineering*, 23(1):259–289, February 2018. 10.1007/s10664-017-9517-1.

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

[31] Aurora Harley. UX Expert Reviews, 2018. URL https://www.nngroup.com/articles/thinking-aloud-the-1-usability-tool/. Last accessed October 2021.

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

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

[34] QSR International. Qualitative Data Analysis Software | NVivo, 2021. URL https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home/. Last accessed November 2021.

[35] Ling Jin, Boyuan He, Guangyao Weng, Haitao Xu, Yan Chen, and Guanyu Guo. MAdLens: Investigating Into Android In-App Ad Practice at API Granularity. *IEEE Transactions on Mobile Computing*, 20(3):1138–1155, 2021. 10.1109/TMC.2019.2953609.

[36] Joel. Top Paying Mobile Ad Networks & App Monetization Platforms [2021 Edition], 2021. URL https://www.appypie.com/top-mobile-ad-networks. Last accessed November 2021.

[37] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "My Data Just Goes Everywhere:"User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 39–52, Ottawa, July 2015. USENIX Association. URL https://www.usenix.org/conference/soups2015/proceedings/presentation/kang.

[38] Blagovesta Kostova, Seda Gürses, and Carmela Troncoso. Privacy Engineering Meets Software Engineering. On the Challenges of Engineering Privacy By Design, 2020. URL https://arxiv.org/abs/2007.08613.

[39] IAB Tech Lab. About IAB Tech Lab, 2018. URL https://wiki.iabtechlab.com. Last accessed November 2021.

[40] J. Richard Landis and Gary G. Koch. The Measurement of Observer Agreement for Categorical Data. *Biometrics*, 33 (1):159–174, 1977. 10.2307/2529310.

[41] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. Chapter 11 - Analyzing qualitative data. In Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser, editors, *Research Methods in Human Computer Interaction*, pages 299–327. Morgan Kaufmann, Boston, second edition edition, 2017. 10.1016/B978-0-12-805390-4.00011-X.

[42] CMS Legal. GDPR Enforcement Tracker – list of GDPR fines, 2021. URL https://www.enforcementtracker.com. Last accessed September 2021.

[43] Randall A. Lewis and David H. Reiley. Online ads and offline sales: measuring the effect of retail advertising via a controlled experiment on Yahoo! *Quantitative Marketing and Economics*, 12(3):235–266, September 2014. 10.1007/s11129-014-9146-6.

[44] Tianshi Li, Yuvraj Agarwal, and Jason I. Hong. Coconut: An IDE Plugin for Developing Privacy-Friendly Apps. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(4), December 2018. 10.1145/3287056.

[45] Tianshi Li, Elizabeth Louie, Laura Dabbish, and Jason I. Hong. How Developers Talk About Personal Data and What It Means for User Privacy: A Case Study of a Developer Forum on Reddit. *Proc. ACM Hum.-Comput. Interact.*, 4 (CSCW3), January 2021. 10.1145/3432919.

[46] Tianshi Li, Elijah B. Neundorfer, Yuvraj Agarwal, and Jason I. Hong. Honeysuckle: Annotation-Guided Code Generation of In-App Privacy Notices. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, 5(3), September 2021. 10.1145/3478097.

[47] Miguel Malheiros, Charlene Jennett, Snehalee Patel, Sacha Brostoff, and Martina Angela Sasse. Too Close for Comfort: A Study of the Effectiveness and Acceptability of Rich-Media Personalized Advertising. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12, pages 579–588, New York, NY, USA, 2012. ACM. 10.1145/2207676.2207758.

[48] Arunesh Mathur, Mihir Kshirsagar, and Jonathan Mayer. What makes a dark pattern... dark? design attributes, normative considerations, and measurement methods. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2021. Association for Computing Machinery. 10.1145/3411764.3445610.

[49] Matomo. Google Analytics alternative that protects your data, 2021. URL https://matomo.org. Last accessed November 2021.

