Understanding Challenges for Developers to Create Accurate Privacy Nutrition Labels

Tianshi Li
Carnegie Mellon University
Pittsburgh, USA
tianshil@cs.cmu.edu

Kayla Reiman
Carnegie Mellon University
Pittsburgh, USA
kreiman@cmu.edu

Yuvraj Agarwal
Carnegie Mellon University
Pittsburgh, USA
yuvraj@cs.cmu.edu

Lorrie Faith Cranor
Carnegie Mellon University
Pittsburgh, USA
lorrie@cmu.edu

Jason I. Hong
Carnegie Mellon University
Pittsburgh, USA
jasonh@cs.cmu.edu

ABSTRACT

Apple announced the introduction of *app privacy details* to their App Store in December 2020, marking the first ever real-world, large-scale deployment of the *privacy nutrition label* concept, which had been introduced by researchers over a decade earlier. The Apple labels are created by app developers, who self-report their app's data practices. In this paper, we present the first study examining the usability and understandability of Apple's privacy nutrition label creation process from the developer's perspective. By observing and interviewing 12 iOS app developers about how they created the privacy label for a real-world app that they developed, we identified common challenges for correctly and efficiently creating privacy labels. We discuss design implications both for improving Apple's privacy label design and for future deployment of other standardized privacy notices.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; • **Software and its engineering**;

KEYWORDS

Privacy, Privacy Nutrition Label, iOS Development, Developer Study, Interview

ACM Reference Format:
Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I. Hong. 2022. Understanding Challenges for Developers to Create Accurate Privacy Nutrition Labels. In *CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 24 pages. https://doi.org/10.1145/3491102.3502012

1 INTRODUCTION

In 2009, Kelley et al. [17] proposed and evaluated the first privacy nutrition label for websites. In this seminal work, they argued that companies should provide a clear, uniform, brief summary of what data is collected along with how it is used and shared (similar to a standardized nutrition label on food) to complement privacy policies, which are often lengthy, ambiguous, and hard to understand. In 2013, some of the same authors proposed privacy nutrition labels for mobile apps [19]. After a decade, this concept has finally made its way from the research lab into the two major mobile app stores. As of December 2020, Apple requires all apps to provide *app privacy details*, which the Apple app store displays as a privacy label in an App Privacy section on each app's product page to empower users to learn about the app's collection and use of data before installation (Figure 1 left). Following Apple's new requirements, Google also announced that a similar *safety section* would be rolled out in the Google Play app store in early 2022 (Figure 1 right).

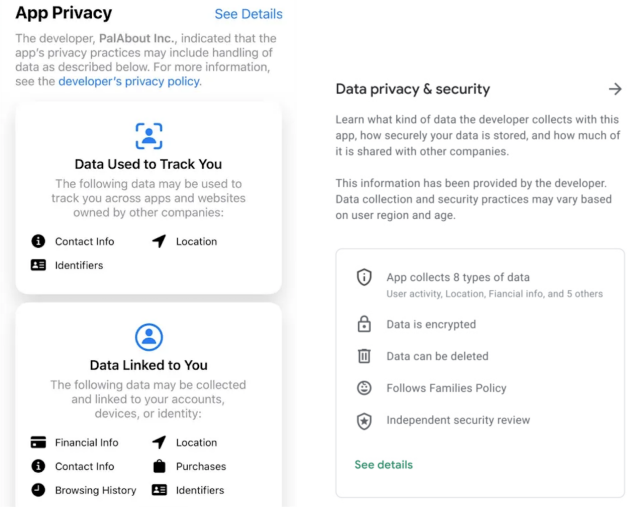

Figure 1: An example of iOS' privacy labels (left) and Android's tentative design for its forthcoming safety section (right).

The usefulness of privacy nutrition labels and any future standardized privacy notices is highly contingent on their accuracy. However, we currently have little understanding of developers' ability to create accurate privacy nutrition labels. Even assuming that developers are motivated to create accurate privacy labels, it

CHI '22, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9157-3/22/04.
https://doi.org/10.1145/3491102.3502012

is not a trivial task. Developers need to comprehend the definitions of all of the data types and uses in the app store's framework. They also need to understand the data practices of their apps, including practices associated with any third-party libraries they may have included. Finally, they need to choose the proper disclosures to describe the data practices of their apps. Furthermore, developers need to be aware of any changes in the app's data practices and update the privacy nutrition labels in a timely manner. This process may be challenging for developers who are often not experts in privacy and treat privacy as a secondary goal [4, 20].

Apple's large-scale deployment of the privacy nutrition label concept offers an opportunity to study how developers create privacy labels for their apps. In this paper, we take the first step to examine the usability and understandability of privacy nutrition labels from the developers' perspective by probing iOS developers' perceptions and practices around Apple's privacy labels. By identifying common errors and challenges that developers face when creating Apple privacy labels, we aim to uncover limitations in Apple's privacy label design and offer timely design recommendations for platforms that want to deploy privacy nutrition labels. Using Apple privacy labels as an example, our findings may also shed light on how to support developers to provide accurate information in any future standardized privacy notices.

More formally, we have three research questions:

RQ1 What are developers' perceptions about privacy labels?
RQ2 What types of errors or misunderstandings do developers exhibit when creating privacy labels?
RQ3 What challenges do developers face in filling out forms to create privacy labels accurately and efficiently?

We investigate these research questions by observing 12 iOS app developers creating an Apple privacy label and interviewing them about this process remotely. During the study, we asked our participants to create a privacy label *for a real-world app that they developed*. We then interviewed them to identify potential mismatches between the actual data collection behavior of the app and what they initially specified in the privacy label, examined what caused the inaccuracies, and probed their attitudes and actions regarding privacy labels. We qualitatively analyzed the interview transcripts using a bottom-up open coding approach to identify developers' perceptions, recurring errors and misunderstandings, and challenges regarding Apple privacy labels.

From our interviews, we learned that although many iOS developers considered Apple's privacy labels beneficial and were willing to disclose their data practices, accurately filling out the forms to create a privacy label was a challenging task. We identified recurring errors and misunderstandings about privacy labels shared by many participants that were potentially caused by knowledge gaps and task complexity. A novel finding was that while Apple uses definitions of privacy-related terms that are relatively unusual and specific, many developers assumed more general definitions, leading to errors in their privacy labels. Furthermore, developers had trouble correctly disclosing data practices of third-party libraries, partly because they were not fully aware of the libraries' data practices and because they did not know about the existence of resources that could help them with this task. We present both concrete short-term design recommendations for the platforms and long-term research directions to improve the accuracy of privacy labels by providing better developer support.

2 BACKGROUND AND RELATED WORK

In this section we introduce the Apple privacy nutrition labels and then discuss prior research on privacy nutrition labels and on the challenges developers face in meeting privacy requirements.

2.1 App Privacy Details

In December 2020, the Apple App Store introduced *App Privacy Details*[1] to help users learn about the privacy practices of an app before downloading it. The privacy details are shown in the *App Privacy* section when installing the app (Figure 1 left). This section contains two layers. On the first layer, users can see the high-level data categories that the app collects (e.g., location) and whether this data category is linked to users or used to track users. Users can click the *see details* link to see the second layer, which includes more specific data types (e.g., Coarse/Precise location), what the data is used for (e.g., Third-Party Advertising, App Functionality), and whether each data type is linked to users or used to track users. If the developer has reported that no data is collected by the app, the *App Privacy* section shows *Data Not Collected*. If the developer has not filled out the privacy details, this section shows *No Privacy Details Provided*.

All the privacy details are self-reported by app developers using a web-based tool on the Apple developer dashboard *App Store Connect* (Figure 2). This tool breaks down the process of submitting privacy details into two stages and walks developers through the process using a series of wizard interfaces. In the first stage (Steps 1 and 2 in Figure 2), the developer needs to select whether their app (or third-party partners) collects data, and if so, what data types are collected. Then, all the selected data types are displayed on one page, with developers expected to provide details for each data type. In the second stage (Steps 3a-3c in Figure 2), the developer needs to indicate what the data type is used for (i.e., purposes), whether the data type is linked to users, and whether the data type is used to track users. Some questions require a binary answer, such as whether data is collected, linked to users, and/or used to track users. Other questions require developers to select options from pre-defined taxonomies (i.e., data types and purposes). The key concept definitions are presented in the developer interface when a related question is encountered.

Importantly, we note that developers can update the privacy details without updating the app itself, while they cannot release a new app or update an existing app if they haven't submitted the privacy details. The privacy details are published immediately after submission and are not verified by the App Store before publishing. In our study, we examined the types of errors that developers may make when submitting privacy details, focusing on non-malicious errors, for example those caused by developer misconceptions.

2.2 Privacy Nutrition Label Research

Website privacy policies are well known for being long and difficult to read [16, 24]. To make it easier for users to quickly glean important information from those policies and to compare privacy

[1] https://developer.apple.com/app-store/app-privacy-details/

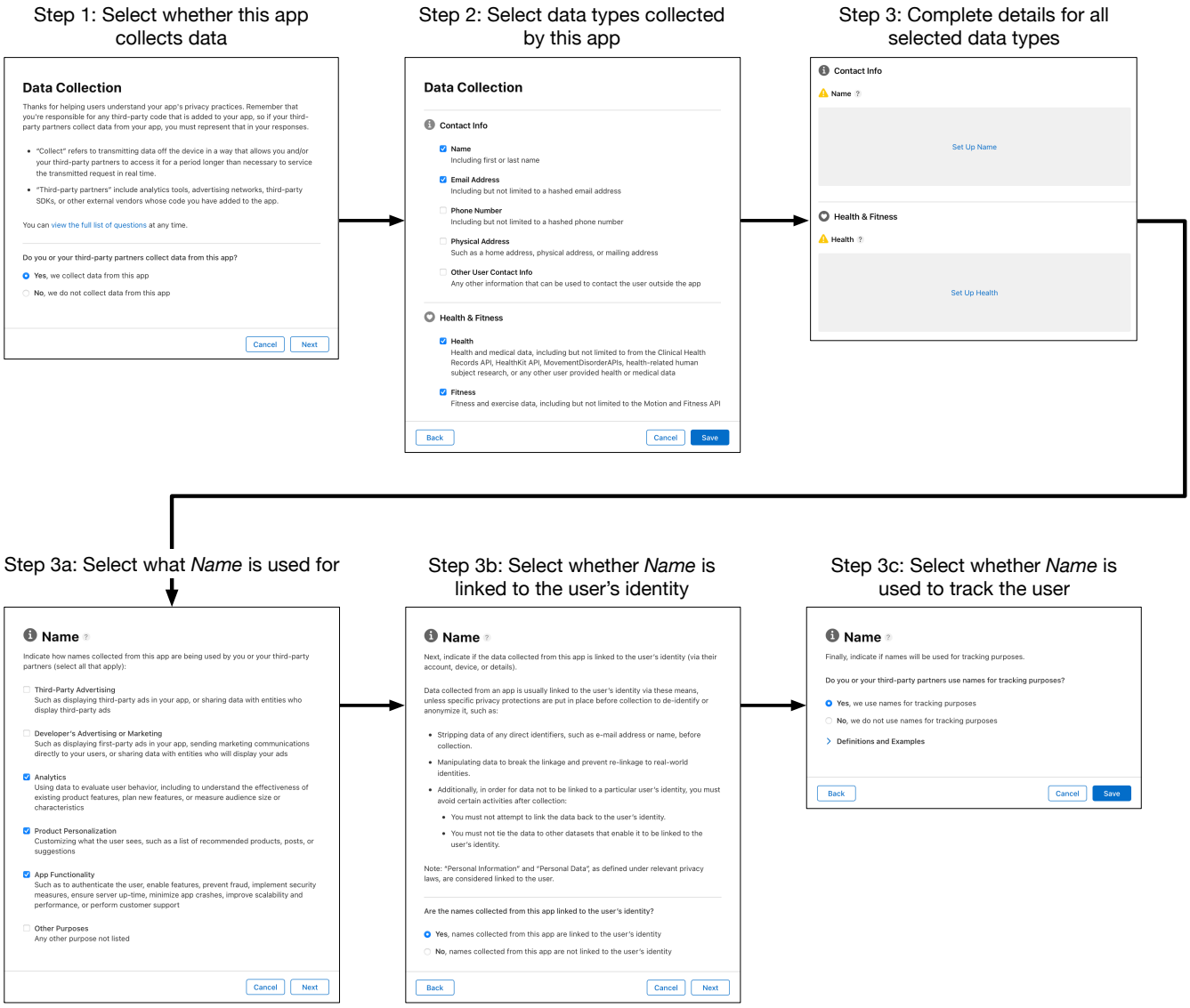

Figure 2: A demonstration of Apple's web-based developer tool for submitting privacy details to create a privacy label (which we replicated for our study). In Step 1 the developer selects whether their app or third-party partner collects data. If the app collects data, the developer indicates what data types are collected in Step 2. In Step 3 the selected data types are displayed in one page with a link next to each data type to a three-part form for providing details about the purposes for which that data type is collected and whether or not it is linked to users and/or used for tracking (Steps 3a-3c, using the data type *Name* as an example).

practices between websites, Kelley et al. [17] proposed and evaluated a design for privacy nutrition labels for websites, drawing on lessons from the food nutrition labeling literature such as adopting a standardized and brief format. Kelley et al. [18] evaluated the proposed privacy label design, comparing it with shorter tabular and text variants as well as traditional long privacy policies in a large-scale randomized controlled trial. The researchers found that standardized labels could increase both speed of finding information and accuracy of users' comprehension. They found that privacy labels allowed users to better compare policies, and users found standardized formats more enjoyable to read.

