USENIX

THE ADVANCED COMPUTING
SYSTEMS ASSOCIATION

User Understandings of Technical Terms in App Privacy Labels

Ishika Keswani, Kerick Walker, Adrian Clement, Eusila Kitur, Nannapas Wonghirundacha, Ryan Aubrey, Vivien Song, and Eleanor Birrell, *Pomona College*

https://www.usenix.org/conference/soups2025/presentation/keswani

This paper is included in the Proceedings of the Twenty-First Symposium on Usable Privacy and Security.

August 11–12, 2025 • Seattle, WA, USA

ISBN 978-1-939133-51-9

Open access to the Proceedings of the Twenty-First Symposium on Usable Privacy and Security is sponsored by USENIX.

User Understandings of Technical Terms in App Privacy Labels

Ishika Keswani
Pomona College

Kerick Walker
Pomona College

Adrian Clement
Pomona College

Eusila Kitur
Pomona College

Nannapas Wonghirundacha
Pomona College

Ryan Aubrey
Pomona College

Vivien Song
Pomona College

Eleanor Birrell
Pomona College

Abstract

Privacy labels are concise, standardized representations of privacy policies that are required for apps on both the iOS and Android app stores. However, prior research shows that users find current app privacy labels confusing and are unable to correctly identify data practices based on these labels. This work explores how understandings of technical terms impact comprehension of app privacy labels. We conduct a pair of online user studies—a qualitative user study ($n = 46$) and a large-scale quantitative study ($n = 383$) in which we identify terms used in privacy labels that are widely misunderstood and explore common misunderstandings. We also formulate evidence-based recommendations for how to improve app privacy labels.

1 Introduction

Mobile apps collect a multitude of data. While some of this data is necessary to support core app functionality, much of this data—including location and interactions with an app—is personal information with potential privacy implications. There is a growing consensus, now legally enforced under privacy and data protection regulations such as the E.U.'s GDPR and California's CCPA, that people have a right to transparency about what personal information is collected and how this personal information is used.

Historically, the primary mechanism for providing transparency about data practices was privacy policies. However, twenty years of research has conclusively demonstrated that privacy policies are too long [1, 2, 10, 28, 29], use complex [2, 3, 10, 13, 15, 24] and ambiguous [6, 16, 30] language, and use technical terms that are commonly misunderstood [31, 39]. Consequently, users struggle to understand data practices based on a privacy policy [33, 35, 37, 40].

Privacy labels—sometimes called *privacy nutrition labels*—are concise, standardized representations of data practices. Research has suggested that privacy labels might be a more effective means of providing transparency about data practices compared to natural-language privacy policies [7–9, 18–20, 44], and both Apple and Google mandate privacy labels for all apps listed on their app stores. However, preliminary research shows that users find current app privacy labels confusing and are unable to correctly identify data practices based on these labels [5, 23, 27, 43]. That research suggests two possible reasons that current implementations of app privacy labels have failed to realize the predicted transparency enhancement: (1) labels may use terminology that users do not understand or correctly interpret and (2) labels may include design elements that make it challenging for users to locate or identify relevant information.

This work evaluates the former hypothesis. Through a pair of surveys, we investigate how users understand technical terms that appear in privacy policies, we explore the potential impact of common misunderstandings and miscomprehensions, and we identify ways to improve current privacy labels with more intuitive terminology.

We start by conducting a qualitative user study ($n = 46$) to explore how users understand technical terms used in iOS and Android privacy labels. We include all four classes of technical terms that appear in app privacy labels—data collection categories, data type categories, specific data types, and purposes—and we include all terms in each category for each label design (55 iOS terms and 61 Android terms). We collect a rich, qualitative dataset about how people interpret these terms. We then qualitatively code user responses for correctness and identify 34 terms that are widely misunderstood or misinterpreted.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2025.
August 10–12, 2025, Seattle, WA, United States.

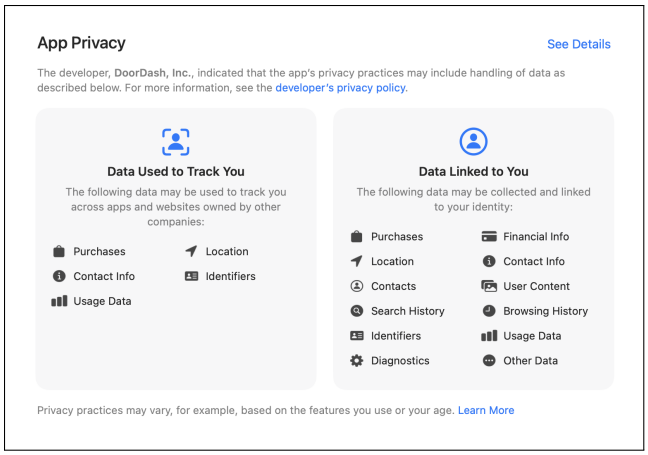


Figure 1: Concise iOS App Privacy Label

We then conduct a large-scale online survey ($n = 383$) in which we ask participants to define various widely misunderstood terms on a multiple-choice survey. For this large-scale survey, the correct response was drawn from the developer documentation [4, 12] and incorrect responses were based on our thematic analysis of the qualitative responses. Our results validate that many users misunderstand these terms and quantify the prevalence of common misinterpretations.

Based on our results, we formulate concrete recommendations for how app stores can improve the design of future app privacy labels.

2 Background: App Privacy Labels

Privacy labels—sometimes called *privacy nutrition labels*—are concise, standardized representations of privacy practices. Apple introduced mandatory privacy labels—called App Privacy Labels—for iOS apps in December 2020, and Google introduced mandatory privacy labels—called Data Safety Labels—for Android apps sold through its play store in July 2022.

Both the iOS and Android privacy labels are intended to enhance transparency about app data practices, including what information is collected and shared and the purpose of each data practice. Both types of label also specify both a concise format—displayed on the app store page for each app—and an expanded format—which provides many more details about data practices and purposes, accessible through a link from the concise label. However the details of the label designs differ.

iOS privacy labels divide data collection into three groups: *Data Used to Track You*, *Data Linked to You*, and *Data Not Linked to You*. The concise label displays which categories of data types are collected within each group (e.g., Figure 1). The expanded label shows all the purposes for which data is collected within each group (with precise data types listed under each purpose), organized by data type category. An excerpt from an expanded iOS label is shown in Figure 2.

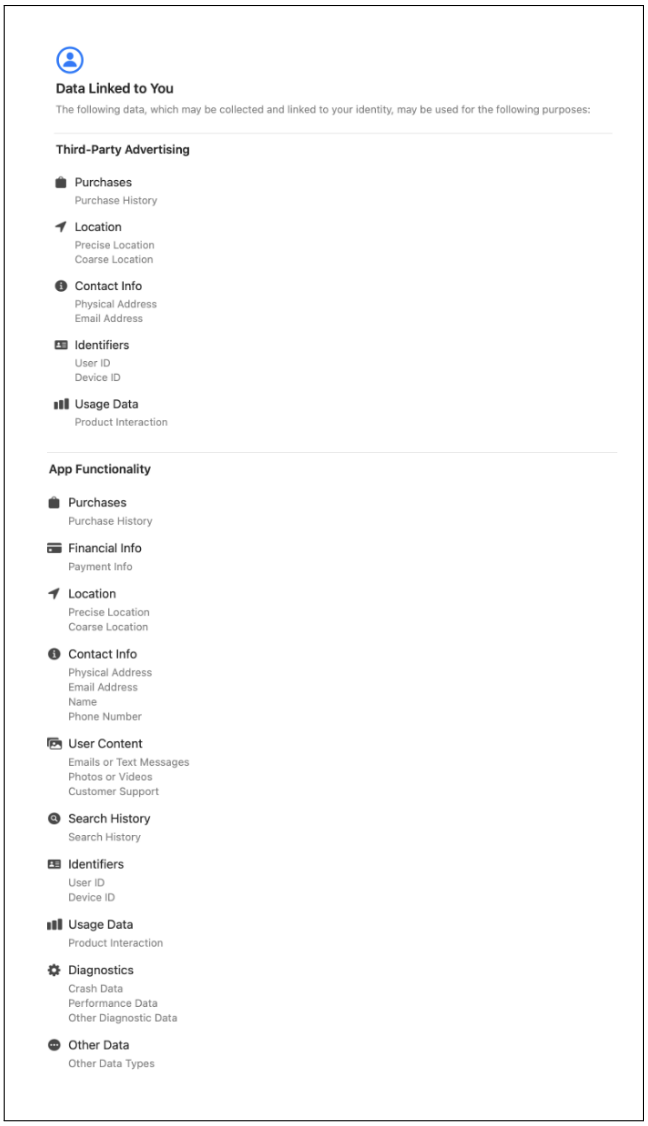


Figure 2: Expanded iOS App Privacy Label (Excerpt)

Android privacy labels divide data collection into two groups: *Data Shared* and *Data Collected*. The concise label displays examples of data type categories within each group (e.g., Figure 3); it also displays whether the app encrypts data in transit and whether data can be deleted. The expanded Android privacy label shows all of the precise data types within each group (organized by data type category); each data type category can be expanded on-click to show the purposes for which each precise data type is collected or shared. An excerpt from an expanded Android label is shown in Figure 4.

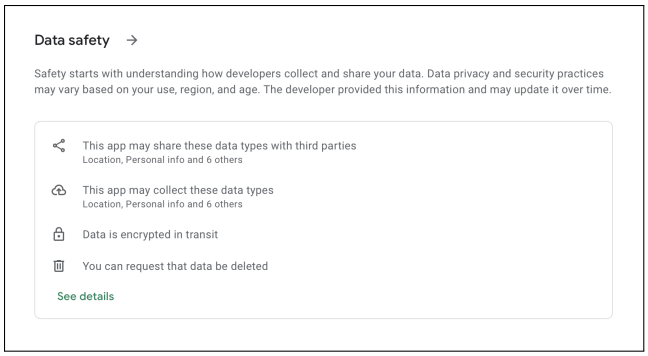


Figure 3: Concise Android Data Safety Label

3 Related Work

This work builds on three lines of prior work, which respectively investigated understandings of technical terminology in various contexts, explored the general transparency of app privacy labels, and measured various aspects of app privacy label implementations.