[50] Celestin Matte, Nataliia Bielova, and Cristiana Santos. Do Cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 791–809, 05 2020. 10.1109/SP40000.2020.00076.

[51] William Melicher, Mahmood Sharif, Joshua Tan, Lujo Bauer, Mihai Christodorescu, and Pedro Giovanni Leon. (Do Not) Track Me Sometimes: Users' Contextual Preferences for Web Tracking. *Proceedings on Privacy Enhancing Technologies*, 2016(2):135–154, 2015. 10.1515/popets-2016-0009.

[52] Abraham H. Mhaidli, Yixin Zou, and Florian Schaub. "We Can'Live Without Them!" App Developers'Adoption of Ad Networks and Their Considerations of Consumer Risks. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, Santa Clara, CA, August 2019. USENIX Association. URL https://www.usenix.org/conference/soups2019/presentation/mhaidli.

[53] Matthew Miles and Michael Huberman. *Qualitative Data Analysis: A Methods Sourcebook*. Sage, 1994.

[54] Lauren Murphy, Mary Beth Kery, Oluwatosin Alliyu, Andrew Macvean, and Brad A. Myers. API Designers in the Field: Design Practices and Challenges for Creating Usable APIs. In *2018 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*, pages 249–258, 2018. 10.1109/VLHCC.2018.8506523.

[55] Brad A. Myers and Jeffrey Stylos. Improving API Usability. *Commun. ACM*, 59(6):62–69, May 2016. 10.1145/2896587.

[56] Jakob Nielsen. Demonstrate Thinking Aloud by Showing Users a Video, 2014. URL https://www.nngroup.com/articles/thinking-aloud-demo-video/. Last accessed September 2021.

[57] Jakob Nielsen. Thinking Aloud: The #1 Usability Tool, 2021. URL https://www.nngroup.com/articles/thinking-aloud-the-1-usability-tool/. Last accessed October 2021.

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

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

[60] Katie O'Donnell and Henriette Cramer. People's Perceptions of Personalized Ads. In *Proceedings of the 24th International Conference on World Wide Web*, WWW '15 Companion, page 1293–1298, New York, NY, USA, 2015. ACM. 10.1145/2740908.2742003.

[61] State of California Department of Justice. California Consumer Privacy Act (CCPA), 2018. URL https://oag.ca.gov/privacy/ccpa. Last accessed November 2021.

[62] Stack Overflow. Developer Survey Results, 2020. URL https://insights.stackoverflow.com/survey/2020. Last accessed November 2021.

[63] The European parliament and the council of the European union. General Data Protection Regulation (GDPR), 2018. URL https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679. Last accessed November 2021.

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

[65] Johnny Saldaña. *The Coding Manual for Qualitative Researchers*. Sage, 2015.

[66] Awanthika Senarath and Nalin A. G. Arachchilage. Why Developers Cannot Embed Privacy into Software Systems?: An Empirical Investigation. In *Proceedings of the 22Nd International Conference on Evaluation and Assessment in Software Engineering 2018*, EASE'18, pages 211–216, New York, NY, USA, 2018. ACM. 10.1145/3210459.3210484.

[67] Katie Shilton, Donal Heidenblad, Adam Porter, Susan Winter, and Mary Kendig. Role-Playing Computer Ethics: Designing and Evaluating the Privacy by Design (PbD) Simulation. *Science and Engineering Ethics*, 26(6):2911–2926, July 2020. 10.1007/s11948-020-00250-0.

[68] Laura Shipp and Jorge Blasco. How private is your period?: A systematic analysis of menstrual app privacy policies. *Proceedings on Privacy Enhancing Technologies*, 2020(4):491–510, October 2020. 10.2478/popets-2020-0083.

[69] Sooel Son, Daehyeok Kim, and Vitaly Shmatikov. What Mobile Ads Know About Mobile Users. In *Network and Distributed System Security Symposium (NDSS)*, 2016. 10.14722/ndss.2016.23407.

[70] Springer-Verlag. *Latin Square Designs*, pages 297–297. Springer New York, New York, NY, 2008. 10.1007/978-0-387-32833-1_223.