In 2013, Kelley et al. [19] followed up with a privacy nutrition label design for mobile apps, demonstrating that labels presented clearly and at relevant times could affect users' decisions when choosing between similar apps. Later Emami-Naeini et al. [13] proposed a privacy and security label for Internet of Things devices and showed it could help consumers incorporate privacy and security into their IoT device purchase decisions.

Table 1: Design Recommendations Based on Research on Privacy Nutrition Labels From the User's Perspective.

Name	Suggested Practice	Main Source(s)
Standardization	Uniformity in formatting and terminology helps consumers gain familiarity and compare practices between labels.	[10, 18, 34]
Length	Shorter policies can be read more quickly and improve users' recall.	[18, 24, 31, 34]
Salience of first layer	A simple first layer helps people focus on critical elements. Since not everybody will click through, this should have the most salient information in it.	[10, 13, 25, 31]
Early usability studies	Users' interpretations of terms in context may not match expert opinions. Checking usability before deployment is crucial, and earlier is better.	[7, 31]
Relevant presentation	Users are more likely to pay attention to notices in-app as the information becomes relevant, rather than only being shown in the app store when scrolling is required and users may lack context and interest to understand them (but they should also be included in the app store for motivated users to view prior to app download).	[6, 12, 31]
Pairing notice with choice	Beyond promoting awareness via notices, privacy controls (i.e. choices) are crucial.	[10, 31]
Machine Readability	Making notices machine-readable is a pre-requisite for automation and the potential for enforcement.	[10, 28]
Incentives and Enforcement	Widespread adoption is dependent on incentives and enforcement, as shown through the failure of P3P adoption.	[10]

Researchers have also investigated how to maximize the benefits of privacy labels by exploring and evaluating design variants of privacy nutrition labels in multiple dimensions [6, 10, 13, 18, 28, 31, 34]. This line of work has yielded design recommendations for improving the design of privacy nutrition labels, as summarized in Table 1.

In this work, we take the first step in studying privacy nutrition labels *from the developer's perspective*. More specifically, we examine challenges developers face in filling out forms to create privacy labels accurately and efficiently. Although our study is contextualized in the specific design of Apple's version of privacy labels and the associated developer tool, we expect our findings can also shed light on issues and design opportunities for other forms of privacy nutrition labels and standardized privacy notices in general.

2.3 Challenges for Developers in Handling Privacy Requirements

Software developers have increasing responsibility to deal with the ever-growing privacy requirements from platform providers (e.g. Apple and Google) and recently enacted laws (e.g. GDPR, CCPA), and consequently face an increasing number of challenges. Although we are not aware of prior work that studied the task of creating privacy nutrition labels, our study was informed by prior work that identified privacy-related challenges for developers in other contexts [4, 20, 21, 33, 35, 36].

A fundamental issue that has been repeatedly identified is that developers often view privacy as a secondary goal [4, 20]. Therefore, they may prioritize other factors over privacy, such as time to market and usability. However, even when developers care about privacy it is still challenging to meet privacy requirements. A major reason is related to blindspots in their knowledge. For example, past work found that developers tend to reduce privacy to security issues, ignoring other privacy goals such as improving data transparency [5, 33]. Tahaei et al. [35] found that developers often rely on Stack Overflow for privacy advice, but these posts were biased towards a partial set of privacy design strategies. Furthermore, it may be challenging for developers to maintain awareness of all of their apps' data practices, especially when apps are developed by large teams or use third-party libraries. Balebako et al. [5] found that developers were overwhelmingly unaware of data collected by pervasive third-party tools for ads and analytics. Li et al. [20] found that developers sometimes lost track of the data practices of their apps because they are not well-documented. Another type of challenge is related to the extra overhead for fulfilling privacy requirements. Specifically, Li et al. [21] observed on the r/androiddev subreddit that many developers held a negative attitude towards platform or legal requirements about privacy because they were perceived as burdensome and not beneficial to developers.

Prior research has identified platform requirements as a major driver for developers to take privacy-related actions, which in turn leads them to ask privacy-related questions on Stack Overflow [1, 35, 36] and have privacy-related discussions on platform-specific developer forums [14, 21].

Other prior work highlights the difficulty that people face in describing data use using a standard set of terms. Balebako et al. [7] tested both crowd workers' and privacy experts' ability to categorize realistic data-sharing scenarios using a predefined taxonomy, which is similar to the task that developers face in creating a privacy label. They found that there was much variance in participants' understanding of the concepts in the taxonomy, even among experts. We found similar variances among developers' understanding in our studies.

To the best of our knowledge, this is the first work that examines the challenges developers face in creating privacy labels. In the context of this new task, we identified challenges echoing prior findings such as developers under-reporting data collection because they were not fully aware of the data practices of their third-party libraries [5]. We also identified new challenges, such as developers relying on their preconceptions, which led to errors in privacy labels. We used a novel study method, observing developers conducting

the task based on the actual apps they developed using a replica of the real-world interface. We believe this approach may yield more in-depth understandings of the challenges developers encountered in real life than recall-based interviews [5, 20] or studies that used hypothetical scenarios [32] or asked developers to modify other people's apps [22].

3 METHODS

We recruited 12 iOS app developers to observe how they filled out the privacy label forms for their own apps. We employed this approach to leverage developers' familiarity with their own apps and their previous experiences creating privacy labels to gain in-depth understandings of real-world challenges. Then we followed up with a semi-structured interview to examine developers' perceptions about this task and to better understand their approach. The study sessions were conducted remotely on Zoom in July and August, 2021.

3.1 Recruitment

We recruited our participants from Prolific, Upwork, and Twitter. Prolific is a website for recruiting research study participants and Upwork is a freelance website. On Prolific, we selected the predefined criteria "Industry - Software" and "Computer Programming - Yes" to narrow down the search scope to only people who self-report as a developer. On Upwork, the job we posted about this study was visible to all registered freelancers, and we sent separate invites to some developers who showcased iOS apps they developed in their portfolios. On Twitter, we posted on our personal accounts about this study. We wanted to gather a diverse sample with varying levels of privacy knowledge and familiarity with privacy labels. Hence, we intentionally did not mention privacy labels or use any other privacy-related language in our recruiting materials. For example, in our recruiting post, we described the study goals as: "We are recruiting iOS developers to offer perspectives on the process of submitting apps to the app store."

We used a pre-screening survey to check the eligibility of potential participants. Among other questions, we asked for the App Store links for up to three iOS apps that they recently developed. Since creating privacy labels is part of the app submission and update process on the App Store, we screened out people who had not participated in developing an English-language app that had been released on the App Store. The complete pre-screening survey appears in Appendix A. We invited participants who provided at least one valid App Store link to participate in our study. Of the 225 people who responded through Prolific, 17 passed the pre-screening and 10 actually participated. Of the 6 people who responded to the job posting on Upwork, 2 passed the pre-screening and 1 actually participated. The only person signed up via our recruiting post on Twitter passed the pre-screening and participated in the study.

Per Prolific's community guidelines, we had a separate study solely for pre-screening purposes and added the IDs of people who passed the pre-screening to the allowlist of the main study. Regardless of acceptance into the interview phase, people who completed the pre-screening survey were compensated $0.50 USD[2]. Upwork supports embedding the pre-screening questions in the job post and therefore requires no extra payment. For Twitter, we embedded the pre-screening survey link in the post. All 12 participants completed the main study and were compensated $70 USD each.

3.2 Demographics and Selected App Information

Our sample covers developers from different countries and with varying iOS development experiences (Table 2). Our participants were fairly young: six participants self-reported to be within the 18-24 age group, five within 25-34, and one within 55-64. One participant self-identified as non-binary and the other 11 all self-identified as males. We interviewed one Black participant, one mixed-race participant, and 10 White participants. Although we tried several platforms to post recruiting messages and invited all qualified participants, our participants were mostly young, White, and male. This may be related to the gender, race, and age gaps in the iOS developer community.

As shown in Table 2, we obtained a diverse set of apps for the study. The 12 apps came from eight categories with different purposes and number of downloads. For example, we interviewed a developer who developed an app as a personal hobby with less than 1,000 downloads, and the developer of a large-scale commercial app with over 500K downloads. The participants held various roles in their respective teams, including six who developed both the front-end and back-end parts of the project, and six who only coded the front-end part.

Moreover, there were some apps that already had a privacy label as well as some that did not, an indicator of participants' varying levels of familiarity with Apple's privacy label. Four out of the 12 apps did not have a privacy label before the study, five apps had a privacy label stating "Data Not Collected," and three apps had a privacy label that specified some data collection practices.

3.3 Study Design

We selected one app for each participant from their pre-screening survey responses so that we could contextualize our inquiries about privacy labels in a concrete and familiar context. For developers who mentioned multiple apps on the screening survey, we selected the most recently updated app that had an English version. Before the main study, we used a pre-study survey to gain more understanding of the app and the developer, such as the number of downloads and the developer's location. The interviewers also browsed the app product page before the interview to familiarize themselves with the app, especially the app functionality, the current privacy label (if it had one), and the current privacy policy.

During the study session, we observed how the developer filled out the privacy label form for the selected app and conducted a semi-structured interview afterward to delve into this process. We asked the participant to keep sharing their screen and recorded both the audio and the screen for later analysis. The length of the study

[2]The first 30 people were offered $0.35 for an advertised two-minute survey, but after seeing the initial timing data, this was subsequently adjusted to $0.50 for a three-minute survey

Table 2: Participant Overview. Our sample features a good sample of developers and apps across several dimensions, including participant's iOS development experience (*iOS Exp.*), participant's geographic location (*Location*), app categories (*App Cat.*), app downloads (*Downloads*), app development purpose (*Purpose*), app development team size (*Team Size*), and participant's role(s) in the development team (*Participant's Role(s) In Team*). The app development purposes involve four options, covering situations when the participant developed the app as part of their job (*Job*), as part of their hobby (*Hobby*), for a course project (*Course*), and for a research project (*Research*).

ID	iOS Exp.	Location	App Cat.	Downloads	Purpose	Team Size	Participant's Role(s) in Team
P1	1-2 years	Portugal	Music	Under 1K	Job	2-5	Mobile App & Backend Developer, Designer, Project Manager
P2	2-3 years	Italy	Games	1K-10K	Course	2-5	Mobile App Developer, Designer, Quality Assurance Analyst
P3	2-3 years	Canada	Business	50K-100K	Job	2-5	Mobile App & Backend Developer
P4	> 5 years	UK	Business	1K-10K	Job	1	Mobile App Developer
P5	< 1 year	Greece	Travel	500K-1M	Job	> 20	Mobile App Developer
P6	1-2 years	South Africa	Education	1K-10K	Job	2-5	Mobile App Developer
P7	1-2 years	USA	Music	1K-10K	Hobby	1	Mobile App & Backend Developer
P8	1-2 years	USA	Food&Drink	Under 1K	Hobby	1	Mobile App & Backend Developer, Designer, Quality Assurance Analyst
P9	2-3 years	USA	Education	10K-50K	Research	1	Mobile App & Backend Developer
P10	4-5 years	USA	Lifestyle	1K-10K	Hobby	2-5	Mobile App & Backend Developer, Project Manager, Quality Assurance Analyst
P11	1-2 years	UK	Education	Under 1K	Job	2-5	Mobile App Developer
P12	> 5 years	UK	Productivity	1K-10K	Research	2-5	Mobile App Developer, Designer, Researcher

session ranged from 1.5 to 2.5 hours. The full version of the pre-study survey and the interview script are included in Appendix B and D.

This study was approved by the Carnegie Mellon University Institutional Review Board. At the beginning of each study session, the interviewer briefed the participant on the study goals and procedures and then asked them to sign a consent form.

3.3.1 Direct observation of privacy label creation. In the first part of the study session we asked the participant to create a privacy label for their app using a replica of Apple's official website for this task that we implemented (detailed in Section 2.1).[3] To make this experience more realistic, the interviewer instructed the participant to handle this task as they normally would and take as long as they needed, and encouraged them to look at any documentation they would normally consult, except for the app's current privacy label on the App Store (if it had one). The interviewer also encouraged them to mention any resources or person they needed to consult, including anyone unavailable at the moment, and anything they were confused about. We also deferred answering their questions to the end of the study, to minimize any potential impact on their perceptions and reasoning process.