Understandings of Technical Terms. Balash et al. [5] empirically evaluated how confident users are in their understandings of technical terms that appear in concise iOS App Privacy Labels. They found that users are confident in their understanding of all data collection groups and all but five data type categories. The five data type categories in which fewer than 70% of user claimed to be at least somewhat confident were: *Diagnostics*, *Identifiers*, *Sensitive Info*, *User Content*, and *Other Data*. Our work complements their results by evaluating whether users actually understand these terms and by extending the scope to include precise data types, purposes, and terms that appear in Android Data Safety Labels.

Prior work has also evaluated user understandings of technical terms in various other contexts. Felt et al. [11] evaluated user comprehension of mobile app permissions in 2012; they found that users answered 21% of permission comprehension questions correctly, and just 2.6% of respondents answered all three questions correctly. Many users could not connect the resource-specific technical terms used in permission names to particular risks that would be enabled by those permissions. However, their work focused exclusively on terms used to describe Android permissions at the time, which is not the same language used in app privacy labels today. Habib et al. [14] looked at technical terms used in cookie banners. They found that less than half of participants could correctly define *performance cookies* and only 16% could define *functional cookies*. Tang et al. [39] conducted a large-scale quantitative evaluation of user understandings of 22 technical terms that commonly appear in privacy policies. They identified commonly misunderstood and poorly understood terms, such as *web beacon*, *local storage*, and *persistent cookies*, and demonstrated that misunderstandings significantly impact comfort with described data practices. However, their work focused on technical terms drawn from privacy policies, which are not the same terms used in app privacy labels. In follow-up work, Moremen et al. [31] conducted focus groups exploring generational differences in comprehension of technical terms; however, their study also focused exclusively on terms drawn from privacy policies.

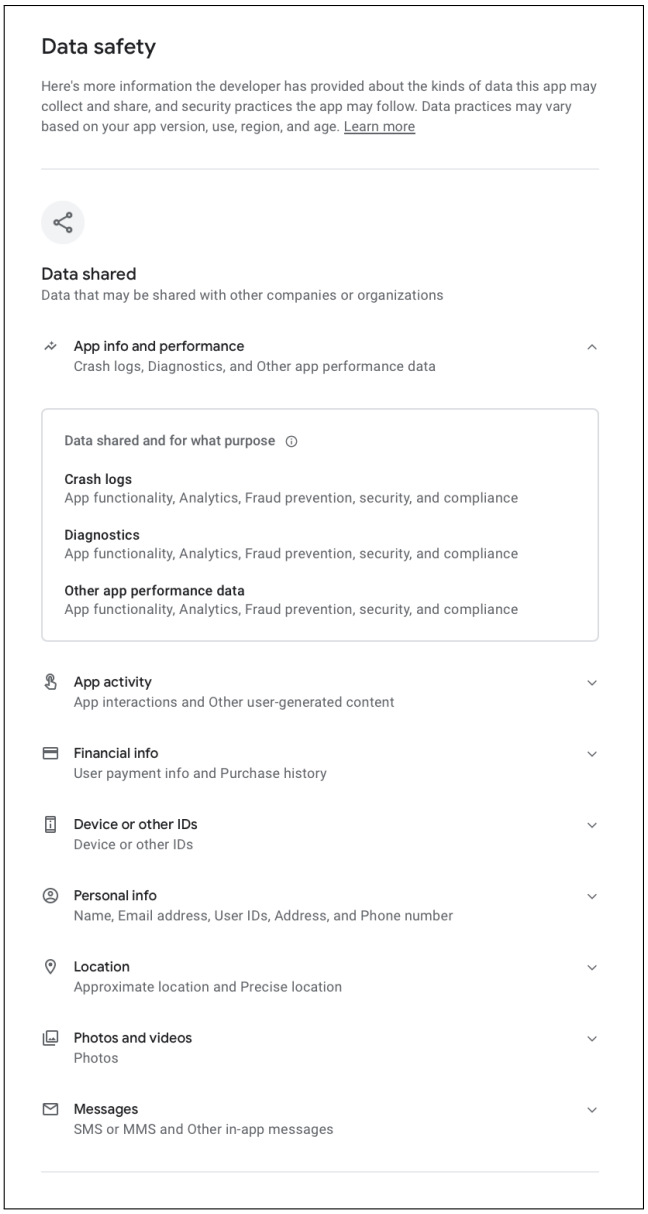


Figure 4: Expanded Android Data Safety Label (Excerpt)

Other work has considered comprehension of specific technical terms. For example, a 2005 study about the online shopping behavior of American consumers found that 75% falsely believed that a *privacy policy* meant that a website

would not share their information with other websites or companies [40]. More recent [36] and longitudinal [41] work showed that this misconception persists. Prior work evaluating app privacy labels more broadly found that users didn't understand the term *Data Used to Track You* [27,43], used in iOS App Privacy labels. However, this work didn't evaluate understandings of technical terms more broadly.

Evaluating Privacy Labels. Prior work has also conducted user studies to evaluate iOS and Android app labels more generally.

Zhang et al. [45] explored the utility of iOS App Privacy Labels by evaluating whether these labels disclose the information that users most want to know. By conducting a thematic analysis of privacy related questions independently generated by mobile app users, they found that privacy labels do not provide answers to these questions in totality.

Zhang et al. [43] conducted a user study of 24 lay iPhone users to learn how they interact with and interpret iOS App Privacy Labels. They found that few users were aware of these privacy labels and that users assumed labels were produced or validated by Apple. They also identified misconceptions relating to both structural design and disclosure requirements imposed by the labels. Many of the users they interviewed found iOS App Privacy Labels vague and confusing. However, while they observed that certain terms in app labels were misunderstood, they did not systematically evaluate term comprehension, they focused exclusively on iOS privacy labels, and the small scale of their study limits generalizability.

Lin et al. [27] conducted an interview study comparing the usability of iOS and Android privacy labels. They found that both designs exhibited usability challenges, both due to shared aspects and to design features unique to each design. However, while they observed that certain terms in app labels were misunderstood, they did not systematically evaluate comprehension term comprehension, and the small scale of their study limits generalizability.

Balash et al. [5] conducted a large-scale experimental study in which they evaluated which app privacy label features affect users' willingness to install an app. They found that iOS App Privacy Labels did impact risk perception and willingness to install, and they found that collecting *Sensitive Info*, *Financial Info*, or *Browsing History* or using *Financial Info*, *Sensitive Info*, or *Other Data* to track had the most significant (negative) impact on users' willingness to install an app.

Measuring App Privacy Labels. Koch et al. [22] conducted a statistical analysis of 11,074 iOS app available on the German app store in November 2021. They noted inconsistencies within app privacy labels—for example labels that claimed to collect data that inherently identified a user, such as *User ID*, in the *Data Not Linked to You* group. They also found that 48.9% of apps analyzed did not have a privacy label.

Additionally, several independent projects have evaluated the accuracy of app privacy labels. This work has found discrepancies between app labels and privacy policies [17, 32, 34] and between app labels and actual data practices [22, 23, 26, 42]. A developer interview study suggests that some inaccuracies may be caused by developer misconceptions about app privacy labels [25].

4 Methodology

The core of this work is comprised of a pair of user studies: (1) a qualitative user study ($n = 46$) exploring understandings of all 116 technical terms used in iOS and Android app privacy labels and (2) a quantitative follow-up study ($n = 383$) quantifying understandings and misinterpretations of 27 technical terms identified as poorly understood based on qualitative coding of free-response definitions from the qualitative study.

4.1 Qualitative Study

To explore how people interpret technical terms that appear in app privacy labels, we conducted a qualitative online survey ($n = 46$) with iOS and Android users recruited through Prolific.

Term Selection. We observed that both iOS App Privacy Labels and Android Data Safety Labels contain four types of terms: (1) data collection groups, (2) data type categories, (3) precise data types, and (4) purposes. iOS labels have 3 data collection groups, 14 data type categories, 32 precise data types, and 6 data types, for a total of 55 terms (shown in Table 1a). Android labels have 2 data collection groups, 14 data type categories, 38 precise data types, and 7 purposes, for a total of 61 terms (shown in Table 1b). For our qualitative survey, we used all terms that appear in either privacy label.

Survey Design. We split our qualitative study into two surveys: one that focused on the 55 iOS terms and one the focused on the 61 Android terms. For each survey, we tailored the type of question to the type of term, and we piloted our survey with three convenience-sample cognitive interviews.

For data collection group terms, precise data types, and purposes, we asked participants to define the term in their own words. Since the definitions of data collection groups include a variety of nuanced corner cases—for example, Android does not consider data to be *collected* if it is only stored locally on the user's device—we also asked follow-up, multiple choice questions designed to explore whether participants understood the nuances and corner cases in how data collection groups are defined. For data type categories, we wanted to learn how well people understood which precise data types were included in that category (since concise privacy labels show only data type categories, not precise data types). We therefore used

Data Collection Groups (3)
**Data Type Categories* (14)
Browsing History
Contact Info
Contacts
Diagnostics
Financial Info
Health & Fitness
Identifiers
Location
Purchases
Search History
Sensitive Info
Usage Data
User Content
Other Data

Purposes (6)
Analytics
**App Functionality*
**Developer's Advertising or Marketing*
Product Personalization
Third-Party Advertising
**Other Purposes*

Data Collection Groups (2)
Data Collected
Data Shared

Precise Data Types (38)
Address
**App Interactions*
Approximate Location
Calendar Events
Contacts
Crash Logs
Credit Score
Device or Other IDs
**Diagnostics*
Email Address
Emails
Fitness Info
Health Info
In-app Search History
Installed Apps
Music Files
Name
Phone Number
Photos
Political or Religious Beliefs
Precise Location
Purchase History
Race and Ethnicity
Sexual Orientation
SMS or MMS
User IDs
User Payment Info
Videos
Voice or Sound Recordings
Web Browsing History
**Other Actions*
**Other App Performance Data*
Other Audio Files
Other In-app Messages
Other Financial Info
**Other Info*
Other User-Generated Content

Data Type Categories (14)
App Activity
App Info and Performance
Audio
Calendar
Contacts
Device or Other IDs
Files and Docs
Financial Info
Health and Fitness
Location
Messages
Personal Info
Photos and Videos
Web Browsing

Purposes (7)
**Account Management*
Advertising or Marketing
Analytics
App Functionality
**Developer Communications*
Fraud Prevention, Security, and Compliance
Personalization

(a) The 55 Terms used in iOS App Privacy Labels

(b) The 61 Terms used in Android Data Safety Labels

Table 1: Technical Terms in Privacy Labels. Terms that are not widely understood are shown in italics.

drag-and-drop question that asked users to map each precise data type to the data type category they believed includes that precise data type.