[71] Statista. Software developer gender distribution worldwide, 2020. URL https://www.statista.com/statistics/1126823/worldwide-developer-gender/. Last accessed September 2021.

[72] Statista. Mobile operating systems' market share worldwide from January 2012 to June 2021, 2021. URL https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/. Last accessed September 2021.

[73] Mohammad Tahaei and Kami Vaniea. A Survey on Developer-Centred Security. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 129–138. IEEE, June 2019. 10.1109/EuroSPW.2019.00021.

[74] Mohammad Tahaei and Kami Vaniea. "Developers Are Responsible": What Ad Networks Tell Developers About Privacy. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems Extended Abstracts*, CHI '21 Extended Abstracts, pages 1–12, New York, NY, USA, 2021. Association for Computing Machinery. 10.1145/3411763.3451805.

[75] Mohammad Tahaei and Kami Vaniea. Recruiting Participants With Programming Skills: A Comparison of Four Crowdsourcing Platforms and a CS Student Mailing List. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '22, pages 1–16, New York, NY, USA, 2022. Association for Computing Machinery. 10.1145/3491102.3501957.

[76] Mohammad Tahaei, Kami Vaniea, and Naomi Saphra. Understanding Privacy-Related Questions on Stack Overflow. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, pages 1–14, New York, NY, USA, 2020. Association for Computing Machinery. 10.1145/3313831.3376768.

[77] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. Privacy Champions in Software Teams: Understanding Their Motivations, Strategies, and Challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, pages 1–15, New York, NY, USA, 2021. Association for Computing Machinery. 10.1145/3411764.3445768.

[78] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. Deciding on Personalized Ads: Nudging Developers About User Privacy. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 573–596. USENIX Association,

August 2021. URL https://www.usenix.org/conference/soups2021/presentation/tahaei.

[79] Mohammad Tahaei, Kami Vaniea, Beznosov Konstantin, and Maria K. Wolters. Security Notifications in Static Analysis Tools: Developers' Attitudes, Comprehension, and Ability to Act on Them. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, CHI '21, pages 1–17, New York, NY, USA, 2021. Association for Computing Machinery. 10.1145/3411764.3445616.

[80] Mohammad Tahaei, Tianshi Li, and Kami Vaniea. Understanding Privacy-Related Advice on Stack Overflow. In *Proceedings on Privacy Enhancing Technologies*, pages 1–18, 2022. 10.2478/popets-2022-0032.

[81] Jenny Tang, Hannah Shoemaker, Ada Lerner, and Eleanor Birrell. Defining Privacy: How Users Interpret Technical Terms in Privacy Policies. *Proceedings on Privacy Enhancing Technologies*, 2021(3):70–94, 2021. 10.2478/popets-2021-0038.

[82] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (Un)Informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, pages 973–990, New York, NY, USA, 2019. Association for Computing Machinery. 10.1145/3319535.3354212.

[83] Katya Uvarova. Top 15 Mobile App Ad Networks and Platforms, 2021. URL https://messapps.com/allcategories/marketing/top-15-mobile-app-ad-networks-and-platforms/. Last accessed September 2021.

[84] Daniel Votipka, Desiree Abrokwa, and Michelle L. Mazurek. Building and Validating a Scale for Secure Software Development Self-Efficacy. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, pages 1–20, New York, NY, USA, 2020. Association for Computing Machinery. 10.1145/3313831.3376754.

[85] Ari Ezra Waldman. Designing Without Privacy. *Houston Law Review*, 55:659, 2018. URL https://ssrn.com/abstract=2944185.

[86] Ari Ezra Waldman. *Industry Unbound: The Inside Story of Privacy, Data, and Corporate Power*. Cambridge University Press, 2021. 10.1017/9781108591386.

[87] Alma Whitten and J. D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8*, SSYM'99, page 14, USA, 1999. USENIX Association. URL https://www.usenix.org/conference/8th-usenix-security-symposium/why-johnny-cant-encrypt-usability-evaluation-pgp-50.