3.3.2 Semi-structured interviews for in-depth understandings of challenges. After the participant created the privacy label, we followed up with a semi-structured interview to help us spot inaccuracies in the privacy label they created and to understand what caused these inaccuracies. Participants were shown an online survey during the interview to help present text information such as the definitions of privacy label concepts (complete version attached in Appendix C). Participants read the information on the survey and discussed their responses with the interviewer, who asked follow-up questions based on participants' responses.

The interviewer first guided the participant to thoroughly report and reflect on their app's data use to identify possible inaccuracies. For each data type initially reported as being collected, we asked the participant to explain whether the data were collected by any third parties, by themselves, or both; whether and where the data were stored; what were the purposes for collecting the data and how they selected the purposes in the privacy label; how they determined whether or not the data were linked to users; and how they determined whether or not the data were used to track users. For developers who did not specify any data collection, we asked them to briefly introduce the app functionality and why they believed no data was collected.

We then used two sets of questions to uncover missing data practices that should have been reported. The first was about use of third-party libraries, which past work has found to be a common source of privacy issues to end users [2, 9, 23] and challenges for developers [5, 27]. During the study, the interviewer first asked the developers to report all libraries used in this app via the online survey. Then the interviewer asked them if they were aware of any

[3]Our source code of the website is available at: https://github.com/i7mist/privacy-label-questions

data collected by these libraries and how they figured out the data practices of these libraries.

The second set of questions was about developers' perceptions of key concepts in Apple's standard vocabulary for privacy labels. The goal was to help the participant align their understanding of these concepts with Apple's definitions, and potentially recall more data practices and recognize errors. This process was also facilitated by the online survey, which presented Apple's official definitions of the concepts and asked participants whether each of them was surprising, unclear, or unreasonable.[4] The definitions were displayed across multiple pages of the survey in random order. To understand their mental model, the interviewer prompted the participant to keep thinking aloud as they read through these definitions and asked follow-up questions about their understandings, confusions, and what they liked or disliked about the definitions.

Then we zoomed out and asked questions about how developers filled out privacy labels in real life, covering aspects including teamwork and collaboration, app monetization, privacy-related design decisions, and app update plans. Finally, we asked participants to compare the privacy label created during the study and the current privacy label on the App Store (if the app had one) and offer their perspectives on the differences. We concluded the interview by soliciting their perceived pros and cons of providing a privacy label for their app on the App Store and gathering feedback on Apple's design of the developer interface for this task.

During the interview, we encouraged participants to identify and fix inaccuracies themselves and reassured them that our goal was not to measure their performance, and that we would anonymize all findings in any publications to make them comfortable talking about fallacies in their understanding and practices. In addition, the interviewers also noted any inconsistencies between what participants told them and what they had implemented in their privacy label during the first part of the study, and prompted participants to verify and fix related errors in the privacy label after examining the definitions of related concepts. For example, the interviewer asked the participant to consider editing the privacy label if they mentioned some user data being stored with the user ID but did not specify the data as *linked to users*.

3.4 Qualitative Analysis

Guided by the three research questions, we qualitatively analyzed the interview transcripts and screen recordings using a bottom-up open coding method facilitated by the software MAXQDA. Our analysis involved two rounds of coding as recommended by Saldaña [30].

In the first round of coding, two researchers coded the same four interviews independently to develop a codebook. When coding the same four interviews, the two researchers held daily meetings to discuss their codes, reconcile coding discrepancies, and iteratively merge their codebooks. By the end of the first round of coding, we derived an initial codebook with 95 codes. Then the two researchers collectively conducted an axial coding analysis to merge similar codes and group them into high-level themes for answering the three research questions.

In the second round of coding, the remaining eight interviews were each independently coded by one of the two researchers using the new codebook (each researcher coded four interviews). Minor changes were made to the codes and themes as needed, and all changes were discussed and agreed by both researchers in a series of weekly meetings. Per the recommendations of McDonald et al. [26], we did not calculate the inter-rater reliability because our goal is to identify emergent themes rather than seek agreement. The final codebook contains 25 codes grouped into 8 themes. The themes are detailed in the following sections, and the complete codebook (including codes and memos) is included in Appendix E.

4 RQ1 RESULTS: DEVELOPERS' PERCEPTIONS OF PRIVACY LABELS

Developers were heavily involved in the creation of privacy labels. Among our participants, nine out of the 12 developers were in charge of releasing or updating the app in the App Store, and five out of the eight developers of the apps that already had a privacy label before the study said that they participated in creating their apps' privacy labels. We observed both positive and negative perceptions of Apple's privacy labels from the developers we interviewed, including mixed feelings from many of our interviewees.

4.1 Privacy Labels Are Helpful to Users and Developers (All but P5)

Most participants agreed that providing a privacy label is beneficial to their users. They felt that users deserved to know their apps' data practices and they had nothing to hide. When speaking of the impact of privacy labels on users, some participants shared their personal experiences as a user to explain why they supported privacy labels.

> *It's something that I care very much about, so I think it's a very good thing that it's happening in general. And I think it's probably overdue based on how much data that you know, has been collected over the past few years, especially given there's more and more data collected. So I really like that Apple has done this, even though it might be a pain for a little bit for developers to get used to. I think it'll be a good thing in the long run for people's privacy.* (P7)

Moreover, because Apple's privacy label provides an easier way for developers to inform users of everything their apps are doing, it was also perceived as beneficial to developers: "*Having transparency as a developer could mean trust, and having users' trust is always something, to me personally, important.*" (P2) When asked what may be some negative aspects of providing a privacy label for his app, P9 said,

> *I don't see any negative aspects to that. I think, if anything, there are benefits that both developers can ensure they're including everything that's relevant to the users need to be aware of, and it just makes it easier for the users to see. So I can't imagine there are any negatives to this.*

[4] The concepts we examined included *data collection*, *data linked to users*, *data used to track users*, and Apple's pre-defined taxonomies of data uses (such as *Third-Party Advertising*) and data types (such as *Contact Info*). Source: https://developer.apple.com/app-store/app-privacy-details/

Conversely, P5, who was part of a large app-development team, did not view the privacy label as helpful to developers because he considered privacy was not the responsibility of developers.

4.2 Filling out Privacy Labels Was Perceived as Challenging Extra Work (P2, P3, P4, P6, P7, P8)

Many participants perceived accurately filling out privacy labels to be challenging, especially for apps that collected a lot of data. For example, P8 individually developed an app as part of their hobby. With the help of the interviewer, he corrected several errors in the privacy label due to misunderstanding of some key concepts in Apple's definitions. Later in the interview, he expressed his frustration as follows: "*I'm not like a big company or whatever, so it's a little hard to go through all this information. And as you can see, I didn't get everything totally accurate.*"

4.3 Filling out Privacy Labels Was Perceived Easy for Apps not Collecting Much Data (P1, P4, P11, P12)

In contrast, we found participants who did not collect much data perceived creating privacy labels a simple task. For example, P12 developed an app without a back-end and therefore did not store any data, and he said, "*In terms of creating it, I mean, for me, it was very easy because I purposefully don't collect data.*" P4 represented an intriguing case because his app originally used the Google Analytics library (part of Google Firebase, which was mentioned interchangeably with Google Analytics by P4) but he had intentionally replaced it with a simpler analytics library to simplify the privacy label creation process. This is a promising example that requiring developers to provide standardized privacy notices may give them incentives to adopt more privacy-friendly designs.

4.4 Erring on Side of Caution for Ambiguities (P3, P4, P7, P8)

Ambiguities are a common issue for developers when creating privacy labels, often due to undefined behaviors and vague concepts in Apple's documentation. Interestingly, we found that a recurring strategy to deal with these ambiguities is to err on the side of caution. For example, P4 was using third-party crash analytics services and was not sure whether they should count as *data used for tracking users*. Although Apple's definition of tracking only mentions "data linked with third-party data for advertising measurement purposes" and "data shared with data brokers," P4 still reported this data use for crash reporting as tracking and explained his rationale as follows: "*If I'm erring, I'm erring on the side of not underestimating how much data we use, if you see what I mean, I'm trying to be as honest as I can.*" At a high level, this strategy is in line with their positive perceptions of using privacy labels to increase transparency for users.

4.5 Filling out Privacy Labels Stimulated Reflections (P1, P4, P6, P7)

Some developers viewed this task as beneficial, as it prompted them to reflect on their privacy practices. P6 reflected on his data use:

> *I think the positive thing is, it forces the developer to think about all the data that they're capturing. Every time you're adding a new column, every time adding a new table, it's important to think of the information that's being collected, you know, and usually, we think about it in performance terms. but we never think about in the privacy context.*"

P7 adjusted his privacy policy to make it more consistent with the privacy label:

> *I tried to make it similar [to the privacy label], like I added this sentence at the end of it, 'any information is possibly collected is not retained longer than reasonably necessary', I added that sentence from the [privacy label] template because any information that's used isn't retained any longer than I needed.*

4.6 Developers Felt Unconcerned About Privacy and that It Was not Their Responsibility (P5, P6)

There were also participants not as concerned about filling out privacy labels or protecting user privacy in general. The app that P5 participated in developing was the most downloaded app in our sample and they also had the most complicated development team structure. This app was a joint effort between four organizations, with one developing the mobile app, two working on the back-end, and one for UI/UX design. All four organizations worked for a client company that actually owned the app. Therefore, P5's perception of developers' responsibility is limited to the specific mobile app development work. "*From my experience, the developer will not handle the app privacy. When an organization have teams for privacy, it's not his work to do this. That's my opinion. We are just here to make things.*" (P5)

4.7 Concerns About Users' Distrust (P2, P7)

Nevertheless, participants who generally supported Apple's privacy labels also expressed concerns about users' distrust in privacy labels, which is related to the fact that all privacy labels are self-reported and do not undergo a standard verification process by Apple. For example, P7 mentioned that one of his users complained that the app was collecting IP addresses while its privacy label indicated "Data Not Collected." Although he explained to the user that the IP addresses were used for serving a request but not stored, which did not count as data collection per Apple's definition, he still got a bad review on the App Store.

5 RQ2 RESULTS: RECURRING ERRORS AND MISUNDERSTANDINGS IN PRIVACY LABELS

Although most participants felt positive about Apple's Privacy Labels and were willing to disclose their data practices, we found that errors and misunderstandings were still prevalent in the privacy labels generated during the study. Specifically, nine out of the 12 participants made errors, and seven confirmed and fixed

them during the interview.[5] Moreover, among the eight apps that already had a privacy label before the study, six of our participants re-created a privacy label in our study that was inconsistent with the label published on the App Store. In this section, we provide an overview of developers' recurring errors and misunderstandings that may lead to errors (summarized in Table 3).

5.1 Errors: Underreporting data collection (False Negative)

The first type of errors are cases where developers did not report an actual data practice.

5.1.1 Missing Linked Data (P1, P2, P5, P6, P7, P9, P11, P12). Many participants had a misconception about *Data Linked to Users* – namely, they did not consider data that is not identifiable on its own as data linked to users, even if the data was stored with other identifiable information. For example, when asked about his understanding of what counts as data linked to users, P2 immediately responded "*anything that could lead me to a person in real life.*" Since this misconception repeatedly emerged among the first five participants, we added a question in our protocol to more formally examine this issue. In this question, we presented a table to represent a hypothetical relational database, containing three columns corresponding to the data types: user ID, phone number, and date of last login respectively. Then we asked our participants which of these three data types were linked to users in this scenario. The correct answer should be all of the three data types because the date of last login is stored on the same row of the other two identifiable data types. However, only two of the seven participants (P8, P10) correctly selected all three data types, with the other five missing date of last login and two of them also missing user ID because these data types were not perceived as identifiable.

5.1.2 Missing Third-party Data Use (P1, P5, P6, P7, P9, P10). Analytics and social media are two types of third-party libraries that were commonly used by our participants and may have unexpected data collection behaviors. However, developers tended to focus on the data directly associated with the libraries' functionality (e.g., user account information for social media libraries) or data they can directly view from the third-party services (e.g., crash reports for analytics libraries). When asked whether he considered if any data can be automatically collected by Firebase, P6 answered, "*I don't think so. My understanding of the data that's collected by Firebase is how we use Firebase.*" This echoes prior work's findings that developers often have limited understanding of libraries' data practices under the hood [5].

5.1.3 Missing Data Types (P3, P6, P10). This error refers to when developers did not report all data types collected and stored on their back-end server. The developer tool for generating privacy labels is structured such that if the developer did not select all data types correctly in the first place, they would not have the chance to provide further details for how these data types were used, stored, and shared (see Figure 2). Some participants missed data types for reasons such as not checking all data types carefully, having wrong preconceptions about a certain data type not being personal, and forgetting to include data types that were newly collected in recent versions.