Our survey concluded with questions about self-perceived privacy attitudes and awareness, smartphone use, and demographic information.

The full set of survey questions for both the iOS and Android versions of our qualitative survey are provided in Appendices A and B.

Analysis Plan. We tailored our analysis plan to the three different types of questions: open-ended definitions, follow-up multiple-choice questions about data collection groups, and drag-and-drop questions about data type categories.

Term	Dev. Doc. Definition	Correct	Part. Correct	Restates	I Don't Know	Wrong
Performance Data	Such as launch time, hang rate, or energy use	*How fast and efficient your device does something on the app*	*speed*	*data on device performance*	*dont know*	*How long I use certain sites and apps*
Account Management	Used for the setup or management of your account with the developer.	*Making sure your account is secure and you are the one using it, making sure your information is current and correct*	*perhaps making sure you are not sharing your account with anyone else*	*It means to manage my account*	*I'm not sure*	*to keep track of areas where app is used*

Table 2: Examples of how qualitative responses defining technical terms were coded for correctness.

To analyze open-ended definitions, we deductively coded each user definition using a five-point scale: (1) Correct, (2) Partially Correct, (3) Restates the term, (4) I Don't Know, and (5) Wrong. Correctness was evaluated based on the definition provided in the relevant developer documentation [4, 12]. Examples of how specific responses were coded for correctness are given in Table 2. We defined a term as *widely understood* if at least 2/3 of participant responses were coded as Correct or Partially Correct. We also thematically coded incorrect responses to identify common misinterpretations and misconceptions. Each term was independently coded by two authors. Terms on which the two codings disagreed were re-visited by two additional authors who made a consensus decision about the final code.

For the follow-up multiple-choice questions about data collection groups, we conducted a frequency analysis of users' selection for the options in each category.

For the drag-and-drop questions about data type categories, we calculated each participant's recall and precision scores for classifying precise data types into each data type category. We defined a term as widely understood if at least 2/3 of users had an F1 score above .66. Additionally, we recorded descriptive statistics about how frequently each precise data type was mis-classified.

Participant Recruitment. We recruited 25 iOS users and 25 Android users through Prolific. Participation was constrained to U.S. residents with either an iOS or Android device, a minimum of 20 prior submissions, and a minimum 90% approval rate on Prolific. iOS users were surveyed about their interpretation of terms that appear in iOS App Privacy Labels and Android users were surveyed about terms that appear in Android Data Safety Labels. One iOS response and three Android responses were omitted after a manual analysis indicated that the responses were likely AI-generated. Our final dataset was therefore comprised of 46 responses: 24 from iOS users and 22 from Android users. The demographics of our user study population are summarized in Table 3.

Demographic		Qua1.	Quant.	U.S.
Age	18-24	23.9%	12.0%	12.0%
	25-34	19.6%	18.8%	17.3%
	35-44	32.6%	17.0%	16.9%
	45-59	17.4%	29.0%	23.4%
	60-74	6.5%	20.3%	21.2%
	75+	0.0%	2.9%	9.2%
Race	White	71.7%	67.9%	60.9%
	Black	13.0%	12.5%	12.2%
	Asian	6.5%	6.5%	5.9%
	Native Am.	0.0%	1.6%	0.3%
	Other	8.7%	10.2%	19.8%
Gender	Male	50.0%	47.5%	49.1%
	Female	43.5%	50.7%	50.9%
	Non-binary	4.4%	1.0%	-
	Self-describe	2.1%	0.8%	-

Table 3: User study demographics compared to the demographics of the United States, as published in the American Community Survey (ACS).

4.2 Quantitative Follow-up Study

Prior work on privacy labels has primarily focused on small-scale qualitative interviews which inherently preclude generalizability. To generate generalizable insights about under-

standings and miscomprehensions, we elected to complement our qualitative findings by conducting a large-scale, quantitative follow-up study. For this follow-up study, we focused on 27 technical terms selected from our qualitative study.

Term Selection. To select terms for this quantitative study, we focused on widely misunderstood terms identified in the free-response definition questions on our qualitative study—defined as terms for which less than 2/3 of participants provided correct or partially correct answers. We excluded the seven widely-misunderstood data type categories because we did not have free-response definitions for those terms. This resulted in a set of 27 widely-misunderstood terms that we further investigated in the quantitative follow-up: 20 terms from iOS App Privacy Labels and 7 terms from Android Data Safety Labels. These 27 terms are identified with *'s in Table 1.

Survey Design. The core of the quantitative follow-up survey was a series of multiple-choice questions asking participants which of a set of possible options they believed most accurately defined a given term. We opted for multiple-choice questions in order to keep the survey length down sufficiently to enable us to complete a large-scale study with our available funding.

Based on the results of our qualitative survey, we divided terms into two categories. For data collection groups and purposes, we provided five possible answers: one correct answer, drawn from the definition specified in the developer documentation [4, 12], three incorrect answers, which were selected based on the thematic coding of incorrect responses provided in the qualitative survey, and "I don't know". For data types, participants were given four examples drawn from our thematic coding and asked to identify which ones were described by that data type ("I don't know" and "None of the above" were also possible responses). We also asked free-response questions (used as an attention check) and demographic questions. We validated question wording through a series of three cognitive interviews. The copy of the quantitative survey can be found in Appendix C of the full version of this paper [21].

Analysis Plan. We report descriptive statistics about the frequency of misconceptions observed in this survey.

Participant Recruitment. We recruited 400 participants online using Prolific's U.S. census-representative survey option.[1] After inspecting the free-response questions, we omitted 17 responses that appeared to have been auto-generated. We analyzed the results of the remaining 383 responses. The demographics of our user study population are summarized in Table 3.

[1]This setting ensures that participant demographics by age, sex, and ethnicity will match the most recent U.S. census data.

4.3 Ethical Considerations

Care was taken to ensure that all research was conducted following ethical best practices. No identifying information was collected, and collection of personal information was minimized. Study participants were provided with full information about the study in advance and consented to participate; they were compensated at a rate that matched pro-rated minimum wage in our jurisdiction: $7.50 for the qualitative survey (took 29 minutes on average) and $4.00 for the quantitative survey (took 15 minutes on average). Both user studies were reviewed and approved in advance by the Pomona College Institutional Review Board.

4.4 Limitations

While prior work has shown that a census-representative Prolific sample is overall fairly representative of the U.S. population for survey questions about security and privacy [38], this population skews younger, more highly-educated, and more tech-savvy than the U.S. population as a whole. This recruitment bias may cause our results to underestimate the number of Americans who do not understand or who misunderstand technical terms.

Additionally, our work was conducted in English with an English-fluent population. Individuals who are not fluent in English may have higher rates of misunderstandings or may have different misunderstandings of terms than those identified in our surveys. Moreover, our results may not apply to translations of privacy labels into other languages.

Finally, the incorrect multiple-choice options provided on our large-scale quantitative follow-up study were selected based on the thematic coding of responses from our qualitative study. Since the qualitative study was relative small-scale (24 iOS users and 22 Android users), there may exist misunderstandings that were not observed in the qualitative responses and therefore were not presented as options in the quantitative survey, potentially adding noise to the quantitative survey responses.

5 Results

Our results provide insight into which terms are commonly misunderstood and how these terms are misunderstood.

5.1 Overall Levels of Understanding

In general, our results show that Android users understand the terms used in Android Data Safety Labels better than iOS users understand terms used in iOS App Privacy Labels. Of the terms for which users provided free-response definitions, 40/47 Android terms (85.1%) were widely understood—which we define as at least 2/3 of users being able to provide a correct or partially correct definition—compared to just 21/41

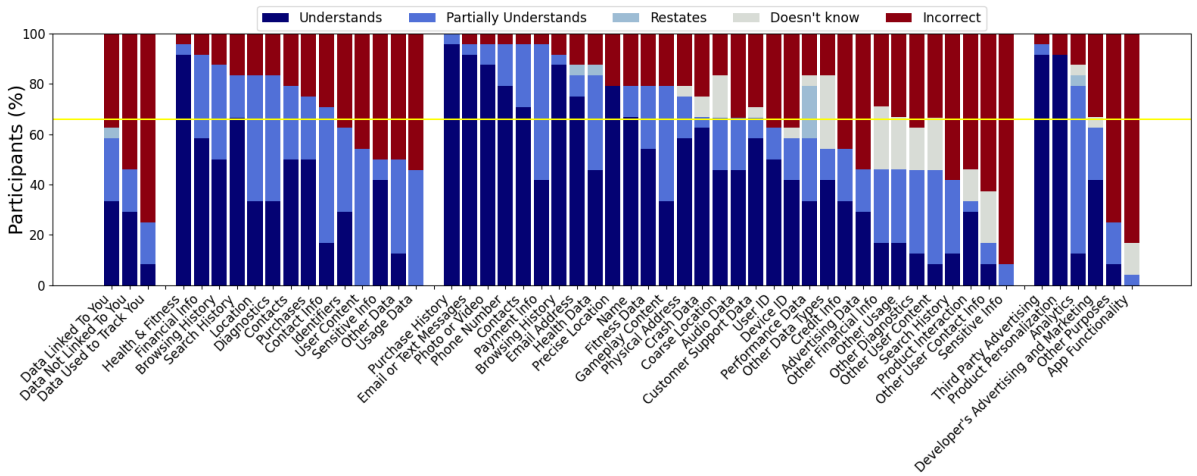


Figure 5: How well people understand technical terms in iOS App Privacy Labels (Qualitative Study).