[88] Eric Zeng, Miranda Wei, Theo Gregersen, Tadayoshi Kohno, and Franziska Roesner. Polls, Clickbait, and Commemorative $2 Bills: Problematic Political Advertising on News and Media Websites around the 2020 U.S. Elections. In *Proceedings of the 21st ACM Internet Measurement Conference*, IMC '21, page 507–525, New York, NY, USA, 2021. Association for Computing Machinery. 10.1145/3487552.3487850.

[89] Fangwei Zhao, Serge Egelman, Heidi M. Weeks, Niko Kaciroti, Alison L. Miller, and Jenny S. Radesky. Data Collection Practices of Mobile Applications Played by Preschool-Aged Children. *JAMA Pediatrics*, 174(12), 12 2020. 10.1001/jamapediatrics.2020.3345.

Appendix

A Screening Survey

[After the participant read the participant information sheet and consent form, and agreed to participant in the study. Answer options were randomized.]

1. Please select the statement that best describes your primary role at your current or most recent job.
   • Jobs NOT related to computer science, informatics, computer engineering, or related fields • Designing products (e.g., UI designer, interaction designer) • Developing software (e.g., programmer, developer, web developer, software engineer) • Testing software (e.g., tester, quality analyst, automation engineer) • Managing software development (e.g., project manager, IT manager, scrum master) • Privacy and/or security engineering (e.g., security engineer, privacy engineer, penetration tester, ethical hacker, cryptographer) • Other (please specify)
2. Are you a student?
   • Yes • No
3. How many years of experience do you have in software development? [Numbers only]
4. How many years of experience do you have in mobile development? [Numbers only]
5. How many years of experience do you have in Android app development? [Numbers only]
6. How many years of experience do you have in How many years of experience do you have in iOS app development? [Numbers only]
7. Which of the following ad networks have used in your apps in the past three years?
   • Google AdMob • Facebook Audience Network • MoPub • Amazon Mobile Ad • Millennial Media • AdColony • InMobi • Unity Ads • Vungle • Flurry • I haven't worked with any ad networks in the past three years • Other (please specify)
8. What is your main source of income in software or mobile development?
   • I don't make money from software or mobile development • Salary, not dependent on software/app revenue • Primarily salary and bonuses, partially dependent on software/app revenue • Primarily direct software/app revenue • Other (please specify)
9. What percentage of your revenue depends on ads? [Slider range: 0%–100%]
10. How involved have you been in in-app advertising activities? [Options were: Not at all, A little, A moderate amount, A lot, A great deal]

• Choosing an advertising partner or advertising network for an app. • Configuring the types of in-app ads shown in an app (e.g., where to place ads, what categories of ads to show, etc.) • Integrating the necessary code into an app to enable in-app advertising. • Other (please specify)

11. How knowledgeable do you consider yourself about the following regulations? [Options were: Not knowledgeable at all, Slightly knowledgeable, Moderately knowledgeable, Very knowledgeable, Extremely knowledgeable]
    • GDPR (General Data Protection Regulation) • CCPA (California Consumer Privacy Act) • COPPA (Children's Online Privacy Protection Act)
12. How many people were employed in the organization for which you worked on the app development most recently?
    • 1-9 employees • 10-99 employees • 100-999 employees • 1,000-9,999 employees • 10,000+ employees
13. How many years old are you? [Numbers only]
14. In which country do you currently reside? [List of countries]
15. If you can't find your country in the above question options, please enter it here. [Open-ended question]
16. What is your gender?
    • Male • Female • Non-binary • Prefer not to say • Prefer to self describe

B Participants Demographics

Table 3 shows participants' demographics.

C Sample Screenshots of Pages Related to Privacy Regulations

Figures 1, 2, and 3 show a sample page related to privacy regulations on the three studied ad networks.

D Resulting Diagrams From Expert Review of Privacy-Related Pages

Figures 4, 5, and 6 show the pages related to privacy regulations on the three studied ad networks.