5.1.4 Missing Interactions Outside the App (P1, P6). Some developers did not report data collected or used outside the app. For example, P6 mentioned that to send a newsletter they only used the email address collected by the app and used an external service MailChimp to look up the customer's name based on the email address. He only reported *Email Address* but not *Name* data as being used for Developer's Advertising or Marketing purpose, because he perceived it as "*a different process that's outside of the app*" (P6).

5.1.5 Missing Optional Data Practices (P3, P4). Some developers did not report data practices that were optional. [6] For example, P4 provided their users with the option to enter their name in the system so the users could be addressed using their name rather than the email address. However, he did not mark it as used for the *Personalization* purpose, because "*It's personalization, but it's optional. We don't insist that they give us the name.*" On the other hand, he did indicate that the collected email addresses were used for personalization, because "*we do insist they give us the email.*" (P4)

5.2 Errors: Overreporting data collection (False Positive)

The second type of errors are cases where developers reported more than the actual data practices.

5.2.1 Overreporting Tracking (P1, P3, P6, P8, P9, P10, P11, P12). Apple's definition of *data used to track users* only covers very specific tracking scenarios – namely, linking data about a particular user or device with third-party data for advertising measurement purposes or sharing the data with data brokers. However, some of our participants did not read the definition in detail and relied on a casual interpretation of tracking, such as location tracking (P9) or tracking users' interactions (P10). Some participants carefully read the definition, and even a few of those had similar misconceptions. For example, P11 explained his interpretation of Apple's tracking definition as "*Obviously, there are other scenarios where, you know, tracking will be used not just for advertisement, but just for kind of user profiling really.*"

5.2.2 Reporting Data Not Stored on Backend (P4, P5, P6). Apple's definition of *data collection* uses very specific criteria – namely, the data is transmitted off the device and stored in the backend. We asked participants if each data type specified in their privacy label was stored, and if so, where it was stored. We found that some developers missed these criteria and reported data that was collected but not stored (P5) or data only stored on device as data collection (P4, P6).

[5] We changed our study protocol slightly after the first two participants. For these two participants, we only told them they were encouraged to correct their errors but did not prompt them about particular errors. Since we found that developers did not seem to have enough incentives to actively make corrections, we changed the protocol and actively confirmed the potential errors that we identified during the interview with the other ten participants.

[6] Apple lists four criteria that must all be satisfied in order for disclosure to be considered optional, with optional data collection satisfying only one of these criteria. Source: https://developer.apple.com/app-store/app-privacy-details/

Table 3: An overview of recurring errors and misunderstandings in privacy label identified during our study (RQ2).

Error Type	Error Name	Explanation
Underreporting	Missing Linked Data	Not reporting data stored with identifiable data as linked because the data itself is not identifiable.
	Missing Third-party Data Use	Not reporting all third-party data use.
	Missing Data Types	Not reporting all collected data types based on Apple's definition.
	Missing Interaction Outside the App	Not reporting data collection happening outside the app.
	Missing Optional Data Practices	Not reporting certain data practices because they were optional.
Overreporting	Overreporting Tracking	Over-generalizing tracking scenarios (Apple's definition only considers data linked with third-party data for advertising measurement purposes or shared with data brokers as data used to track users)
	Reporting Unstored Data	Reporting data not stored on the back-end as collected
	Reporting Apple SDK Data Use	Reporting data collected by Apple SDK (Per Apple's guideline, developers are not responsible for disclosing Apple's data collection)

5.2.3 Reporting Apple Data Use (P1, P6, P8). The documentation for developers mentions that developers are not responsible for disclosing data collected by Apple services, such as using MapKit, CloudKit, or App Analytics (which is automatically available for all iOS apps on the Apple app store). However, some developers still reported data practices that were only due to these Apple frameworks in their privacy label. We note that these data practices may be relevant to users, and this exception case for data collection by Apple may result in inconsistencies between what apps report and what users understand about an app's data practices.

6 RQ3 RESULTS: CHALLENGES FOR CREATING ACCURATE PRIVACY LABELS

In this section, we delve into developers' challenges for creating accurate privacy labels to identify possible causes of errors and misunderstandings discussed in the previous section. We grouped these challenges into three themes (see Table 4). The first two themes are related to gaps in developers' knowledge, and the last theme is related to complexities that developers may encounter throughout the app development life cycle.

6.1 Unknown Unknowns: Situations Where Developers Don't Realize that They Don't Know Something

The first theme is *Unknown Unknowns*, which encompass situations where developers were unaware of the errors that they may have introduced into the privacy labels. Under these circumstances, developers often trusted in their own judgement (and were sometimes wrong), and only realized their problems later on with the help of external prompts.

6.1.1 Blinded by Preconceptions (All but P12). As we guided the participants to closely examine all the definitions, almost all of them realized some of the errors they made due to their preconceived understandings of Apple privacy label concepts that were inconsistent with Apple's definitions. These preconceptions were deeply tied to many of the errors identified in the previous section (Table 3). For example, P9 initially explained his understanding of "data used for tracking" as "*live tracking.... where, you know, some apps will track your location in the background even when you're not using them.*" However, after the interviewer showed him Apple's definition of this concept again, he was surprised that it differed from his expectations:

> *I guess my question so much as just being surprised that tracking here only refers to advertising. That's not what I would anticipate that to mean, like, either as an end user or developer. That's not the word I would use for that.*

Note that the same definition was shown to him in Apple's interface while he created the privacy label, but he did not realize the discrepancy between his understanding and Apple's definition, indicating that he likely did not read or did not remember Apple's definition when trying to accomplish this task during the study. In fact, we believe these errors may be more frequent in practice than in our study, since some participants told us they were more careful creating their privacy label for the study than they were in real life. When asked to contrast the experience for our study versus in the real world, P11 said, "*As obviously, with regards to the study, I just probably thought about it more, whereas I might have glanced over it (in real life).*"

6.1.2 Knowledge Blindspots (All but P3, P7, P8). We found two types of knowledge blindspots during the study.

Not familiar with Apple Privacy Labels (P2, P6, P9, P10, P11, P12). Many participants acknowledged that they were not familiar with Apple Privacy Labels before the study. Some developers had never heard about privacy labels and so had never considered creating them for their own apps, though this was mainly true of developers for apps that had not been updated for a while. Some had heard about it or seen it on the App Store as a user, but had never created a privacy label themselves. Some developers knew they needed to create a privacy label but had misunderstandings about the overall process and therefore deferred their plan. For example, some misunderstandings include believing that they can only update the privacy label with a new version release, or that updating the privacy label will trigger a new round of review process. One participant said,

Table 4: An overview of developer's challenges for filling out privacy labels accurately and efficiently (RQ3).

Challenge Level	Challenge Type	Summary of Challenges
Unknown unknowns	Blinded by Preconceptions	Developers were overconfident in their preconceptions of certain concepts (e.g., data collection, linking, tracking) while their understanding differed from Apple's definitions.
	Knowledge Blindspots	Developers were not familiar with Apple privacy labels and did not know resources that could help them with the task.
	Misinterpreting Definitions	Developers misinterpreted Apple's definitions and did not realize the issue without external prompts.
Known unknowns	Limitations of the Apple's Documentation	Developers found part of the developer tool and the official documentation hard to understand, confusing, or ambiguous.
	Lacking Team and Org Support	Developers were only responsible for part of the project and did not know all data practices.
Complexities	Overwhelmed due to Info Load	Developers needed to spend a lot of time and effort to read and understand the large amount of information in the official content.
	Memory Challenge	Developers struggled with multiple types of memory challenges, such as recalling the exact definitions of certain concepts and their apps' data practices.
	Challenges of Cross-platform Apps	Developers who developed cross-platform apps needed to deal with duplicate requirements from different platforms.
	Communication Cost	Developers had trouble communicating and collaborating with their teammates, employers, and clients to create and update privacy labels.

> *I assumed that if you would change something, that might trigger something on [the App Store], and we have the need to be temporarily pulled for review. That would be the only thing that would make me hesitant.* (P9)

Not accessing library documentation (P1, P4, P5, P6, P9, P10). Many libraries have created documentation to specifically prepare developers for creating privacy labels, such as analytics libraries like Google Analytics and social media libraries like the Facebook SDK. However, during our interview, none of the developers that used these libraries pulled up any of these resources made for this task or mentioned that they had checked them in real life when asked about how they figured out what data was collected by the libraries used in their apps, which suggested that they were unaware that this documentation existed. We discussed this issue with P4, since he switched from Google Analytics to another library because he could not figure out exactly what data types were collected by Google Analytics and also distrusted Google's privacy practices. Initially he said,

> *What you really need is something I don't think Google will ever provide, which is a quick way of answering Apple's questions in the context of Google Analytics. But I've never found a document that does that.* (P4)

After the interviewer showed him the Google Analytics' documentation for this task,[7] he was very surprised and said, "*And then I apologize to Google. But this was not there when I was doing this.*" (P4)

6.1.3 Misinterpretation of Definitions (P1, P2, P4, P5, P7, P8, P10, P11). We further observed that developers may misinterpret Apple's definitions even after reading them carefully. For example, although P8 had been asked to carefully read the definition of *data used to track users*, he still held an incorrect understanding of the scope of tracking per Apple's definition: "*Data tracked is like you're using it to personalize stuff, and like personalized ads or other content.*" (P8) Although he did notice "used for advertising purposes," he expanded that to content personalization in general, which is an over-generalization of the tracking definition that may lead to overreporting of tracking (as discussed in Section 5.2.1).

6.2 Known Unknowns: Situations Where Developers Are Unsure About Their Own Understanding

In the second theme, we report on developers' confusion about Apple's requirements and uncertainty about their understanding and their answers for generating the privacy label.

6.2.1 Limitations of Apple's Documentation (All participants). Our participants voiced much confusion regarding Apples documentation related to privacy labels, including the instructions in the web-based developer tool and the documentation about app privacy details, especially about concept definitions presented in both the tool and the documentation.

[7] https://support.google.com/analytics/answer/10285841

Table 5: A summary of expressions that more than one developers found confusing or hard to comprehend in Apple's official documentation and the web-based developer tool for filling out privacy labels.

Reasons for confusion	Expressions that developers found hard to understand
Unfamiliar tech concept	screen name, social graph, *hashed* email address/phone number, approximate location services, a latitude and longitude with *three or more decimal places*, link the data back to users' identity, the Motion and Fitness API
Jargon	data broker, third-party data, purchase tendencies
Difference by country	credit score

Hard-to-understand expressions in Apple's documentation (All but P11). Many participants found certain concepts and definitions hard to understand because they used unfamiliar jargon, unfamiliar technologies, or concepts that were not commonly used in countries other than the U.S. (summarized in Table 5).

For the first group of issues, developers did not have sufficient technical knowledge about what certain terms mean or how to obtain certain types of data. For example, Apple defines the data type *Email Address* as "Including but not limited to a hashed email address." However, several developers were not sure what *hashed* email address means here. Specifically, P12 explained his confusion as follows, "*I'm gonna sound like a noob for a person who has computer science background, but I don't know what a hashed email address is. In this case, I'll google this.*"

The second group of issues includes privacy-related concepts that developers were unfamiliar with. For example, many developers had never heard of the term *data broker*, which is an essential part of Apple's definition of tracking. When P7 examined the definition, he said, "*I suppose one question I have is mostly just what is a data broker? I'm not actually sure off the top of my head. That would be something I would want to look up.*"

Because Apple's definitions seemed to be designed primarily for the U.S., some issues were caused by developers from outside the U.S. not understanding terminology specific to the U.S. P1 and P2 both mentioned that they did not understand the term *credit score*. P2 said, "*The other one credit score, I feel like it's something there that only works in the U.S., which I'm not familiar with.*"

Vague, ambiguous definitions need clarification or examples (All but P5 and P9). Our participants also found many of the official definitions vague and ambiguous, and hoped that Apple could provide more examples or clarifications. One representative example is the frequent use of "other types" categories, such as Other Data Types and Other Purposes. Although participants understood the necessity of providing a catch-all term to cover corner cases, they found it hard to imagine what instances could fall into these categories and hence found them very confusing. Specifically, P11 considered the *Other Data Types* concept "*the most egregious one*" as compared to other similar concepts such as Other Financial Info, because "*the other ones were a bit vague, but at least they were tied into something.*" (P11)

Ineffective examples (P4, P7, P8, P12). Conversely, developers did not always perceive providing more examples as helpful. For example, when defining *Sensitive Info*, Apple simply lists a number of data types such as racial or ethnic data, sexual orientation, or biometric data. One participant found it confusing, because, "*It seems like it's just giving random things. I guess they could clarify more on what it means by that, instead of just giving examples.*" (P8)

6.2.2 Lacking Support for Teams and Organizations (P3, P4, P5, P6, P7, P8, P9). Developers also talked about challenges regarding not receiving sufficient support from their development team or their organization, as well as the challenges of working on their own. One type of challenge was that developers may only have control over and understand part of the life cycle of data collected by their apps. This problem mainly applied to developers employed by large companies (e.g., P5) or developers developing apps for a client (e.g., P3, P6, P9). For example, P9 developed an app for a research project and shared much of the back-end data with the researchers, but he was not sure how the researchers used the data from then on. Nevertheless, P9 was responsible for submitting the app to the App Store and filling out the privacy label, which suggests that he may not be able to comprehensively summarize the data practices of this app.