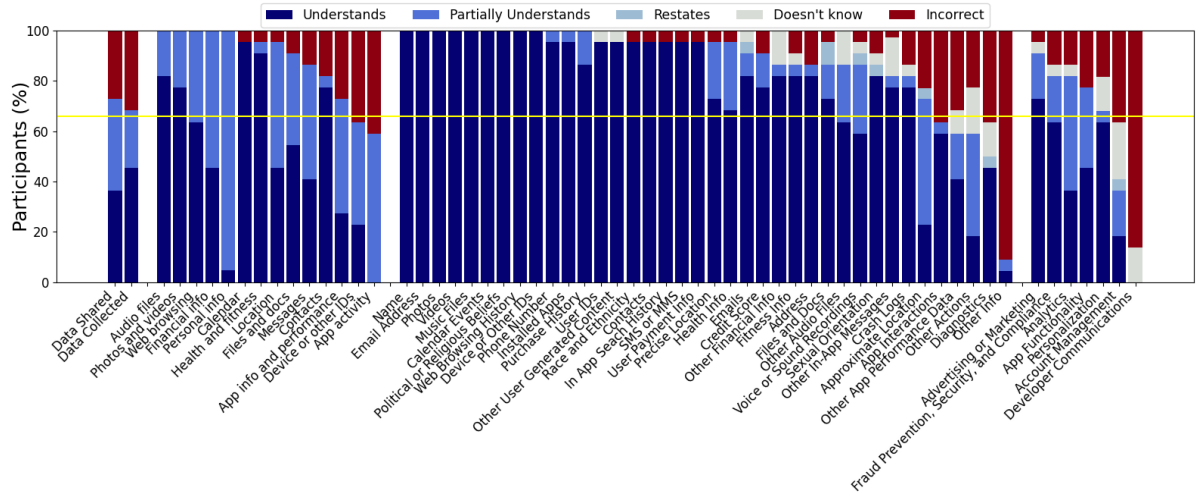


Figure 6: How well people understand technical terms in Android Data Safety Labels (Qualitative Study).

of the iOS terms (51.2%). We also found that levels of understanding varied significantly between terms, ranging from 100% of people understanding the term *Web Browsing History* to 0% understanding the term *Developer Communications*. An overview of these results is shown in Figures 5 and 6.

Both of the Android data collection categories (*Data Shared* and *Data Collected*) were widely understood, whereas none of the iOS data collection categories (*Data Linked to You*, *Data Not Linked to You*, and *Data Used to Track You*) were widely understood. This may indicate that Android's adoption of less technical terms—shared and collected are widely used in non-technical contexts—successfully increases transparency. However, this did not imply that users understood exactly how Android Data Safety labels use these terms. For example, 10/22 participants thought that apps must report collecting data that is only processed locally (they do not). And 21/22 thought that apps must report data shared with governments in response to legal requests (they do not).

Most data type categories were generally understood across both privacy labels. For 9/14 iOS data type categories (64.3%) and 12/14 Android data type categories (85.7%), at least 2/3 of users had an F1 score above .66. However, many iOS users were confused about which data types were included in *User Content* and *Usage Data*. They also frequently misclassified *Contact Data*—assuming that it included *User ID*, perhaps because email addresses are often used as user IDs, and omitting *Physical Address*, which was most commonly classified as location data. Moreover, as discussed in Section 5.2, there were widespread misconceptions about what is considered *Sensitive Data* and about the term *Other Data*. Android users were most frequently confused about what was considered *App Activity*—mistakenly omitting *Installed Apps*, *Other Actions*, and *Other User-Generated Content* and mistakenly including *Other In-App Messages* (which is actually included in the data type category *Messages*). Android responses about *Personal Info* reflected similar misconceptions to those observed

among iOS users, including classifying *Address* as *Location* instead of *Personal Info*.

Most precise data types were also widely understood. However, more Android types were widely understood (86.8%) compared to iOS types (56.3%). Some of this appears to be due to differences in the exact language used, for example, Android's term *In-app Search History* was widely understood while the iOS equivalent *Search History* was not. In other cases, the fact that Android uses more granular terms appears to improve understanding. For example, iOS's *Sensitive Info* was only understood by 8.3% of users, where as all three terms that Android labels use instead—*Political or Religious Beliefs*, *Race and Ethnicity*, and *Sexual Orientation*—were widely understood. There were also significant differences in level of understanding between different terms. Many terms, including non-technical terms such as *Name* and *Photos* and common technical terms such as *Email Address* and *SMS or MMS*, were understood by all or almost all users. Some terms—including terms that used the word "other" such as *Other User Contact Info* and *Other Info*—were understood by less than a quarter of the users surveyed.

How well people understood purpose terms varied significantly. Half of the iOS purpose terms (*Third-Party Advertising; Product Personalization; Analytics* and 4/7 Android purpose terms (*Advertising or Marketing*; *Fraud Prevention, Security, and Compliance*; *Analytics*; and *App Functionality*) were widely understood. However, other terms such as *Developer Communications*, *Account Management*, and *Other Purposes* were misunderstood by many users. Almost all iOS users also misunderstood the purpose *App Functionality*, due to the broader way that iOS labels use this term compared to the definition used by Android labels.

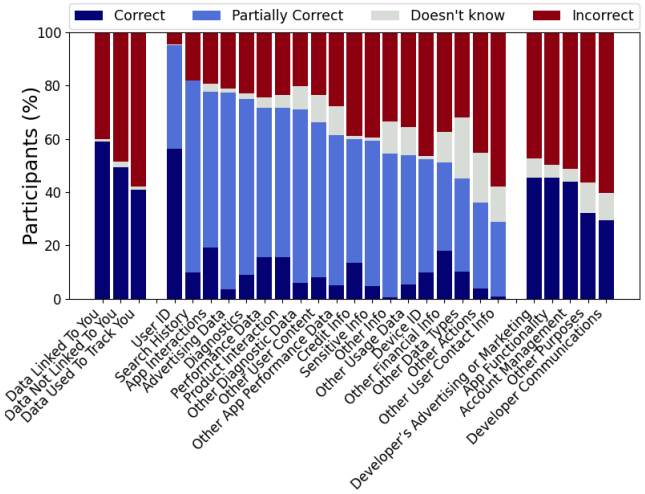


Figure 7: How accurately people can define selected privacy label terms (Quantitative Study).

5.2 Miscomprehensions about Specific Terms

Our qualitative survey together with the quantitative follow-up give insight into which individual terms people don't understand, how they misinterpret those terms, and how common those miscomprehensions are.

5.2.1 Data Collection Groups

Data Used to Track You. Apple defines the data collection group *Data Used to Track You* as any data that is linked to an individual or device that is used for targeted advertising or sold to a data broker. However, only 40.9% of users correctly identified this definition. Our thematic coding identified the three most common misconceptions as associating *Data Used to Track You* (1) with any online tracking—for example, "Data that is used to identify what you are doing on the internet"—(2) with all identifiable or personal data—for example, "personal identification and how i use the app"—and (3) with physical location tracking—for example, "That my location would be tracked." In our quantitative follow-up, the most common misunderstanding was interpreting *Data Used to Track You* as any online tracking, a misunderstanding held by 37.3% of users. This response demonstrates a vague understanding of the term but misses the fact that iOS privacy labels only use this term in the context of targeted advertising. Additionally, 12.8% of users mistakenly believed that *Data Used to Track You* covers all identifiable data, a misconception that could cause users to underestimate how much identifiable data is being collected and shared, and 4.8% of users mistakenly believed that *Data Used to Track You* referred to GPS or other physical location data.

Data Not Linked to You. As described in the Apple developer documentation, in order for data to be considered *Data Not Linked to You*, apps must not only remove any identifiers but also manipulate the data to prevent re-linkage to real-world identities. However 31.9% of users who responded to our quantitative survey thought that *Data Not Linked to You* included any data that does not specifically identify the users—a theme that appeared in qualitative survey responses like "Data not linked to you includes your purchases, contact information, usage data, as well as diagnostics. This is not linked to your identity."—compared to 49.3% who correctly recognized that this group requires that data cannot be tied back to a specific individual. This misconception could result in users significantly underestimating how much data is being collected about them that is or can be associated with their identity. While users were more confident about the definition of "linked to you" without the negation, 18.3% also described *Data Linked to You* as only including information that specifically identifies them, such as name and email address.

5.2.2 Data Type Categories and Precise Data Types

Our surveys identified many misconceptions about data types. Some of these constitute alternate interpretations of a term, for example *Sensitive Info* and *App Interactions*. In many other cases, users interpreted data types more broadly than they are defined in the developer documentation. Additionally, we observed widespread confusion about technical terms that include the word "other."

Sensitive Info. Apple defines *Sensitive Info* as including "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." This definition is consistent with how the term is used in privacy regulations and data protection laws, such as the E.U.'s General Data Protection Regulation and the California Consumer Privacy Act, both of which define similar classes of sensitive personal information as meriting additional protections.

However, we found that users interpret *Sensitive Info* broadly to include any information they consider privacy-sensitive. In our qualitative study, people included a wide range of information, including "ss#, passwords, mother's maiden name," "photos and contact info," "information about health, sexual orientation, etc," and "personally identifying information." 3/24 respondents simply provided a broad description such as, "Things that one would not readily give out." In our quantitative follow-up, 74.9% of users thought *Sensitive Info* included "Phone numbers, email, name and mailing address," 72.6% thought it included "Social security number, credit card number, and making information," and 67.1% thought it included "Health and medical history." Only 4.7% of users correctly understood the narrow scope of the term *Sensitive Info* as used in iOS App Privacy Labels.