Fig. 1. A sample section related to privacy regulations on Facebook Audience Network [Seen under developer account].

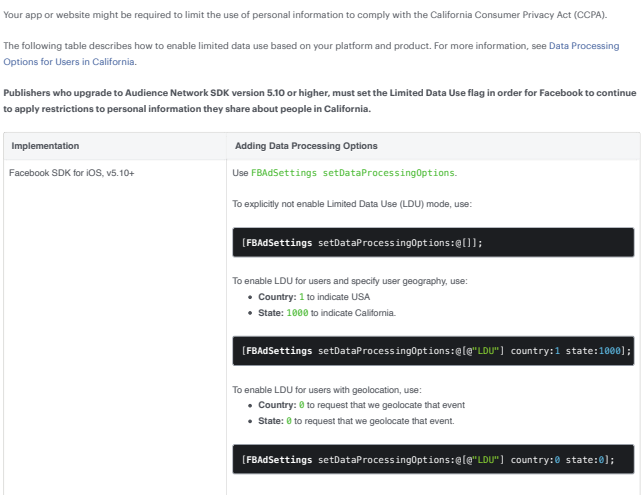


Fig. 2. A sample section related to privacy regulations on Google AdMob [Create a site message for EU consent].

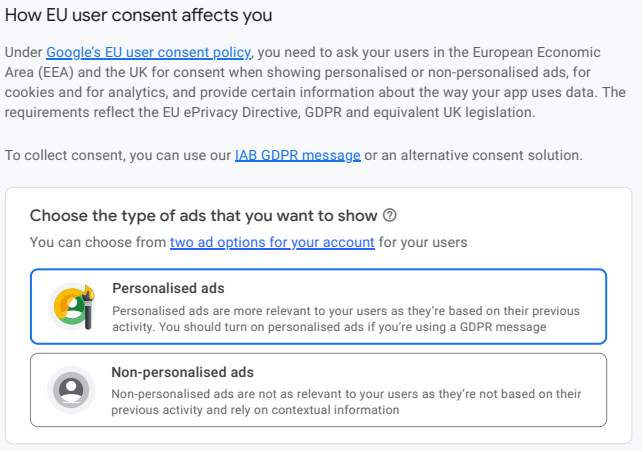


Fig. 3. A sample section related to privacy regulations on Twitter MoPub [GDPR Publisher Integration Guide].

For publishers with MoPub SDK 5.1 and higher:

- If the publisher is *not* using the `forceGDPRApplies` (Android) or `forceGDPRApplicable` (iOS, Unity) flag, consent is considered valid where `isGDPRApplicable` is true as defined by the MoPub SDK, as described here.

  If a publisher then starts using the "Force GDPR Applies" flag for a user who was not identified by MoPub as being subject to GDPR, our SDK will treat that user as subject to GDPR for the duration of the app's lifetime.