Other challenges include lacking sufficient written documentation to understand the apps' data practices especially when they were a new member of an old project (P3, P4, P5), organizational training for fulfilling this task (P4, P6, P8), and wanting help from legal experts for interpreting complicated definitions (P3, P7, P8).

6.3 Complexities: Extra Overhead Required for Creating Privacy Labels

The third theme of challenges concerns factors that caused significant overhead in creating privacy labels, which is orthogonal to the previous themes about knowledge gaps that may cause inaccuracies in the privacy labels.

6.3.1 Overwhelmed due to Information Load (All but P3 and P11). Most participants felt this task overwhelming and time-consuming due to information load, especially for first timers. The vagueness and ambiguities in the definitions aggravated the problem, since developers had to read certain definitions several times to gain enough confidence in their understanding. For example, when explaining his confusion about the definition of tracking, P12 said, "*I didn't find it unclear after reading it several times. But I think that's just the nature of these things are quite complicated.*"

Moreover, the pain of reading all the information may discourage developers from updating privacy labels in a timely manner. P1 expected to update privacy labels twice per year, which means "*you have a six month gap where you can collect data without telling people,*" because "*upgrading it, or at least reviewing it on every update would be tiresome.*" (P1)

6.3.2 Memory Challenges (P1, P2, P3, P4, P8, P10, P11, P12). To correctly fill out privacy label forms, developers need to grapple with multiple types of memory challenges. First, developers sometimes did not remember their rationale for selecting certain options when

previously generating a privacy label, which could cause inconsistencies. For example, P10 changed the selection of purposes for a specific data type during the study, but he couldn't recall why he initially made a different selection. The second type concerns the challenge of remembering the definitions. We noticed that some developers who had just read and discussed the definitions of some concepts roughly thirty minutes earlier had trouble recalling these concepts. For example, P4 and P12 both forgot the exact resolution of coarse and precise location.

The third type was related to challenges of keeping track of their apps' data practices. When comparing P10's re-created privacy label with the real-world privacy label, he found that he forgot they collected search history during the interview.

> *I don't think we keep track of search history? That's why I think that was a miscommunication there... Okay, I take that back. Sorry. We actually do [store the search history] on Algolia. It keeps track of like, what searches popped up the most, but it's not linked to specific users.*

The fourth type was regarding challenges of remembering to update a privacy label in a timely manner. P10 found that the *Contacts* data type was missing on their privacy label on the App Store, because they forgot to update the privacy label when adding Contacts data collection in recent versions.

6.3.3 Challenges of Cross-platform Apps (P1, P3, P6, P7, P8, P9, P11, P12). Many participants developed one web app for both the Apple App Store and the Google Play Store, which means that they need to handle requirements on both platforms. Since Android recently announced their plans of rolling out a similar requirement on Google Play (see Figure 1), these developers would need to do duplicate work for generating the Google privacy label. Another challenge is regarding maintaining the privacy label. Because these web apps allow for server-side updates, data practice updates may not need to go through the App Store, increasing the likelihood of having outdated privacy labels.

6.3.4 Communication Cost (P3, P4, P6, P8, P9, P12). We identified many challenges for creating and maintaining privacy labels regarding developers' communication with different entities, such as other developers, their boss, their clients, and their former employers. First, different people on the team may have different priorities and may not all care about privacy and privacy labels. P4 said he had a big fight with other team members when deciding to replace Google Analytics with a library to trade off functionality for better privacy: "*I have to say not everybody was happy with that choice*" (P4). He explained that the complexity of creating the label and the ambiguities of Apple's documentation made it hard to fulfill his boss' expectations:

> *...at the end of the day, you have to go to your boss and say, 'Well, I don't know if I really understood this correctly. But here's the answer.' You know, my boss wants a definite answer. He doesn't want ambiguities. Especially if I spent three days doing it.* (P4)

Second, communication was harder when early members already left the team, and for projects that were a joint effort of several different teams or even different organizations (P10). Third, some developers released the app using an organization account, which made it harder to update the privacy label if they have left the organization. Although theoretically the employer should take over the responsibility of updating the privacy label once the original developers have left, this may not be realistic in some situations. For example, P12's app developed for his research project published under the university's account did not have a privacy label at the time we interviewed him. He explained that "*I no longer work for this university. I worked very closely with them, but ultimately, this is managed by the university and their IT team.*"

7 DISCUSSION

We begin by discussing why it is important for privacy labels to be accurate and the barriers to label accuracy that we observed. Next we discuss the positive impact of privacy labels, including the possibility that they may encourage developers to adopt more privacy-friendly practices. We offer several short-term design implications and suggest directions for future research. Finally we review some limitations of our study.

7.1 Importance of and Barriers to Creating Accurate Privacy Labels

Accuracy is an essential requirement for privacy labels and any standardized privacy notice in general. Individual users can only get a correct understanding of apps' data practices if labels are accurate. Conversely, if many privacy labels are inaccurate, it may lead to distrust by users and impede long-term adoption. Through our studies, we learned that the causes of inaccuracies are complicated, and even developers with benign intentions may inadvertently introduce errors. Table 4 summarizes challenges developers face regarding privacy labels. Although knowledge gaps are the direct causes of many inaccuracies, the fundamental issue is the general complexity of this task. Furthermore, we believe this task will be even more challenging in practice; during the study, developers were fully concentrating on this task and could discuss any confusion with the interviewers, who were privacy researchers already familiar with privacy labels.

Our findings echo developers' challenges for other privacy tasks as identified by prior work, such as limited awareness of third-party library data use [5], regarding privacy as a secondary concern [1, 4, 20], and lacking privacy design and engineering knowledge [3, 15, 32]. These same problems are present in this new task and may substantially diminish the usefulness and trustworthiness of privacy labels or standardized privacy notices in general. This suggests the importance of studying developers' perceptions and practices in usable privacy research.

The three *Unknown unknowns* challenges are novel findings that have not been identified in prior work. They are crucial problems, as developers do not actively do further research to check their understanding and correct their mistakes under these circumstances. Moreover, some kinds of resources to help developers handle privacy requirements (e.g., third-party libraries' guides to filling out the label form) may not be useful unless they are more accessible to developers.

7.2 The Positive Impact of Privacy Labels on User Data Privacy

We observed some positive impacts of privacy labels on user privacy. First, several developers considered privacy labels a convenient and transparent way to disclose data practices and therefore beneficial to both users and developers (Section 4.1). Second, some developers liked the label creation task because it offered them an opportunity to reflect on their data practices and the privacy implications (Section 4.5). Third, a few developers even took further action to modify their apps and traded functionality for privacy. For example, P7 updated his app's privacy policy to improve the consistency with the privacy label (Section 4.5) and P4 replaced Google Analytics with a less privacy-invasive data analytics library to streamline the privacy label creation process (Section 4.3 and 6.3.4). These findings suggest that requiring developers to offer a more succinct, readable privacy notice may incentivize them to adopt privacy-friendly designs, since collecting less data will make creating privacy labels easier. All these positive implications echo findings about the important role platforms play in shaping developers' perceptions and practices regarding privacy [21, 36]. Importantly, past research has found that developers do not like platform policies that impose rigid restrictions on data collection [21], but our study observes that they do seem to support the requirements for more disclosure of data practices to end users. This suggests that developers may be more amenable to improving data transparency and that privacy labels may also lead to a voluntary reduction in data collection.

7.3 Design Implications: Short-term Design Recommendations and Future Research Directions

7.3.1 Short-term Recommendations. We first present design recommendations that require relatively minor changes.

Revise definitions to improve clarity. We identified minor changes in definitions that may be helpful for improving developers' comprehension. Many participants mentioned that they wanted to see more concrete examples in the definitions. For example, what is considered data linked to users? What might fall under the *Other Data Type* category? Developers may be unfamiliar with certain technologies or jargon (e.g., *hashed* email address, data broker), which should be avoided or explained. Furthermore, platforms should be wary of using a common term like *tracking* but associating it with an unusual or special definition because developers may not always pay attention to or fully understand that definition. To improve clarity, terms like "longer than necessary" that are subject to developers' interpretations should generally be avoided, or facilitated with more objective criteria.

Clarify common misconceptions proactively. Given that the misconceptions were concentrated on certain concepts, such as *data linked to users* and *data used to track users*, platforms may want to provide proactive warnings of potential misconceptions. Furthermore, some developers had misconceptions about the process of filling out the privacy label, such as they had to wait until the next version release to update the privacy label or that updating the privacy label would trigger an app review. The platform should also clarify these misconceptions up front in the developer tool.

Check internal validity and consistency of labels. Per Apple's definitions, some concepts are interrelated, though developers used them independently. For example, if the developer specified certain data is used for *Third-Party Advertising*, it is likely that the data is also *used to track users*. If the developer reported the collection of personally identifiable information such as name or email address, it is likely that the data is also *linked to the users*. Currently, Apple does not verify the privacy labels, but it would be useful and relatively easy if platforms check them for internal validity and consistency, and prompt developers when there is a potential error. A complementary approach is to auto-fill part of the answers based on their dependencies with information that have already been provided by developers.

Use formats other than text for guidance. Parts of the current privacy label documentation and the developer tool (specifically the paragraphs about optional disclosure, linking, and tracking) are text-heavy, making comprehension difficult. Thus, it may be beneficial to present the same information in other formats, perhaps using diagrams, videos, or interactive materials with quizzes to help developers check whether their understanding of key points is correct. For example, since we found that developers often only perceived data identifiable on its own as linked to users, it may be helpful to use a diagram that emulates the structure of a database to showcase under what circumstances the data is considered linked to users, similar to the example we used in our study (Section 5.1.1).

7.3.2 Directions for Future Research. Next, we discuss future research directions to address more fundamental issues.

Verify the privacy label against actual data practices. Currently, Apple does not check for the validity of the self-reported privacy labels, which means that developers do not get feedback that would help them discover their misconceptions. One essential reason is that Apple currently employs a definition of data collection that prevents complete verification unless auditors have access to the app's back-end data storage (which is infeasible). However, partial verification may still be possible, for example if auditors consider separately local access, data transmission, and remote storage. Local access and data transmission could be more easily verified. In iOS 15, a new feature called "Apple Privacy Report" already reveals some information about local data access and data transmission to end-users.[8] The privacy report shows which apps access permission-protected resources such as location, camera, and photos at what times. Analyzing the exact data transmitted outside of an iOS app is a very challenging problem, but researchers have demonstrated some promising solutions. For example, Egele et al. [11] statically analyzed more than 1,400 iOS apps and found over half of the apps leaked the unique ID of the device over the network. Note that the difficulty largely comes from the heavy security restrictions imposed by the iOS platform such as app encryption, which means that it is likely an easier task if conducted by the platform.

Even using the current definitions, it is feasible to verify parts of the privacy label automatically — for example, using the identifier for advertising (IDFA) as an indicator of tracking and analyzing third-party libraries used in the app [8].

[8] Apple App Privacy Report: https://developer.apple.com/news/?id=n5jlz7ox

Support code-based auto-filling or auto-generation of privacy labels. Another direction to both improve the accuracy of privacy labels and reduce the burden on developers is to automatically fill out part of the privacy label forms based on code analysis. Prior research has studied code-based generation of privacy policies [37] and in-app privacy notices [22]. Similarly, we envision code-based auto-generation of privacy labels would also be a compelling idea, especially for handling third-party libraries and for generating different versions of privacy labels of cross-platform apps. The privacy label generator may be integrated with the IDE [20, 22, 29] and use developers' annotations to improve the accuracy (e.g., detecting network requests and asking developers to specify storage practices).

Conduct usability tests with a wider range of developers. Although a number of studies have investigated the usability of privacy labels from users' perspectives (Table 1), there is limited understanding from developers' perspectives. Our study offers a first step towards understanding developers' perspectives, but further testing with a more diverse sample of developers would be helpful — aiming for diversity in location, technical proficiency, gender, English fluency, and other factors.

Reconcile differences across platforms and helping developers handle platform differences. We already noticed a few differences between Apple's design and Google's tentative design of privacy labels (Figure 1). For example, Google requires developers to disclose data as *Collected* as long as it is transmitted off the device, while Apple's definition of data collection requires both transmission and backend storage (i.e. having access for "a period longer than what is necessary").A further challenge is that the iOS guidance specifies"You are not responsible for disclosing data collected by Apple", while Google does not offer the same stipulation. Therefore, developers handling requirements from both platforms may get more confused and make more errors. Ideally, these platforms should work together to make their definitions as consistent as possible and provide usable and accessible developer support to handle the differences.