App Interactions. Google defines *App Interactions* as "information about how a user interacts with the app. For example, the number of times they visit a page or sections they tap on." However, only 19.0% of users recognized that app clicks and time spent on the app was the only example of *App Interactions* provided in our survey. Two of the themes identified in our qualitative analysis turned out to reflect common misconceptions. 7/22 participants in the qualitative Android survey misunderstood *App Interactions* as referring to interactions between two apps rather than interactions between a user and an app, for example defining it as "How applications have interacted with each other," a misunderstanding that was also held by 40.8% of users who responded to our quantitative survey. Additionally, 41.5% of users thought that actions such as gameplay, likes, and dialog options would be considered *App Interactions*, although Google specifically provides these as examples of *Other Actions*.

Device ID. Apple defines *Device ID* as an identifier that uniquely identifies a device, for example an advertising identifier. This is similar to how Google defines their similar term *Device or Other IDs*, which also specifies that information must uniquely identify a device or app. However, many people interpreted this term more broadly. 8/24 participants in the qualitative survey and 75.5% of users in the quantitative study believed that *Device ID* includes non-identifying information. For example, one person described *Device ID* as "phone brand and model" and another said, "the specificities of the device you are using, such as which version and which software you use." Additionally, 26.2% of users misconstrued *Device ID* as including authentication credentials used to log-in to a device, such as a PIN or biometric identifiers, a theme that we also observed in our qualitative survey, where we received examples such as "face id and fingerprint id to access your device or app." Only 9.6% of users correctly understood that *Device ID* meant identifiers unique to a device.

Diagnostics. Google defines *Diagnostics* as, "Information about the performance of your app. For example battery life, loading time, latency, framerate, or any technical diagnostics." While 74.9% of users correctly identified loading time and battery life as example diagnostics, most people interpreted the term more broadly. Only 8.9% selected this correct option without also including additional incorrect options. In the qualitative survey, 15/22 responses included data that was not specific to an app or its performance, such as "information about your device, usage, etc." Additionally, 2/22 specifically mentioned crash data (e.g., "a history of any problems with - and troubleshooting - the device"), despite the fact that Android considers this a separate data type, *Crash Logs*. (By contrast, Apple includes crash data in its *Diagnostics* data type category.) Our quantitative survey confirmed that these misconceptions are widespread. 69.2% of participants thought diagnostics included general information about the device unrelated to performance or general information about phone performance not related to the specific app. And 65.5% of users incorrectly thought that Android's *Diagnostics* type would include when and how many times an app has crashed.

"Other" Terms. iOS privacy labels use six precise data types that include the word "Other," e.g., *Other Usage Data*, as well as an *Other Data* category and *Other Purposes*. Android labels include seven precise data types that include the word "Other", e.g., *Other Actions*. Of these 15 terms, 10 were included in our quantitative follow-up survey.

Both iOS and Android privacy labels use "Other" to refer to types of data (or purposes) that are not covered by any of the other provided data types (resp. purposes). For example, the precise data type *Other Usage Data* is defined as any data within the *Usage Data* category (i.e., data about user activities in the app) that is not either *Product Interaction* data or *Advertising Data*. However, users were consistently

confused about what information was covered our by these "Other" data types, presumably because they did not have the full list of possible types for comparison. For example, 54.3% of users correctly thought that gender and veteran status would be considered *Other Info* on an Android label, but 61.9% incorrect believed that race and ethnicity would be considered *Other Info* when in fact they are described by the separate *Race and Ethnicity* precise data type. Similarly, 55.1% of users incorrectly thought the iOS type *Other Contact Info* would include physical mailing address, which is in fact described by the separate *Physical Address* type.

Large minorities of users misinterpreted "Other" to be referring to other users or other apps. For example, 31.5% of users thought *Other Info* would include name and contact info about other users in the app, and 27.2% of users thought that *Other User Content* would include content generated by other users. 41.5% of users thought *Other Info* would include contact info available on other apps, and and 45.7% of users thought *Other App Performance Data* would include performance data about other apps.

We also observed specific misconceptions about some of these terms. In particular, Apple specifies that apps that use a payment service—and therefore never have access to credit card information—should not report collecting any sort of financial info. However, 53.8% of users thought that *Other Financial Info* would include credit cards stored in Apple's digital wallet app. Apple also specifies that contact information excludes identifiers and usernames that are used only for messaging inside the app, but 50.7% of users thought this information would be described by *Other User Contact Info*.

Finally, we saw a higher rate of "I don't know" responses for technical terms including the term "Other" compared to the other technical terms we asked about. On the qualitative survey, users frequently said things like "can't imagine" and "You have me stumped on this one! I have no idea." In the quantitative survey—where they were presented with a multiple choice question—on average 13.3% of users responded "I don't know" for "Other" terms, compared to just 2.0% on average for terms that did not include the word "Other."

5.2.3 Purposes

Five purposes were not widely understood on our qualitative survey, but for three of these almost half of users recognized the correct definition: *Developer's Advertising or Marketing* (45.4%), *App Functionality* (45.4%), and *Account Management* (43.6%). Moreover, no misconception was held by more than 25% of users for any of these three purposes. However, users demonstrated significant misconceptions about two purposes: *Developer Communications* and *Other Purposes*.

Developer Communications. Android defines data as being used for *Developer Communications* if it is "used to send news or notifications about the app or the developer." However, our thematic analysis identified three unique misunderstandings about this purpose. 12/22 participants assumed it referred to communicating information to the developer, including collecting diagnostic and analytic information, e.g., "Developers are the people who write the code (I think), so this would be telling those people [the data]." 3/22 definitions described communication between developers, for example, "Communications between developers working on the apps or maybe between developers working on different apps." And 2/22 described communications between apps, for example, "This might mean that it is used for developers to be able to make apps that work together." Our quantitative survey validated that the first two themes represent common misconceptions. Only 29.5% of users selected the correct definition. Instead, 29.8% of users thought this purpose referred to data used to improve app functionality or performance and 27.7% thought it referred to using data to communicate among app developers or with makers of other apps. However, only 2.9% thought it referred to coordination between apps.

Other Purposes. Similar to the results observed for data types with the term "Other," our results suggest that users cannot reliably determine what is considered "Other" without being shown all the non-"Other" options. Given an example in which data were used for *App Functionality* and *Other Purposes*, only 32.1% correctly recognized that *Other Purposes* excluded unlisted purposes such as advertising, analytics, and personalization. 31.1% incorrectly believed that *Other Purposes* in that example would include any purpose other than *App Functionality*. This suggests that having a purpose named *Other Purposes* is extremely misleading and impedes transparency about the purposes for which data are collected.

6 Discussion and Conclusions

In this work, we evaluated how well people understand the technical terms used in iOS and Android privacy labels. We found that although some common terms are well-understood, other terms are confusing or misleading to many users. We identified these poorly understood terms and identified common misinterpretations and misunderstandings. These results enrich the prior literature about understandings of app privacy labels. They also form an empirical basis for new guidelines for improving app privacy labels.

Recommendation 1: *Privacy labels should only use terms in ways that are consistent with their widespread and non-technical definitions.*

Our results confirm earlier qualitative findings that users misunderstand terms like *Data used to Track* [27, 43], despite prior work showing that users are at least somewhat confident that they understand this term [5]. Moreover, our results validate Zhang et al.'s finding that this term is commonly confused with both physical location tracking and with general

online tracking [43]. In both cases, those misconceptions represent assumptions that a more commonly-used definition of "tracking" should also apply in this context. An alternate term that would be consistent with standard definitions could be *Data Used for Targeted Advertising*.

We also identify another term that is poorly understood due to conflation with its non-technical usage: *Sensitive Info*. Prior work found that users are not confident in their understanding of this term [5]; our results show that users indeed do not understand this term and that these misunderstandings are primarily due to assumptions that "sensitive" is used in its non-technical sense—meaning anything privacy-sensitive or that the user would be reluctant to share publicly—whereas iOS labels use it to refer only to sensitive demographic information. To avoid this confusion, labels could instead use a more explicit term like *Sensitive Demographic Information* or could list specific types of sensitive information individually.

Recommendation 2: *Privacy labels should avoid terms with ambiguous syntax.*

Like prior work [5, 27, 43] we found that users frequently misinterpreted or were confused by terms that use the word "Other." However, our results provide insight into how users misinterpet these terms. A common misinterpretation is that users were unsure how to interpret "Other" grammatically, for example interpreting *Other App Performance Data* as performance data about other apps rather than as other data about app performance or interpreting *Other User Contact Information* as contact information for other users rather than other types of contact information. We also identified additional terms that are widely misunderstood for similar reasons, for example *Developer Communications*. Our results suggest that common misunderstandings of this term arise because many users misinterpret the developer as the object of the phrase—the one receiving the communication, either from the app or from other developers—rather than the subject of the phrase—the one doing the communicating, specifically communicating to the user. These results suggest that app stores should take care to avoid terms with ambiguous syntax or grammatical interpretation. Renaming data types to be grammatically unambiguous, e.g., *App Performance Data (Other)* instead of *Other App Performance Data*, could improve comprehension and enhance transparency.

Recommendation 3: *Privacy labels should only use terms that can be understood in isolation.*

Our results also identify a second factor contributing to confusion and misunderstandings about "Other" terms: the fact that most users did not understand what the alternatives to "Other" were. In fact, many users assumed that "Other" meant anything other than the things listed in this specific label. For example, 56.7% of users shown a label stating that an app collects three types of *User Content—Photos or Videos*, *Gameplay Content*, and *Other User Content*—interpreted *Other User Content* to include audio data; in fact, *Audio Data* is a different precise data type, and its omission is intended to signal that the app does not collect audio data.

One way to implement this guideline would be to ensure that label terms provide a complete taxonomy without relying on terms that include the word "Other." If this proves infeasible, alternate solutions that would mitigate these misunderstanding include: (1) clarifying what the alternatives to "Other" are on hover or (2) requiring developers to explicitly list things they are categorizing as "Other."