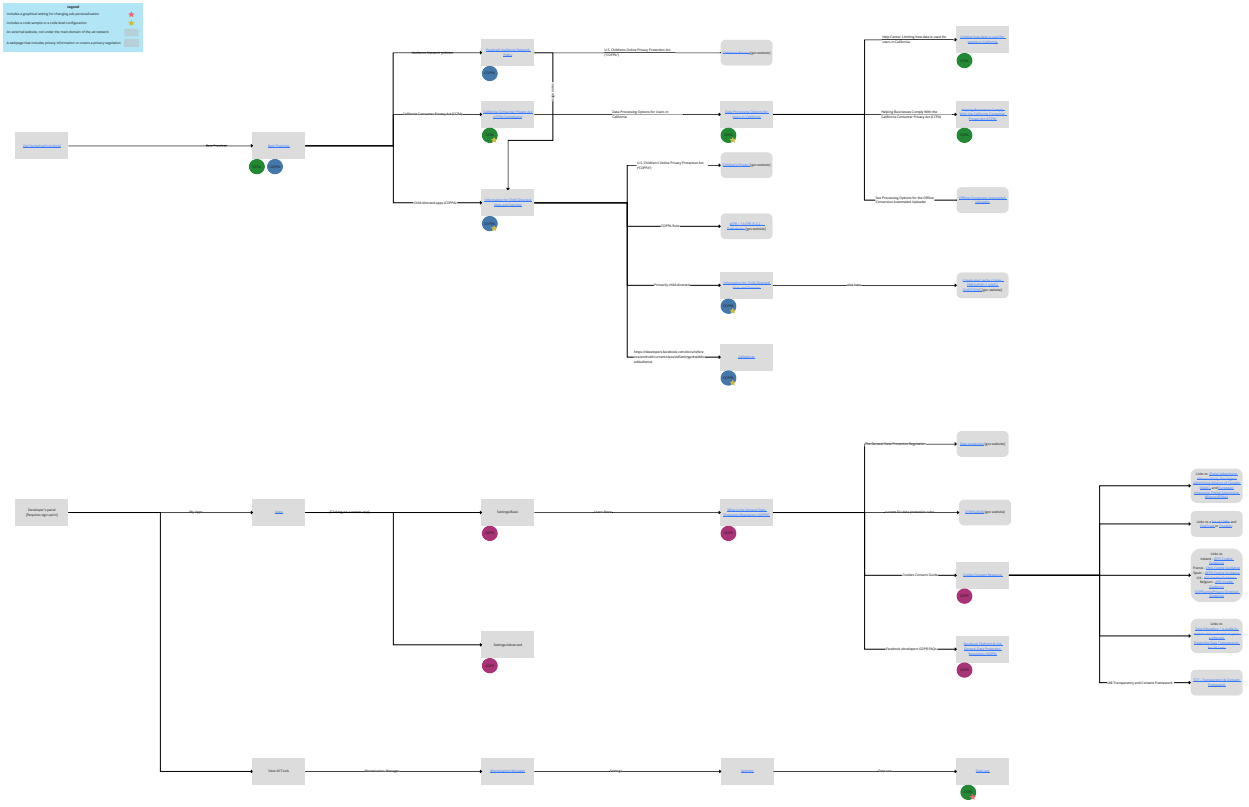
- If the publisher *is* using the "Force GDPR Applies" flag, consent is valid for users for whom the `forceGDPRApplies` (Android) or `forceGDPRApplicable` (iOS, Unity) flag is on.

  If, in a later update, the publisher decides that they no longer want to use the "Force GDPR Applies" flag, new users will be treated as subject to GDPR as determined by MoPub, and any existing users for whom the `forceGDPRApplies` flag was previously set will still be treated as subject to GDPR as defined by publisher. This cannot be revoked by any means except with app deletion and re-installation.

Table 3. Participants' demographics. Seen ad networks: F: Facebook Audience Network, G: Google AdMob, and T: Twitter MoPub.