Iteratively evaluate and improve the label design and developer tools. In our analysis, we regarded Apple's definitions of privacy label terminologies as the gold standard and referred to the difference in developers' understandings from Apple's definitions as "misinterpretations." However, we acknowledge that Apple's definitions may be imperfect and that the label design itself may benefit from improvements. Ideally, the design of a standardized privacy notice should use definitions that match the intuitive understandings of users and developers (or other roles who are responsible for filling out privacy label forms). Further work is needed to assess users' understanding of Apple privacy labels and the extent to which the labels are useful to them as they make decisions about downloading apps and providing information to them. Given our observations of the difficulties developers had in understanding privacy label concepts and jargon, we would expect to find even more confusion among end users. We recommend a more holistic assessment of what information is most useful to convey to users, how best to convey it, and how to support developers in reporting their app's data practices accurately and efficiently.

7.4 Limitations

This research has several limitations. First, due to the recruiting platforms and the gender, age, and race gaps of the iOS developer community, our sample mainly comprises young, White, male developers coming from North America and Europe. A useful future direction is to conduct survey studies at scale with a more diverse sample. Second, although we reassured our participants that we would only release anonymized findings and we did not intend to evaluate their abilities, they may not have all felt comfortable expressing controversial or negative opinions about privacy labels. Lastly, although we have confirmed potential errors and misunderstandings with participants, we did not have access to their code or database and therefore could not verify these errors. Hence there may have been more errors than the interviewers were able to observe. However, given the context provided, we consider our findings still yielded useful insights into the patterns and fallacies in developers' perceptions and practices about privacy labels.

8 CONCLUSIONS

In this paper, we present the results of 12 semi-structured interviews with iOS developers regarding Apple's privacy labels. This is the first study that examined the usability and understandability of privacy labels from developers' perspectives. We learned that our participants generally held positive attitudes towards privacy labels, but were also concerned about users' distrust in the labels and the extra workload associated with creating them. We identified a set of common errors and misunderstandings, and discussed the challenges of knowledge gaps and task complexity that caused these issues. Finally, we discussed the design implications, including concrete short-term design recommendations for platform providers such as Apple and Google to improve their design of privacy labels from developers' perspectives, as well as long-term research directions that may benefit the adoption of standardized privacy notices in general.

ACKNOWLEDGMENTS

This research was supported in part by the National Science Foundation under Grant No. CNS-1801472, Air Force Research Laboratory under agreement number FA8750-15-2-0281, and Innovators Network Foundation. Tianshi Li was supported in part by the CMU CyLab Presidential Fellowship. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Laboratory or the U.S. Government. We thank the anonymous reviewers for their constructive feedback.

REFERENCES

[1] Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L. Mazurek, and Christian Stransky. 2016. You Get Where You're Looking for: The Impact of Information Sources on Code Security. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE. https://doi.org/10.1109/sp.2016.25

[2] Yuvraj Agarwal and Malcolm Hall. 2013. ProtectMyPrivacy: detecting and mitigating privacy leaks on iOS devices using crowdsourcing. In *Proceeding of the 11th annual international conference on Mobile systems, applications, and services - MobiSys '13*. ACM Press. https://doi.org/10.1145/2462456.2464460

[3] Nitin Agrawal, Reuben Binns, Max Van Kleek, Kim Laine, and Nigel Shadbolt. 2021. 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*. ACM. https://doi.org/10.1145/3411764.3445677

[4] Rebecca Balebako and Lorrie Cranor. 2014. Improving App Privacy: Nudging App Developers to Protect User Privacy. *IEEE Security & Privacy* 12, 4 (jul 2014), 55–58. https://doi.org/10.1109/msp.2014.70

[5] Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason Hong, and Lorrie Faith Cranor. 2014. The Privacy and Security Behaviors of Smartphone App Developers. In *Proceedings 2014 Workshop on Usable Security*. Internet Society. https://doi.org/10.14722/usec.2014.23006

[6] Rebecca Balebako, Florian Schaub, Idris Adjerid, Alessandro Acquisti, and Lorrie Cranor. 2015. The Impact of Timing on the Salience of Smartphone App Privacy Notices. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*. ACM. https://doi.org/10.1145/2808117.2808119

[7] Rebecca Balebako, Richard Shay, and Lorrie Faith Cranor. 2014. Is Your Inseam a Biometric? A Case Study on the Role of Usability Studies in Developing Public Policy. In *Proceedings 2014 Workshop on Usable Security*. Internet Society. https://doi.org/10.14722/usec.2014.23039

[8] Kai Chen, Xueqiang Wang, Yi Chen, Peng Wang, Yeonjoon Lee, XiaoFeng Wang, Bin Ma, Aohui Wang, Yingjun Zhang, and Wei Zou. 2016. Following Devil's Footprints: Cross-Platform Analysis of Potentially Harmful Libraries on Android and iOS. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE. https://doi.org/10.1109/sp.2016.29

[9] Saksham Chitkara, Nishad Gothoskar, Suhas Harish, Jason I. Hong, and Yuvraj Agarwal. 2017. Does this App Really Need My Location?: Context-Aware Privacy Management for Smartphones. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 3 (sep 2017), 1–22. https://doi.org/10.1145/3132029

[10] Lorrie Faith Cranor. 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *J. on Telecomm. & High Tech. L.* 10 (2012), 273.

[11] Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna. 2011. PiOS: Detecting Privacy Leaks in iOS Applications.. In *NDSS*. 177–183.

[12] Serge Egelman, Janice Tsai, Lorrie Faith Cranor, and Alessandro Acquisti. 2009. Timing is everything? The effects of timing and placement of online privacy indicators. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 319–328.

[13] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. 2020. Ask the Experts: What Should Be on an IoT Privacy and Security Label?. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE. https://doi.org/10.1109/sp40000.2020.00043

[14] Daniel Greene and Katie Shilton. 2017. Platform privacies: Governance, collaboration, and the different meanings of "privacy" in iOS and Android development. *New Media & Society* 20, 4 (apr 2017), 1640–1657. https://doi.org/10.1177/1461444817702397

[15] Irit Hadar, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. 2017. Privacy by designers: software developers' privacy mindset. *Empirical Software Engineering* 23, 1 (apr 2017), 259–289. https://doi.org/10.1007/s10664-017-9517-1

[16] Carlos Jensen and Colin Potts. 2004. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the 2004 conference on Human factors in computing systems - CHI '04*. ACM Press. https://doi.org/10.1145/985692.985752

[17] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. 2009. A "nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*. ACM Press. https://doi.org/10.1145/1572532.1572538

[18] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing privacy notices: an online study of the nutrition label approach. In *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*. ACM Press. https://doi.org/10.1145/1753326.1753561

[19] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. 2013. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. https://doi.org/10.1145/2470654.2466466

[20] Tianshi Li, Yuvraj Agarwal, and Jason I. Hong. 2018. Coconut: An IDE Plugin for Developing Privacy-Friendly Apps. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4 (dec 2018), 1–35. https://doi.org/10.1145/3287056

[21] Tianshi Li, Elizabeth Louie, Laura Dabbish, and Jason I. Hong. 2021. How Developers Talk About Personal Data and What It Means for User Privacy: A Case Study of a Developer Forum on Reddit. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (jan 2021), 1–28. https://doi.org/10.1145/3432919

[22] Tianshi Li, Elijah B. Neundorfer, Yuvraj Agarwal, and Jason I. Hong. 2021. Honeysuckle: Annotation-Guided Code Generation of In-App Privacy Notices. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 3 (sep 2021), 1–27. https://doi.org/10.1145/3478097

[23] Jialiu Lin, Norman Sadeh, Shahriyar Amini, Janne Lindqvist, Jason I. Hong, and Joy Zhang. 2012. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing - UbiComp '12*. ACM Press. https://doi.org/10.1145/2370216.2370290

[24] Aleecia M McDonald and Lorrie Faith Cranor. 2008. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* 4 (2008), 543.

[25] Aleecia M. McDonald, Robert W. Reeder, Patrick Gage Kelley, and Lorrie Faith Cranor. 2009. A comparative study of online privacy policies and formats. In *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09*. ACM Press. https://doi.org/10.1145/1572532.1572586

[26] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (nov 2019), 1–23. https://doi.org/10.1145/3359174

[27] Abraham H. Mhaidli, Yixin Zou, and Florian Schaub. 2019. "We Can't Live without Them!" App Developers' Adoption of Ad Networks and Their Considerations of Consumer Risks *(SOUPS'19)*. USENIX Association, USA, 225–244.

[28] Victor Morel and Raúl Pardo. 2020. SoK: Three Facets of Privacy Policies. In *Proceedings of the 19th Workshop on Privacy in the Electronic Society*. 41–56.

[29] Duc Cuong Nguyen, Dominik Wermke, Yasemin Acar, Michael Backes, Charles Weir, and Sascha Fahl. 2017. A Stitch in Time: Supporting Android Developers in WritingSecure Code. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM. https://doi.org/10.1145/3133956.3133977

[30] Johnny Saldaña. 2015. *The coding manual for qualitative researchers*. Sage.

[31] Florian Schaub, Rebecca Balebako, Adam L. Durity, and Lorrie Faith Cranor. [n.d.]. A Design Space for Effective Privacy Notices. In *The Cambridge Handbook of Consumer Privacy*. Cambridge University Press, 365–393. https://doi.org/10.1017/9781316831960.021

[32] Awanthika Senarath and Nalin A. G. Arachchilage. 2018. 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*. ACM. https://doi.org/10.1145/3210459.3210484

[33] Swapneel Sheth, Gail Kaiser, and Walid Maalej. 2014. Us and them: a study of privacy requirements across north america, asia, and europe. In *Proceedings of the 36th International Conference on Software Engineering*. ACM. https://doi.org/10.1145/2568225.2568244

[34] FTC Staff. 2011. Protecting Consumer Privacy in an Era of Rapid Change–A Proposed Framework for Businesses and Policymakers. *Journal of Privacy and Confidentiality* (jun 2011). https://doi.org/10.29012/jpc.v3i1.596

[35] Mohammad Tahaei, Tianshi Li, and Kami Vaniea. 2022. Understanding Privacy-Related Advice on Stack Overflow. In *Proceedings on Privacy Enhancing Technologies*. 1—-18. https://doi.org/10.2478/popets-2022-0032

[36] Mohammad Tahaei, Kami Vaniea, and Naomi Saphra. 2020. *Understanding Privacy-Related Questions on Stack Overflow*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3313831.3376768

[37] Sebastian Zimmeck, Rafael Goldstein, and David Baraka. 2021. PrivacyFlash Pro: Automating Privacy Policy Generation for Mobile Apps. In *Proceedings 2021 Network and Distributed System Security Symposium*. Internet Society. https://doi.org/10.14722/ndss.2021.24100

A PRE-SCREENING SURVEY

Our group in the Human Computer Interaction Institute at Carnegie Mellon University has been researching tools for software developers for many years. We are currently working on a 90-minute interview study for understanding the process of submitting apps to the Apple app store. The findings may also inspire us to design better developer tools to streamline this task.

This study was approved by the Institutional Review Board (IRB) at CMU. **We will not identify you, your app, or your organization** in any publications that come out of this research **without your written permission**.

To be eligible for this study, you must be 18 or older and have some experience in iOS app development. We will contact you if you are selected for the study. Thanks!

(1) Are you 18 or older?
- Yes
- No

(2) Approximately how many years have you been **coding** iOS apps?
- I don't have iOS develpoment experience
- less than a year
- 1-2 years
- 2-3 years
- 3-4 years
- 4-5 years
- more than 5 years

(3) When was the last time you participated in developing an app published in the Apple App store?
- I don't have apps published in the Apple App Store
- Within a month
- Within 6 months
- Within a year
- within 2 years
- More than 2 years ago

(4) Please submit Apple App Store links for the app(s) you worked on most recently.
- Most recent app (required for eligibility)
- 2nd most recent app
- 3rd most recent app

(5) Please check all types of data that you have collected via iOS apps.
- Financial Information
- User content
- Usage data
- Diagnostics
- Sensitive Information
- Contacts
- Browsing History
- Search History
- Purchases/Purchase History
- Health & Fitness
- Location
- Identifiers
- Other (please specify)
- None of the above

(6) What is your prolific ID?

Thanks for completing this pre-screening. We will contact you soon to let you know whether you have been selected for the 90-minute interview and associated $70 compensation. The next page will redirect you to Prolific.

B PRE-STUDY SURVEY

Thank you for agreeing to participate in this Carnegie Mellon study on the process of submitting apps to the Apple app store. We look forward to interviewing you.

For this interview study, we will ask you to report on one iOS app that we selected from your recent iOS apps. The selected app has been sent to you via the Prolific messaging system. If you are not sure which app to report on, please message us to ask.