Recommendation 4: *Privacy labels should use more granular terms to describe data types.*

Data types that encompass a broad range of values should be separated into multiple, more granular data types. For example, the iOS data type category *Usage Data*—which includes values such as *Email or Text Messages*, *Photo or Video*, *Audio Data*, and *Gameplay Content*—was almost universally misunderstood, despite the fact that prior work shows users are confident they understand this term [5]. By contrast, precise data types included in this category were widely understood. This suggests that breaking some data type categories and precise data types into additional, more fine-grained categories and types could improve comprehension. We anticipate that more granular terms would be particular impactful for (1) data type categories—since these appear in concise privacy labels, which users are more likely to look at [27]—and (2) terms that include both values that decrease willingness to download [5] and values that users view as benign—since conflating these values into a single term may make it more difficult for users to evaluate an app's data practices.

Recommendation 5: *Terminology should be user-tested before introducing new standards for privacy labels.*

Our results—the first to systematically evaluate label term comprehensions with a user study—suggest that many misunderstandings could be eliminated by tweaking the terminology used to describe a data practice. For example, *Search History* could become *In-App Search History*—eliminating the misconception that *Search History* includes browser search history—*Credit Info* could become *Credit Score*—eliminating the misconception that *Credit Info* includes credit card information—and *App Interactions* could become *Your Interactions with the App*—eliminating the misconception that *App Interactions* refers to interactions between apps. However, to prevent the introduction of new misunderstandings, we recommend that any new terminology be tested with user studies to confirm that it doesn't introduce new misinterpretations before deploying a revised taxonomy of terms for app privacy labels.

Overall, our results provide insight into how users interpret technical terms in app privacy labels and form the foundation for empirical guidelines into how to improve technical language for a second generation of app privacy labels.

References

[1] Andrick Adhikari, Sanchari Das, and Rinku Dewri. Evolution of composition, readability, and structure of privacy policies over two decades. *Proceedings on Privacy Enhancing Technologies*, 2023(3):138–153, 2023.

[2] Ryan Amos, Gunes Acar, Elena Lucherini, Mihir Kshirsagar, Arvind Narayanan, and Jonathan Mayer. Privacy Policies Over Time: Curation and Analysis of a Million-Document Dataset. In *The Web Conference*, pages 2165–2176, 2021.

[3] Annie Anton, Julia Earp, Qingfeng He, William Stufflebeam, Davide Bolchini, and Carlos Jensen. Financial privacy policies and the need for standardization. *IEEE Security & Privacy*, 2(3):36–45, 2004.

[4] Apple. App privacy details on the app store. https://developer.apple.com/app-store/app-privacy-details/.

[5] David G. Balash, Mir Masood Ali, Chris Kanich, and Adam J. Aviv. "I would not install an app with this label": Privacy label impact on risk perception and willingness to install iOS apps. In *20th Symposium on Usable Privacy and Security*, pages 413–432, 2024.

[6] Rex Chen, Fei Fang, Thomas Norton, Aleecia M. McDonald, and Norman Sadeh. Fighting the fog: Evaluating the clarity of privacy disclosures in the age of CCPA. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*, pages 73–102, 2021.

[7] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, and Hanan Hibshi. Ask the experts: What should be on an IoT privacy and security label? In *IEEE Symposium on Security and Privacy*, pages 447–464, 2020.

[8] Pardis Emami-Naeini, Janarth Dheenadhayalan, Yuvraj Agarwal, and Lorrie Faith Cranor. An informative security and privacy "nutrition" label for Internet of Things devices. *IEEE Security & Privacy*, 20(2):31–39, 2021.

[9] Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019.

[10] Benjamin Fabian, Tatiana Ermakova, and Tino Lentz. Large-scale readability analysis of privacy policies. In *Proceedings of the International Conference on Web Intelligence*, pages 18–25, 2017.

[11] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android permissions: User attention, comprehension, and behavior. In *8th Symposium on Usable Privacy and Security*, 2012.

[12] Google. Provide information for Google Play's data safety section. https://support.google.com/googleplay/android-developer/answer/10787469.

[13] Mark Graber, Donna D'Alessandro, and Jill Johnson-West. Reading level of privacy policies on internet health web sites. *The Journal of Family Practice*, 51(7):642–645, 2002.

[14] Hana Habib, Megan Li, Ellie Young, and Lorrie Cranor. "Okay, whatever": An evaluation of cookie consent interfaces. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–27, 2022.

[15] Mark Hochhauser. Lost in the fine print: Readability of financial privacy notices. https://privacyrights.org/resources/lost-fine-print-readability-financial-privacy-notices-hochhauser, June 2001.

[16] Irene Ioannidou and Nicolas Sklavos. On general data protection regulation vulnerabilities and privacy issues, for wearable devices and fitness tracking applications. *Cryptography*, 5(4):29, 2021.

[17] Akshath Jain, David Rodriguez, Jose M. Del Alamo, and Norman Sadeh. Atlas: Automatically detecting discrepancies between privacy policies and privacy labels. In *IEEE European Symposium on Security and Privacy Workshops*, pages 94–107, 2023.

[18] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. A "nutrition label"' for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.

[19] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. Standardizing privacy notices: An online study of the nutrition label approach. In *Proceedings of the 2010 CHI Conference on Human Factors in Computing Systems*, pages 1573–1582, 2010.

[20] Patrick Gage Kelley, Lorrie Faith Cranor, and Norman Sadeh. Privacy as part of the app decision-making process. In *Proceedings of the 2013 CHI Conference on Human Factors in Computing Systems*, pages 3393–3402, 2013.

[21] Ishika Keswani, Kerick Walker, Adrian Clement, Eusila Kitur, Nannapas Wonghirundacha, Ryan Aubrey, Vivien Song, and Eleanor Birrell. User understandings of

technical terms in app privacy labels. http://www.cs.pomona.edu/~ebirrell/docs/SOUPS25-PrivLabelTerms-full.pdf, 2025.

[22] Simon Koch, Malte Wessels, Benjamin Altpeter, Madita Olvermann, and Martin Johns. Keeping privacy labels honest. *Proceedings on Privacy Enhancing Technologies*, 2022(4):486—-506, 2022.

[23] Konrad Kollnig, Anastasia Shuba, Max Van Kleek, Reuben Binns, and Nigel Shadbolt. Goodbye tracking? Impact of iOS app tracking transparency and privacy labels. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*, pages 508–520, 2022.

[24] Barbara Krumay and Jennifer Klar. Readability of privacy policies. In *IFIP Annual Conference on Data and Applications Security and Privacy*, pages 388–399, 2020.

[25] Tianshi Li, Kayla Reiman, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I. Hong. Understanding challenges for developers to create accurate privacy nutrition labels. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–24, 2022.

[26] Yucheng Li, Deyuan Chen, Tianshi Li, Yuvraj Agarwal, Lorrie Faith Cranor, and Jason I. Hong. Understanding iOS privacy nutrition labels: An exploratory large-scale analysis of app store data. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, pages 1–7, 2022.

[27] Yanzi Lin, Jaideep Juneja, Eleanor Birrell, and Lorrie Faith Cranor. Data safety vs. app privacy: Comparing the usability of Android and iOS privacy labels. *Proceedings on Privacy Enhancing Technologies*, 2024(2):182–210, 2024.

[28] Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz. The privacy policy landscape after the GDPR. *Proceedings on Privacy Enhancing Technologies*, 2020(1):47–64, 2020.

[29] Aleecia M. McDonald and Lorrie Faith Cranor. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4:540–565, 2008.

[30] Jayashree Mohan, Melissa Wasserman, and Vijay Chidambaram. Analyzing GDPR compliance through the lens of privacy policy. In *Heterogeneous Data Management, Polystores, and Analytics for Healthcare*, pages 82–95, 2019.

[31] Charlotte Moremen, Jordan Hoogsteden, and Eleanor Birrell. Generational differences in understandings of privacy terminology. *Proceedings on Privacy Enhancing Technologies*, 2024(3):589–605, 2024.

[32] Mozilla. Data privacy labels for most top apps in Google play store are false or misleading. https://foundation.mozilla.org/en/campaigns/googles-data-safety-labels/, 2023.

[33] Robert Proctor, Athar Ali, and Kim-Phuong Vu. Examining usability of web privacy policies. *International Journal of Human-Computer Interaction*, 24(3):307–328, 2008.

[34] David Rodriguez, Akshath Jain, Jose M. Del Alamo, and Norman Sadeh. Comparing privacy label disclosures of apps published in both the App Store and Google Play Stores. In *2023 IEEE European Symposium on Security and Privacy Workshops*, pages 150–157, 2023.

[35] Ravi Inder Singh, Manasa Sumeeth, and James Miller. A user-centric evaluation of the readability of privacy policies in popular web sites. *Information Systems Frontiers*, 13(4):501–514, 2011.

[36] Aaron Smith. What internet users know about technology and the web. https://www.pewresearch.org/internet/2014/11/25/web-iq/, November 2014.

[37] Daniel Solove. Privacy self-management and the consent dilemma. *Harvard Law Review*, 126(7):1880–1903, 2013.

[38] Jenny Tang, Eleanor Birrell, and Ada Lerner. Replication: How well do my results generalize now? The external validity of online privacy and security surveys. In *18th Symposium on Usable Privacy and Security*, pages 367–385, 2022.

[39] Jenny Tang, Hannah Shoemaker, Ada Lerner, and Eleanor Birrell. Defining privacy: How users interpret technical terms in privacy policies. *Proceedings on Privacy Enhancing Technologies*, 2021(3):70–94, 2021.

[40] Joseph Turow, Lauren Feldman, and Kimberly Meltzer. Open to exploitation: America's shoppers online and offline. *Departmental Papers (ASC)*, 2005.

[41] Joseph Turow, Michael Hennessy, and Nora Draper. Persistent misperceptions: Americans' misplaced confidence in privacy policies, 2003–2015. *Journal of Broadcasting & Electronic Media*, 62(3):461–478, 2018.