ID	Recruitment channel	Seen ad networks	Target OS	Primary role at most recent job	Student	Yrs of experience in software dev	Yrs of experience in mobile dev	Yrs of experience in Android dev	Yrs of experience in iOS dev	Used ad networks in the past 3 yrs	Main source of income in software dev	% of revenue dependent on ads	Involvement in choosing ad networks	Involvement in configuring ad networks	Involvement in integration of ad networks	GDPR knowledge	CCPA knowledge	COPPA knowledge	Number of employees in most recent app development company	Age	Continent of residence	Gender
P1	CS student mailing lists	FGT	iOS	Developing software	Yes	5	5	1	5	Google AdMob	Salary from software or mobile development but NOT dependent on software revenue	10%	A great deal	A little	A lot	Moderately knowledgeable	Not knowledgeable at all	Not knowledgeable at all	Freelancer	21	Europe	Male
P2	CS student mailing lists	T	Android	Developing software	Yes	6	2	2		Google AdMob	I don't make money from software or mobile development		A great deal	A great deal	A great deal	Slightly knowledgeable	Not knowledgeable at all	Not knowledgeable at all	1-9 employees	33	Europe	Male
P3	Prolific	FGT	Android	Developing software	No	15	6	6		I haven't worked with any ad networks in the past three years	Primarily salary and bonuses, partially dependent on software revenue		Not at all	Not at all	Not at all	Very knowledgeable	Not knowledgeable at all	Moderately knowledgeable	1,000-9,999 employees	35	Europe	Male
P4	Freelancer.com	FGT	iOS	Developing software	Yes	5	5	5	3	Google AdMob, Unity Ads	Salary from software or mobile development but NOT dependent on software revenue		A great deal	A moderate amount	A great deal	Not knowledgeable at all	Not knowledgeable at all	Slightly knowledgeable	Freelancer	25	Asia	Male
P5	Linkedin	GT	iOS	Developing software	No	11	11	1	10	Google AdMob, InMobi, Flurry	Salary from software or mobile development but NOT dependent on software revenue		A lot	A lot	A great deal	Slightly knowledgeable	Not knowledgeable at all	Slightly knowledgeable	1,000-9,999 employees	33	Asia	Male
P6	Freelancer.com	FG	Android	Developing software	No	3	2	2	1	Google AdMob, Facebook Audience Network, Flurry	Primarily direct software revenue		A moderate amount	A moderate amount	A moderate amount	Very knowledgeable	Moderately knowledgeable	Very knowledgeable	Freelancer	23	Asia	Male
P7	Prolific	FGT	iOS	Developing software	No	10	5	3	5	Google AdMob, Facebook Audience Network, Unity Ads	Salary from software or mobile development but NOT dependent on software revenue		A little	A lot	A moderate amount	Moderately knowledgeable	Not knowledgeable at all	Not knowledgeable at all	10-99 employees	40	Europe	Male
P8	Twitter	FT	Android	Developing software	No	5	4	4		I haven't worked with any ad networks in the past three years	Salary from software or mobile development but NOT dependent on software revenue		Not at all	Not at all	A little	Slightly knowledgeable	Not knowledgeable at all	Not knowledgeable at all	10-99 employees	24	Asia	Male
P9	Linkedin	FGT	iOS	Developing software	No	6	6	5	6	Unity Ads, Flurry	Salary from software or mobile development but NOT dependent on software revenue		A little	A little	A little	Very knowledgeable	Not knowledgeable at all	Moderately knowledgeable	1,000-9,999 employees	30	Europe	Female
P10	Freelancer.com	FG	Unity	Developing software	No	3	3	3		Google AdMob, Unity Ads	Salary from software or mobile development but NOT dependent on software revenue		A little	A little	A little	Slightly knowledgeable	Not knowledgeable at all	Slightly knowledgeable	Freelancer	26	Europe	Female
P11	Slack	FGT	Android	Other (Bioinformatics researcher)	No	2	1	2		Google AdMob, Facebook Audience Network, Amazon Mobile Ad	I don't make money from software or mobile development	15%	A lot	A moderate amount	A moderate amount	Very knowledgeable	Slightly knowledgeable	Moderately knowledgeable	1-9 employees	30	Europe	Male

Fig. 4. Diagram of pages related to privacy regulations on Facebook Audience Network. The zoomed in section shows a part of the diagram for demonstration purposes.



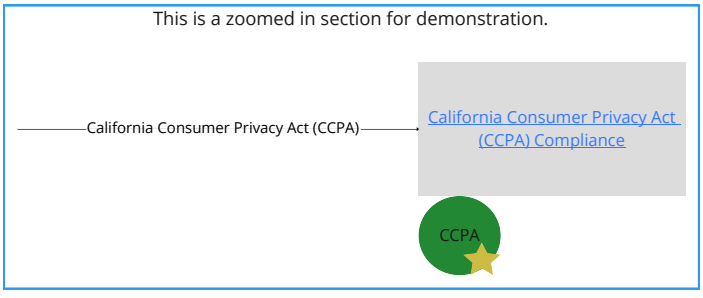


Fig. 5. Diagram of pages related to privacy regulations on Google AdMob.