In this pre-study survey, we would like to ask a few questions about you and the selected app. At the end of the survey, you will see a scheduling link where you can make a booking for our interview. After submitting the response, you will be redirected to the Prolific completion link.

(1) What is your participant ID for this study? (The ID was sent to you via the Prolific messaging system.)

(2) What is the app store link to the app that you will report on? (The selected app was sent to you via the Prolific messaging system.)

(3) How many times has this app been downloaded?
- Under 1,000
- 1,001 - 10,000
- 10,001 - 50,000
- 50,001 - 100,000
- 100,001 - 500,000
- 500,001 - 1,000,000
- 1,000,001 - 5,000,000
- 5,000,001 - 10,000,000
- 10,000,001 - 50,000,000
- 50,000,001 - 100,000,000
- 100,000,001 - 500,000,000
- Over 500 million

(4) Which option best describes this iOS app?
- Research project
- Course project
- Hobby Project
- Other

(5) If this iOS app is part of a commercial project, how many employees work in the company that developed this app?
- 1-4
- 5-9
- 10-19
- 20-49
- 50-99
- 100-249
- 250-499
- 500-999
- 1,000 or more

(6) Is this an individual-developed app or group-developed app?
- individual
- group

(7) Which of these roles describe your job for developing this app? (Please select all that apply)
- Backend developer
- Data Scientist and Analyst
- Designer
- Project Manager
- Security Engineer
- Privacy Engineer
- Quality Assurance Analyst
- Other Roles (please specify)

(8) Are you a professional Software Developer, i.e. software development is the major component of your job?
- Yes
- No

(9) Did you major in computer science or related fields in school?
- Yes
- No

(10) What is your gender?
- Man
- Woman
- Non-binary/third gender
- Prefer not to answer

(11) What is your age group?
- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65+
- Prefer not to answer

(12) Choose one or more races/ethnicities that you consider yourself to be:
- White
- Black or African American
- American Indian or Alaska Native
- Asian
- Native Hawaiian or Pacific Islander
- Hispanic/Latino
- Other (fill in the blank)
- Prefer not to answer

(13) In which country do you currently reside? (drop-down menu of countries from Qualtrics)

Thanks for completing the pre-study survey! Before submitting your response, please open this link in a new tab to schedule the interview: https://iosdeveloperstudy.youcanbook.me/

We would appreciate it if you could schedule earlier time slots (e.g., time slots in the first week). If none of the time slots works for you, please message us on Prolific and we will send you more options.

C MAIN SURVEY (USED DURING THE INTERVIEW)

C.1 Libraries

Please enter your participant ID

What libraries are used in this app? Here is a list of common types of third-party libraries and representative examples to help refresh your memory.

(1) Tools from Apple
- SKAdNetwork
- MapKit
- CloudKit
- App Analytics

(2) Multi-use libraries
- AppsFlyer
- Adjust
- Tenjin
- Firebase
- Facebook Audience Network
- Google AdMob: Mobile Ads SDK
- hyprmx SDK
- Yandex - AppMetrica

(3) Ad Networks
- AppLovin
- IAB Open Measurement SDK
- Integral Ad Science SDK
- Vungle
- unityADS
- AdColony
- Chartboost
- Start.io (formerly StartApp)
- Twitter MoPub
- Fyber
- PubNative

(4) Analytics
- MOAT
- Flurry
- Branch
- IronSource
- Google Analytics (now part of firebase)
- Crashlytics (now part of firebase)

(5) Social libraries
- Facebook SDK
- Twitter Kit
- Kakao
- VKontakte SDK
- Snapkit
- TikTok open SDK

(6) Billing
- PayPal SDK
- Stripe
- AliPay

(7) Gaming
- FMOD Ex
- Unity 3D
- Cocos2D-X

Please note any libraries you used that are not listed above. You are welcome to copy/paste the library list from your code if that is convenient.

Please return to the React App for the next set of questions.

C.2 Definitions

Randomization note: Participants saw the definitions of Data Collection, Data Categories/Types, Data Use (purposes), Linking, and Tracking in random order. Within categories there was additional randomization so one participant might see "Contact Info" first while a different would see "Location" first.

C.2.1 Data Collection. Please review Apple's definition of data collection:
"Collect" refers to transmitting data off the device in a way that allows you and/or your third-party partners to access it for a period longer than necessary to service the transmitted request in real time
Do you find this definition unclear, surprising, or unreasonable?

- Yes
- No

C.2.2 Data Categories/Types. (presented in random order)

(1) For **Contact Info**, Apple presents the following definitions. Do you find any of them confusing, surprising, and/or unreasonable? (Select 'yes' or 'no' for each item)
- **Name**: Such as first or last name
- **Email Address**: Including but not limited to a hashed email address
- **Phone Number**: Including but not limited to a hashed phone number
- **Physical address**: Such as home address, physical address, or mailing address
- **Other User Contact Info**: any other information that can be used to contact the user outside the app

(2) For **Health & Fitness**, Apple presents the following definitions. Do you find either of them confusing, surprising, and/or unreasonable? (Select 'yes' or 'no' for each item)
- **Health**: Health and medical data, including but not limited to data from the Clinical Health Records API, HealthKit API, MovementDisorderAPIs, or health-related human subject research or any other user provided health or medical data
- **Fitness**: Fitness and exercise data, including but not limited to the Motion and Fitness API

(3) For **Financial Info**, Apple presents the following definitions. Do you find any of them confusing, surprising, and/or unreasonable? (Select 'yes' or 'no' for each item)
- **Payment Info:** Such as form of payment, payment card number, or bank account number. If your app uses a payment service, the payment information is entered outside your app, and you as the developer never have access to the payment information, it is not collected and does not need to be disclosed.
- **Credit Info:** Such as credit score
- **Other Financial Info:** Such as salary, income, assets, debts, or any other financial information

(4) For **Location**, Apple presents the following definitions. Do you find either of them confusing, surprising, and/or unreasonable? (Select 'yes' or 'no' for each item)
- **Precise Location**: Information that describes the location of a user or device with the same or greater resolution as a latitude and longitude with three or more decimal places
- **Coarse Location:** Information that describes the location of a user or device with lower resolution than a latitude and longitude with three or more decimal places, such as Approximate Location Services

(5) For **Sensitive Info**, Apple presents the following definition. Do you find it confusing, surprising, and/or unreasonable? (Select 'yes' or 'no')
- **Sensitive Info**: Such as racial or ethnic data, sexual orientation, pregnancy or childbirth information, disability, religious or philosophical beliefs, trade union membership, political opinion, genetic information, or biometric data

(6) For **Contacts**, Apple presents the following definition. Do you find it confusing, surprising, and/or unreasonable? (Select 'yes' or 'no')
- **Contacts**: Such as a list of contacts in the user's phone, address book, or social graph

(7) For **User Content**, Apple presents the following definitions. Do you find any of them confusing, surprising, and/or unreasonable? (Select 'yes' or 'no' for each item)
- **Email or Text Messages**: Including subject line, sender, recipients, and contents of the email or message
- **Photos or Videos**: The user's photos or videos
- **Audio Data**: The user's voice or sound recordings
- **Gameplay Content**: Such as saved games, multiplayer matching or gameplay logic, or user-generated content in-game
- **Customer Support**: Data generated by the user during a customer support request
- **Other User Content**: Any other user-generated content

(8) For **Browsing History**, Apple presents the following definition. Do you find it confusing, surprising, and/or unreasonable? (Select 'yes' or 'no')
- **Browsing History**: Information about content the user has viewed that is not part of the app, such as websites

(9) For **Search History**, Apple presents the following definition. Do you find it confusing, surprising, and/or unreasonable? (Select 'yes' or 'no')
- **Search History**: Information about searches performed in the app

(10) For **Identifiers**, Apple presents the following definitions. Do you find either of them confusing, surprising, and/or unreasonable? (Select 'yes' or 'no' for each item)
- **User ID**: Such as screen name, handle, account ID, assigned user ID, customer number, or other user- or account-level ID that can be used to identify a particular user or account
- **Device ID**: Such as the device's advertising identifier, or other device-level ID

(11) For **Purchases**, Apple presents the following definition. Do you find it confusing, surprising, and/or unreasonable? (Select 'yes' or 'no')
- **Purchase History**: An account's or individual's purchases or purchase tendencies

(12) For **Usage Data**, Apple presents the following definitions. Do you find any of them confusing, surprising, and/or unreasonable? (Select 'yes' or 'no' for each item)
- **Product Interaction**: Such as app launches, taps, clicks, scrolling information, music listening data, video views, saved place in a game, video, or song, or other information about how the user interacts with the app
- **Advertising Data**: Such as information about the advertisements the user has seen
- **Other Usage Data**: Any other data about user activity in the app

(13) For **Diagnostics**, Apple presents the following definitions. Do you find any of them confusing, surprising, and/or unreasonable? (Select 'yes' or 'no' for each item)
- **Crash Data**: Such as crash logs
- **Performance Data**: Such as launch time, hang rate, or energy use
- **Other Diagnostic Data:** Any other data collected for the purposes of measuring technical diagnostics related to the app

(14) For **Other Data**, Apple presents the following definition. Do you find it confusing, surprising, and/or unreasonable? (Select 'yes' or 'no')
• **Other Data Types:** Any other data types not mentioned
Note: This was the only non-randomized data category was and always presented last

C.2.3 Data Use (purposes). Apple presents the following definitions for data uses (i.e. purposes). Do you find any of them confusing, surprising, and/or unreasonable? (Select 'yes' or 'no' for each item)

- **Third-Party Advertising**: Such as displaying third-party ads in your app, or sharing data with entities who display third-party ads
- **Developer's Advertising or Marketing**: Such as displaying first-party ads in your app, sending marketing communications directly to your users, or sharing data with entities who will display your ads
- **Analytics**: Using data to evaluate user behavior, including to understand the effectiveness of existing product features, plan new features, or measure audience size or characteristics
- **Product Personalization**: Customizing what the user sees, such as a list of recommended products, posts, or suggestions
- **App Functionality**: Such as to authenticate the user, enable features, prevent fraud, implement security measures, ensure server up-time, minimize app crashes, improve scalability and performance, or perform customer support
- **Other Purposes**: Any other purposes not listed

C.2.4 Linking. Please read Apple's definition below:
Data Linked to Users
Next, indicate if the data collected from this app is linked to the user's identity (via their account, device, or details).
Data collected from an app is usually linked to the user's identity via these means, unless specific privacy protections are put in place before collection to de-identify or anonymize it, such as:

- Stripping data of any direct identifiers, such as e-mail address or name, before collection.
- Manipulating data to break the linkage and prevent re-linkage to real-world identities. Additionally, in order for data not to be linked to a particular user's identity, you must avoid certain activities after collection:
  - You must not attempt to link the data back to the user's identity.
  - You must not tie the data to other datasets that enable it to be linked to the user's identity

Note: "Personal Information" and "Personal Data", as defined under relevant privacy laws, are considered linked to the user
Linking question 1: Do you find this definition unclear, surprising, or unreasonable?

- Yes
- No

Linking question 2 (on a separate page): In this example data table (assuming there were more rows, shown in Figure 3), which data would you consider linked to users, if any? Please explain your reasoning.

- User ID
- Phone Number
- Date of last login

	A	B	C
1	**User ID**	**Phone number**	**Date of last login**
2	a1asdfasdfaser21245df3	111-111-1111	7/27/21
3	as34sdim39bnas84mgi	222-222-2222	7/27/21
4	s28end83nbm38505n1	333-333-3333	7/7/21
5	a3mbit6hmasdg93hm	444-444-4444	7/8/21

Figure 3: Example data used to ask respondents whether they thought each field would be linked to users.

C.2.5 Tracking. Please read Apple's definition below:
Data used to track users:
Tracking
Tracking is linking data collected from your app about a particular end-user or device such as a user ID, device ID, or profile, with Third-Party Data for targeted advertising or advertising measurement purposes. It also refers to sharing data collected from your app about a particular end-user or device with a data broker.
Tracking does not apply in the following situations:

- When the data is linked solely on the end-user's device and is not sent off the device in a way that can identify the end-user or device
- When the data broker uses the data shared with them solely for fraud detection or prevention or security purposes
- When the data broker is a consumer reporting agency and the data is shared with them for purposes of (1) reporting on a consumer's creditworthiness, or (2) obtaining information on a consumer's creditworthiness for the specific purpose of making a credit determination.

Third-Party Data
Third-Party Data is any data about a particular end-user or device collected from the apps, websites, or offline properties not owned by the developer.
Examples
To help put tracking into context, here are a few examples:

- Displaying targeted advertisements in your app based on user data collected from apps and websites owned by other companies
- Sharing device location data or email lists with a data broker
- Sharing a list of emails, advertising IDs, or other IDs with a third-party advertising network that uses that information to retarget those users in other developers' apps or to find similar users
- Placing a third-party SDK in your app that combines user data from your app with user data from other developers' apps to target advertising or measure advertising efficiency, even if you don't use the SDK for these purposes. For example, using a login SDK that repurposes the data it collects from your app to enable targeted advertising in other developers' apps.