[42] Yue Xiao, Zhengyi Li, Yue Qin, Xiaolong Bai, Jiale Guan, Xiaojing Liao, and Luyi Xing. Lalaine: Measuring and characterizing non-compliance of Apple privacy

labels. In *32nd USENIX Security Symposium*, pages 1091–1108, 2023.

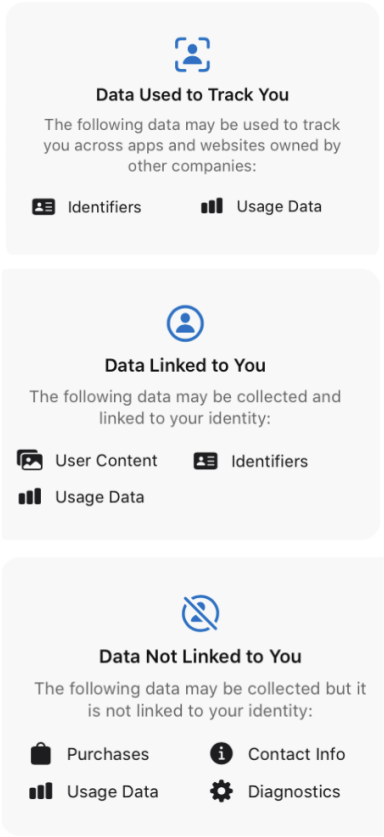
[43] Shikun Zhang, Yuanyuan Feng, Yaxing Yao, Lorrie Faith Cranor, and Norman Sadeh. How usable are iOS app privacy labels? *Proceedings on Privacy Enhancing Technologies*, 2022(4):204–228, 2022.

[44] Shikun Zhang, Lily Klucinec, Kyerra Norton, Norman Sadeh, and Lorrie Faith Cranor. Exploring expandable-grid designs to make iOS app privacy labels more usable. In *20th Symposium on Usable Privacy and Security*, pages 139–157, 2024.

[45] Shikun Zhang and Norman Sadeh. Do privacy labels answer users' privacy questions? In *Workshop on Usable Security and Privacy*, 2023.

A Qualitative Survey (iOS Version)

Consider the following iOS App Privacy Label:



1. In your own words, how would you define the term "Data Used to Track You" in this context?

2. In your own words, how would you define the term "Data Linked to You" in this context?

3. In your own words, how would you define the term "Data Not Linked to You" in this context?

4. Which of the following definitions best matches your interpretation of "Data Used to Track You"?

   - Data from the app that is linked with your data collected from other companies' apps, websites, or offline properties, and used for ads or shared with a data broker.
   - Data from the app that is linked with your data collected from other companies' apps, websites, or offline properties.
   - Data collected in a way that is linked to your identity, such as to your account, your device, or your details.
   - Data collected in a way that is not linked to your identity.
   - Data collected from the app regarding your device's location

5. Which of the following would you consider to be an example of "Data Linked to You"?

   ☐ Name
   ☐ email address
   ☐ Credit card number when it is associated with a name
   ☐ Credit card number that is *not* associated with a name
   ☐ IP address when it is associated with a name
   ☐ Anonymous IP address when it is *not* associated with a name
   ☐ MAC address or other device identifier when it is associated with a name
   ☐ Anonymous MAC address or other device identifier when it is *not* associated with a name
   ☐ health records when they are associated with a name
   ☐ anonymous health records that are *not* associated with a name or any other identifier
   ☐ Interactions with an app when they are associated with a name or other identifier
   ☐ Anonymous interactions with an app that are not associated with a name or other identifier

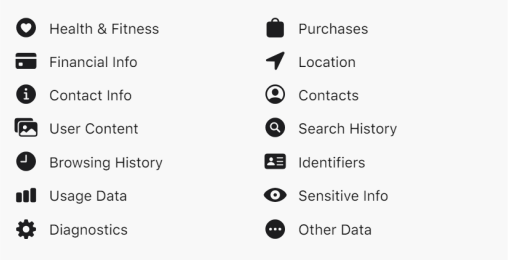
6. If an app states that it collects "Name" data, what types of information do you think that could include?

7. If an app states that it collects "Email Address" data, what types of information do you think that could include?

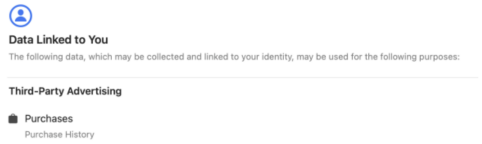
8. If an app states that it collects "Phone Number" data, what types of information do you think that could include?

9. If an app states that it collects “Physical Address” data, what types of information do you think that could include?
10. If an app states that it collects “Health” data, what types of information do you think that could include?
11. If an app states that it collects “Fitness” data, what types of information do you think that could include?
12. If an app states that it collects “Payment Info” data, what types of information do you think that could include?
13. If an app states that it collects “Credit Info” data, what types of information do you think that could include?
14. If an app states that it collects “Precise Location” data, what types of information do you think that could include?
15. If an app states that it collects “Coarse Location” data, what types of information do you think that could include?
16. If an app states that it collects “Sensitive Info” data, what types of information do you think that could include?
17. If an app states that it collects “Contacts” data, what types of information do you think that could include?
18. If an app states that it collects “Email or Text Messages” data, what types of information do you think that could include?
19. If an app states that it collects “Photos or Videos” data, what types of information do you think that could include?
20. If an app states that it collects “Audio Data,” what types of information do you think that could include?
21. If an app states that it collects “Gameplay Content” data, what types of information do you think that could include?
22. If an app states that it collects “Customer Support” data, what types of information do you think that could include?
23. If an app states that it collects “Browsing History” data, what types of information do you think that could include?
24. If an app states that it collects “Search History” data, what types of information do you think that could include?
25. If an app states that it collects “User ID” data, what types of information do you think that could include?
26. If an app states that it collects “Device ID” data, what types of information do you think that could include?
27. If an app states that it collects “Purchase History” data, what types of information do you think that could include?
28. If an app states that it collects “Advertising Data,” what types of information do you think that could include?
29. If an app states that it collects “Product Interaction” data, what types of information do you think that could include?
30. If an app states that it collects “Crash Data,” what types of information do you think that could include?
31. If an app states that it collects “Performance Data," what types of information do you think that could include?
32. If an app states that it collects “Other User Contact Info” data, what types of information do you think that could include?
33. If an app states that it collects “Other Financial Info” data, what types of information do you think that could include?
34. If an app states that it collects “Other User Content” data, what types of information do you think that could include?
35. If an app states that it collects “Other Usage Data," what types of information do you think that could include?
36. If an app states that it collects “Other Diagnostics Data,” what types of information do you think that could include?
37. If an app states that it collects “Other Data Types,” what types of information do you think that could include?

Consider the following data type categories as they appear on the Apple App Store:

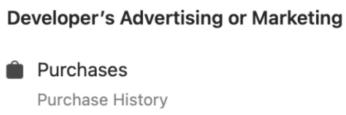


38. For each data type on the left, please drag and drop it into the category you think it belongs in.
[On the left was a list of the 32 iOS precise data types, on the right was a list of the 14 iOS data type categories]



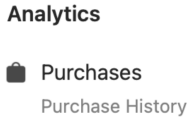
39. The privacy label above shows that your purchase history is used for "Third-Party Advertising". In your own words, what do you think "Third-Party Advertising" means in this context?

40. Give examples of how an app might use your purchase history that would count as using it for "Third-Party Advertising".



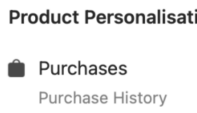
41. The privacy label above shows that your purchase history is used for "Developer's Advertising or Marketing". In your own words, what do you think "Developer's Advertising or Marketing" means in this context?

42. Give examples of how an app might use your purchase history that would count as using it for "Developer's Advertising or Marketing".



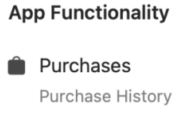
43. The privacy label above shows that your purchase history is used for "Analytics". In your own words, what do you think "Analytics" means in this context?

44. Give examples of how an app might use your purchase history that would count as using it for "Analytics".



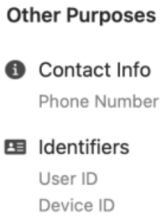
45. The privacy label above shows that your purchase history is used for "Product Personalisation". In your own words, what do you think "Product Personalisation" means in this context?

46. Give examples of how an app might use your purchase history that would count as using it for "Product Personalisation".



47. The privacy label above shows that your purchase history is used for "App Functionality". In your own words, what do you think "App Functionality" means in this context?

48. Give examples of how an app might use your purchase history that would count as using it for "App Functionality".



49. The privacy label above shows that your Phone Number, User ID, and Device ID are used for "Other Purposes". In your own words, what do you think "Other Purposes" means in this context?