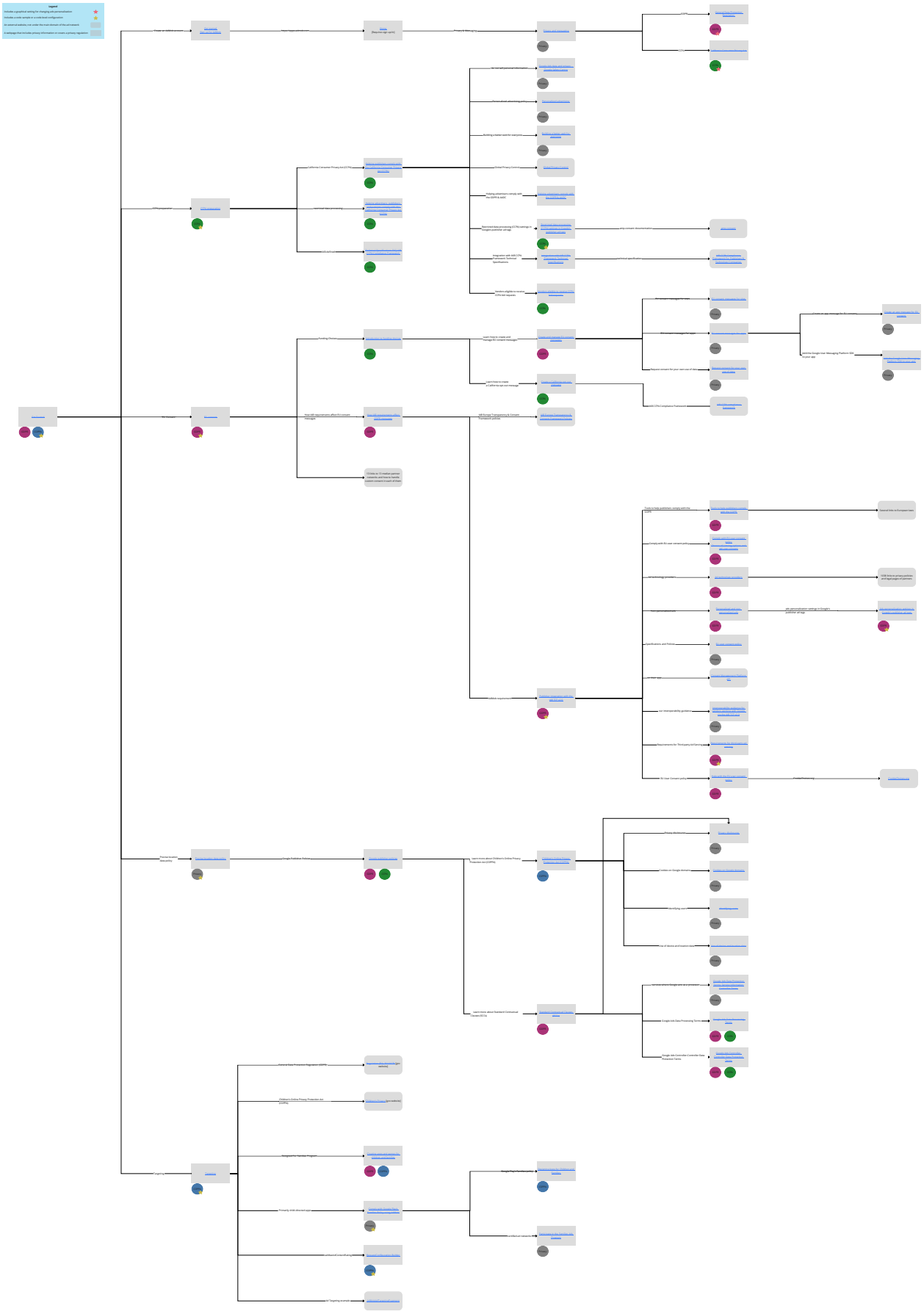


Fig. 6. Diagram of pages related to privacy regulations on Twitter MoPub.