If you plan to request access to the advertising identifier (IDFA), you must indicate on your App Store privacy label that you collect Device IDs and use them for tracking purposes.

Question Do you find this definition unclear, surprising, or unreasonable?

- Yes
- No

C.3 Personal Data & Linking

Under the definition of linked data, there is a note:

Note: "Personal Information" and "Personal Data", as defined under relevant privacy laws, are considered linked to the user.

Which of these data categories (if any) do you think privacy laws would define as personal and therefore automatically linked, given where your potential app users live? **Note**: These showed up in random order.

- Crash Data
- Performance Data
- Other Diagnostic Data
- Product Interaction
- Advertising Data
- Other Usage Data
- Purchase History
- User ID
- Device ID
- Search History
- Browsing History
- Emails or Text Messages
- Photos or Videos
- Audio Data
- Gameplay Content
- Customer Support
- Other User Content
- Contacts
- Sensitive Info
- Coarse Location
- Precise Location
- Payment Info
- Credit Info
- Other Financial Info
- Health
- Fitness
- Name
- Email Address
- Phone Number
- Physical Address
- Other User Contact Info
- Other Data Types

D INTERVIEW SCRIPT

D.0.1 Introduction. Thanks for agreeing to participate in our study. First, I need to read our standard introduction, as required by our study protocol.

Our group at Carnegie Mellon University has been doing research for many years on tools for developers. We are currently working on a research project about the iOS privacy labels, which is a new feature of the iOS app store that shows details of iOS apps to end users. iOS developers are now required to provide the privacy details for their apps by answering certain questions about data collection, use, and whether users are being tracked. The general goal of our research is to learn about how iOS developers accomplish this task, how they perceive the concepts used to describe data practices, and what barriers there are for correctly and efficiently accomplishing this task. The findings may also inspire us to design better developer tools to streamline this task.

We understand that you have published an app named [the app name] on the iOS app store. We would like to interview you about the process of submitting apps to the app store and have you complete some tasks about that app on our website. We expect the entire study session to take approximately 90 minutes, though timing may vary depending on the complexity of the app. During the study, we will ask you to answer some questions about your app's data practices using a website built by our group that implements the privacy label questionnaire from the official Apple developer website. Then we will ask you some follow-up questions regarding why you selected certain options, how you perceive certain concepts, and whether you encountered any difficulty during the process. Since we want to observe how you completed this task, we would like you to share your screen during the interview. We need to record both the audio and the screen during the entire interview solely for analysis purposes. We will use Zoom to make the recordings. Only researchers in our group working on this project will have access to the recordings. The interviews will be transcribed automatically by Zoom and we may include parts of the transcripts in our research papers that do not identify you, your app, or your organization.

Your participation is entirely voluntary and you may quit the study at any time. If you don't feel comfortable answering a question, feel free to skip it and it will not affect your compensation. You must be 18 or older to participate in this study. You will be compensated $70 for participating. The interview will be conducted remotely through the computer. Since the interview will be recorded, it is important that you be in a private room, and not in an open-space cubicle, for example. These recordings may be stored on protected computers at CMU and on Zoom, with transcripts potentially edited using a service called Otter. There are no expected risks or benefits to you for participating, beyond the benefits of helping improve the understanding of privacy labels in general.

This study was approved by the Institutional Review Board (IRB) at CMU. We will not identify you, your app, or your organization in any publications that come out of this research without your written permission.

Is that all OK? If yes, please sign the consent form (digitally). Is it OK if I record the interview? [Start recording after receiving their positive answer]

D.0.2 Observation of Answering Privacy Questions About the App. In the first part, we'll ask you to use an interface that imitates Apple's developer website. There, you'll answer questions about if and how your app [the app name] uses data.

Please handle this task as you normally would and take as long as you need. You are welcome to look at any documentation you would normally consult, except for the app's privacy label. In order for us to see any resources you use, please either share your full

screen or open any additional resources in the same window where you're completing the task.

If you need a resource that is not currently available or would ordinarily ask somebody for help, please say aloud what resources you would use and who you would usually contact.

I won't be able to answer questions during the task but please voice any areas of confusion, and we'll answer them to the best of our ability at the end of this interview.

I will put the website in the chat now. Your participant ID is [participant ID]. Please start sharing your screen as soon as the website is open. Do you have any questions?

allow time for filling it out

Thanks so much! We'll now delve into some more questions about your process. You are welcome to change your answers at any time. As a reminder, we're not measuring your performance and will not include any information about you, your app, or your organization in our publications. The goal of this study is to understand developer perspectives on using the Apple interface for filling out privacy labels. We're also interested in tools to improve the accuracy. It's actually helpful if you point out and fix any inaccuracies during the rest of this interview, since that will help us understand sources of inaccuracies in the labels.

D.0.3 Libraries. What libraries are used in this app? Here is a list of common types of third-party libraries and representative examples to help refresh your memory.

Direct participants to the Qualtrics survey

How did you figure out the data practices of the libraries you use?

D.0.4 Explanation of Answers. For each block, will you help us understand how you filled it out based on the following questions?

- Which 3rd party library collects this data, or is it just collected by you?
- If you collect this data manually, where is this data stored? Examples include on the user's device, a database you built, or via a database service like Firebase.
- How did you select these data uses (i.e. purposes)?
- How did you determine whether the data is linked to the user's identity?
- How did you determine whether the data is used for tracking purposes?

D.0.5 Definitions and Follow-up Questions. In the next section, we would like to examine some key concepts that were used in Apple's privacy label. We are curious about what they mean to you, and whether any part of Apple's definition looks surprising, unclear, or unreasonable to you. By identifying both matches and mismatches between developers' understanding and Apple's definitions of these concepts, we hope to gain a better understanding of what may cause difficulty in filling out the privacy label and also help you improve the accuracy of privacy labels. Please let us know if anything surprises you or does not make sense to you, even if it's just a tiny part of the definition. Alternatively, if there are definitions or parts that are defined very clearly and/or in line with your previous understanding, that's good to know too. We'll ask you to keep screen-sharing the Qualtrics survey.

Note: This part will be facilitated by the Qualtrics survey with a verbal component (full version in Appendix C). The structure is below.

Process for Discussing Definitions

- Show Apple Definition
- For each definition, ask whether they find it unclear, surprising, and/or unreasonable
- Ask follow-up questions about whatever they flag
- If they express a change in understanding, ask if it would change how they fill out the label

Definitions in the Survey

- Data Collection (1 definition)
- Data Categories/Types (14 categories such as "Contact info" and 32 types such as "Name" or "Email Address")
- Data use (6 definitions)
- Linking (1 definition w/ 1 follow-up question)
- Tracking (1 definition)

Personal Data & Linking

For the final task in the survey, when developers are selecting which items they consider "personal data", ask them which laws - if any - are informing how they answer the question.

D.0.6 How developers fill out the labels in real life. The next section focuses on learning more about how your app was created and understanding your perspective as a developer.

- Teamwork and Collaboration
  - Have you filled out an Apple privacy label before?
  - If yes:
    - Was it for this app?
    - How long ago did you fill it out?
    - Approximately how long did it take you?
  - Which parts of the app, if any, were implemented by other members of your team?
    - For these parts, how did you figure out the corresponding data practices and select the option to describe them?
  - If their app has already provided a privacy policy and it's a group app: Which team member created the privacy policy, and was it discussed among multiple team members?
  - If their app has already provided a privacy label and it's a group app: We're curious to learn more about the process of filling this out in real life. Which team member filled in the privacy label questionnaire, and was it discussed among multiple team members?
  - Given that the questions are the same, was the experience of filling out this form in real life different from doing this task in today's study?
    - Are there any challenges that you have encountered when filling out this form in real life but were not covered in this study?
- Monetization
  - How is your app monetized, if at all?
  - Did it affect how you answered these questions?
- Privacy-enhancing design or technologies
  - Did you use any approaches to protect the data privacy of your app?
    - Did they affect how you answered these questions?

- Data collected for future use
  - Is filling out the label information a one-time task, or do you expect to edit it over time?
  - If editing over time: how often do you anticipate editing it?

D.0.7 Compare with the privacy label on the App Store. Now we would like to compare the privacy label you just provided with the privacy label of your app on the App Store. We're anticipating there may be some discrepancies. The goal of this study is not to measure your ability, and discussing these discrepancies will help us identify challenges developers may encounter when handling this task so please don't be shy in noting any inaccuracies in either label. Your perspective is really helpful, and no identifying information will be shared about you, your app, or your company, in our report.

(If there are any discrepancies between the two privacy labels) What do you think could possibly cause the difference between the two privacy labels?

D.0.8 How developers think about privacy labels and Apple's tool for filling out the privacy label. As a concluding task, we'd like to ask some big-picture questions about privacy label interface.

- What do you think are positive and negative aspects of having a privacy label from a developer's perspective?
- Do you use iOS products, such as an iphone or ipad, that offer these labels?
  - If yes: how do the labels influence your decisions, if at all
  - If no:
    - Would you like your phone or tablet to offer these labels for your apps?
    - How do you think the labels might influence your decisions, if at all?
- If you could improve Apple's implementation of privacy labels in any way, how would you do it?
- What do you think are the strengths and weaknesses of the design of the web-based tool that Apple provides (and we replicated) for this task?
- Are there any other tools or features that you wish to have to help you with this task?

That's everything for our study today! Could you click the "submit logs" button to submit the results? Also, do you have any questions for us?

E CODEBOOK

Theme	Code	Memo
Underreporting	Missing third-party data use	The developer did not properly report all third-party data use in their privacy label (including both third-party libraries and services)
	Missing linked data	The developer only considered personally identifiable data as linked to users.
	Missing data types	The developer did not properly report all data types in their privacy label.
	Missing interaction outside the app	Developers did not report data use outside of the app (e.g., sending newsletters) in the privacy label, which implies that they didn't consider data use outside of the app as part of the data use of the app.
	Missing optional data practices	The developer did not report certain data practices because they are optional.
Overreporting	Overreporting tracking	The developer overgeneralized the definition of tracking to scenarios outside Apple's definitions (i.e., third-party advertising or sharing with data brokers).
	Reporting unstored data	The developer reported data that was not stored as being collected.
	Reporting Apple SDK data collection	Data solely collected by Apple doesn't need to be reported, but developers may not understand this scope limitation. This can apply to gaming, payment, and analytics, along with libraries like Map Kit.
Other errors	Got link and tracking mixed up	The developers confused the meaning of *data linked to users* with *data used to track users*
Unknown unknowns	Knowledge blindspot	Developers were not aware of privacy label requirements or related resources
	Blinded by preconceptions	Clearly defined in Apple's documentation, but the developer did not check them carefully enough or completely missed them and interpreted the terms using their previous understanding
	Misinterpretation of definition	The developer had a wrong understanding of Apple's definition even after being asked to read it and answer questions about it.

Known unknowns	Limitations of the official content	The developer discussed perceived limitations of the official developer tool and documentation.
	Lacking support	The developer did not know certain data practices due to the lack of support from their collaborators.
Complexity	Overwhelming (or time-consuming)	This tag can be used when participants either express that the task is time-consuming in real life, reference how it was time-consuming in the study, or show other evidence that limitations on time are a barrier to filling out the labels either accurately or at all. This can also include information overload.
	Workplace	The developer mentioned obstacles to creating privacy labels in the workplace, e.g., they rarely received privacy-related requests (e.g., adding a privacy label, checking about data practices when drafting a privacy policy) internally from their team/manager/company/client.
	Cross-platform	The developer mentioned their app was made as a cross-platform app for iOS and Android and/or compares the two platforms.
	Memory challenges	When the developer has trouble remembering something about their app or the Apple definitions. This also includes when the developer has seen the definition but didn't realize they'd seen it.
Perceptions from users' perspectives	Privacy label is beneficial	Developers thought about users' experiences and considered privacy labels beneficial to them and correspondingly also beneficial to developers.
	Err on caution	When the developer indicates there may be false positives on the label because of wanting to be cautious.
	Users' distrust	The developer expressed concerns about users' distrust in the privacy label.
Perceptions from devs' perspectives	Difficult extra work	The developer expressed negative feelings about privacy labels because it required extra work and filling out privacy labels was perceived a difficult task.
	Bonus for apps collecting less data	The developer considered introducing privacy labels gave bonus to developers who collected less data
	Dev unconcerned with privacy	The developer mentioned they had never thought deeply about privacy in practice or considered privacy not their responsibilities
	Chance to reflect on data practices	The developer appreciated the fact that filling out privacy labels gave them an opportunity to reflect on how the collected and used data and get a better understanding of their data practices.