50. Give examples of how an app might use your Phone Number that would count as using it for "Other Purposes".

51. How much do you feel you understand what companies are doing with the data they collect about you?
    - A great deal
    - Some
    - Very little
    - Nothing

52. How concerned are you, if at all, about how companies are using the data they collect about you?
    - Very concerned
    - Somewhat concerned
    - Not too concerned
    - Not at all concerned

53. What sort of smartphone do you primarily use?
    - Android
    - iOS
    - other
    - I don't use a smartphone

54. What is your current age?
    - 18-24
    - 25-34
    - 35-44
    - 45-59
    - 60-74
    - 75+

55. What is your gender?
    - Man
    - Woman
    - Non-binary person
    - Prefer not to answer

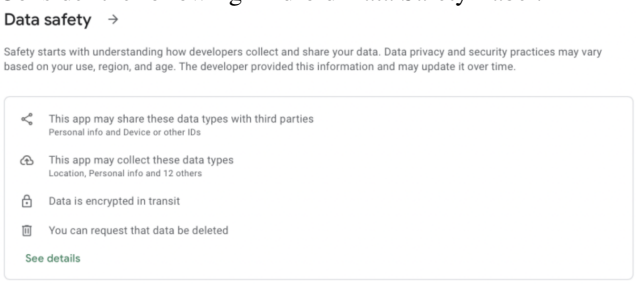
- Prefer to self-describe

56. Choose one or more races that you consider yourself to be:
    - ☐ White
    - ☐ Black or African American
    - ☐ Native American or Alaska Native
    - ☐ Asian
    - ☐ Pacific Islander or Native Hawaiian
    - ☐ Other

57. Do you consider yourself to be Hispanic/Latino/Latinx?
    - Yes
    - No

B Qualitative Survey (Android Version)

Consider the following Android Data Safety Label:



1. In your own words, how would you define the term "share" in this context?

2. In your own words, how would you define the term "collect" in this context?

3. Which of the following would you consider to be an example of "data shared"?
    - ☐ Transfer of user data collected from your app from your server to a third-party server
    - ☐ Transferring user data from your app to another app directly on the device.
    - ☐ Transferring data collected from your app off a user's device directly to a third party
    - ☐ Transferring user data to a "service provider" that processes it on behalf of the developer
    - ☐ Transferring user data for specific legal purposes, such as in response to a legal obligation or government requests
    - ☐ Data from your app sent to other locations using specific tools that are included in your app
    - ☐ Data collected from a webview which has been opened from your app, if your app is in control of the code/behavior delivered through that webview.
    - ☐ Data accessed by your app that is only processed locally on the user's device and not sent off device
    - ☐ Data that is sent off device, but that is unreadable by you or anyone other than the sender and recipient as a result of end-to-end encryption.
    - ☐ Data that is accessed by an app and transferred off the user's device
    - ☐ Data that is accessed by an app and transferred to a third party

4. Which of the following would you consider to be an example of "data collected"?
    - ☐ Transfer of user data collected from your app from your server to a third-party server
    - ☐ Transferring user data from your app to another app directly on the device.
    - ☐ Transferring data collected from your app off a user's device directly to a third party
    - ☐ Transferring user data to a "service provider" that processes it on behalf of the developer
    - ☐ Transferring user data for specific legal purposes, such as in response to a legal obligation or government requests
    - ☐ Data from your app sent to other locations using specific tools that are included in your app
    - ☐ Data collected from a webview which has been opened from your app, if your app is in control of the code/behavior delivered through that webview.
    - ☐ Data accessed by your app that is only processed locally on the user's device and not sent off device
    - ☐ Data that is sent off device, but that is unreadable by you or anyone other than the sender and recipient as a result of end-to-end encryption.
    - ☐ Data that is accessed by an app and transferred off the user's device
    - ☐ Data that is accessed by an app and transferred to a third party

5. If an app states that it collects your "Approximate Location", what types of information do you think that could include?

6. If an app states that it collects your "Precise Location", what types of information do you think that could include?

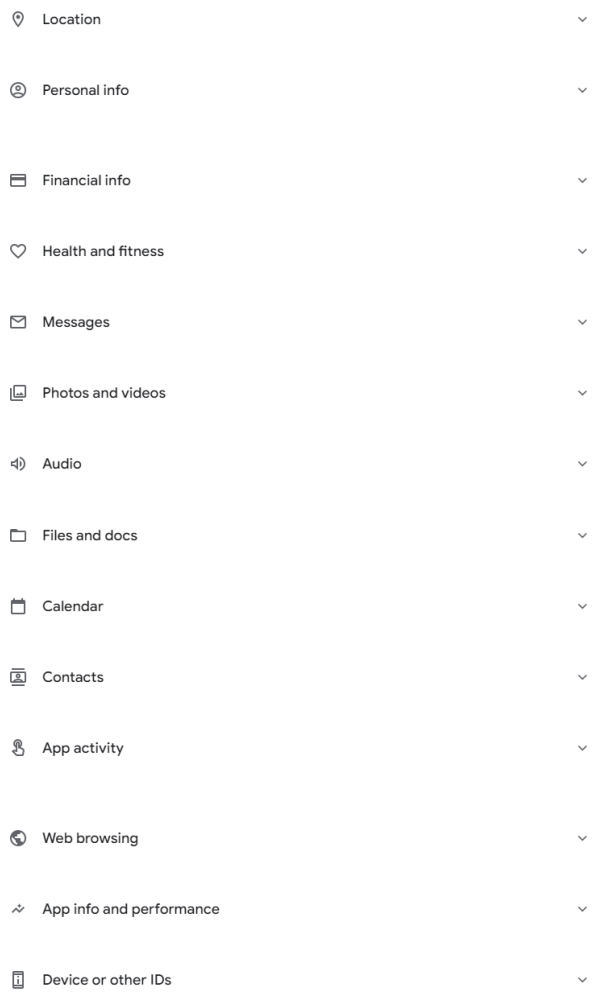
7. If an app states that it collects your "Name", what types of information do you think that could include?

8. If an app states that it collects your "Email Address", what types of information do you think that could include?

9. If an app states that it collects your "User IDs", what types of information do you think that could include?

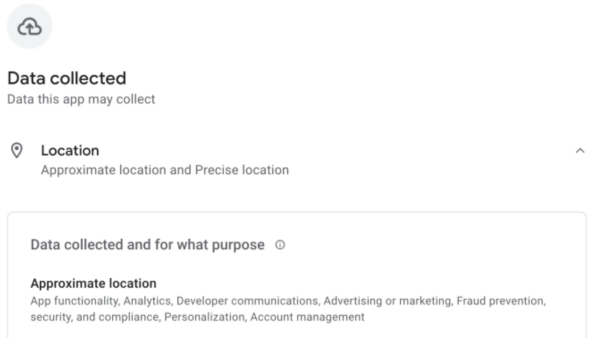
10. If an app states that it collects your "Address", what types of information do you think that could include?

11. If an app states that it collects your "Phone Number", what types of information do you think that could include?
12. If an app states that it collects your "Race and Ethnicity", what types of information do you think that could include?
13. If an app states that it collects your "Political or Religious Beliefs", what types of information do you think that could include?
14. If an app states that it collects your "Sexual Orientation", what types of information do you think that could include?
15. If an app states that it collects your "User Payment Info", what types of information do you think that could include?
16. If an app states that it collects your "Purchase History", what types of information do you think that could include?
17. If an app states that it collects your "Credit Score", what types of information do you think that could include?
18. If an app states that it collects your "Health Info", what types of information do you think that could include?
19. If an app states that it collects your "Fitness Info", what types of information do you think that could include?
20. If an app states that it collects your "Emails", what types of information do you think that could include?
21. If an app states that it collects your "SMS or MMS", what types of information do you think that could include?
22. If an app states that it collects your "Photos", what types of information do you think that could include?
23. If an app states that it collects your "Videos", what types of information do you think that could include?
24. If an app states that it collects your "Voice or Sound Recordings", what types of information do you think that could include?
25. If an app states that it collects your "Music Files", what types of information do you think that could include?
26. If an app states that it collects your "Files and Docs", what types of information do you think that could include?
27. If an app states that it collects your "Calendar Events", what types of information do you think that could include?
28. If an app states that it collects your "Contacts", what types of information do you think that could include?
29. If an app states that it collects your "App Interactions", what types of information do you think that could include?
30. If an app states that it collects your "In-app Search History", what types of information do you think that could include?
31. If an app states that it collects your "Installed Apps", what types of information do you think that could include?
32. If an app states that it collects your "Web Browsing History", what types of information do you think that could include?
33. If an app states that it collects your "Crash Logs", what types of information do you think that could include?
34. If an app states that it collects your "Diagnostics", what types of information do you think that could include?
35. If an app states that it collects your "Device or Other IDs", what types of information do you think that could include?
36. If an app states that it collects your "Other Info", what types of information do you think that could include?
37. If an app states that it collects your "Other Financial Info", what types of information do you think that could include?
38. If an app states that it collects your "Other In-app Messages", what types of information do you think that could include?
39. If an app states that it collects your "Other Audio Files", what types of information do you think that could include?
40. If an app states that it collects your "Other User-Generated Content", what types of information do you think that could include?
41. If an app states that it collects your "Other Actions", what types of information do you think that could include?
42. If an app states that it collects your "Other App Performance Data", what types of information do you think that could include?
43. Consider the following data type categories as they appear on the Android Play Store:



For each data type on the left, please drag and drop it into the category you think it belongs in.

[On the left was a list of the 38 Android precise data types, on the right was a list of the 14 Android data type categories]



44. The data safety label above shows that your approximate location is used for "App Functionality". In your own words, what do you think "App Functionality" means in this context?
45. Give examples of how an app might use your approximate location that would count as using it for "App Functionality".
46. The data safety label above shows that your approximate location is used for "Analytics". In your own words, what do you think "Analytics" means in this context?
47. Give examples of how an app might use your purchase history that would count as using it for "Analytics".
48. The data safety label above shows that your approximate location is used for "Developer Communications". In your own words, what do you think "Developer Communications" means in this context? ef
49. Give examples of how an app might use your approximate location that would count as using it for "Developer Communications".
50. The privacy label above shows that the approximate location is used for "Advertising or Marketing". In your own words, what do you think "Advertising or Marketing" means in this context?
51. Give examples of how an app might use your purchase history that would count as using it for "Advertising or Marketing".
52. The privacy label above shows that your approximate location is used for "Fraud prevention, security, and compliance". In your own words, what do you think "Fraud prevention, security, and compliance" means in this context?
53. Give examples of how an app might use your purchase history that would count as using it for "Fraud prevention, security, and compliance".
54. The privacy label above shows that your approximate location is used for "Personalization". In your own words, what do you think "Personalization" means in this context?
55. Give examples of how an app might use your purchase history that would count as using it for "Personalization".
56. The privacy label above shows that your approximate location is used for "Account Management". In your own words, what do you think "Account Management" means in this context?
57. Give examples of how an app might use your purchase history that would count as using it for "Account Management".

The Android version then concluded with the same seven questions about privacy attitudes and demographics as the iOS version (Questions 51–57 in Appendix A).