From Discovery to Decisions: Archetypal Journeys of Mobile App Users and Their Implications on Privacy

HTMA Riyadh
CISPA Helmholtz Center for Information Security, *and* Saarland University
Saarbrücken, Germany
htma.riyadh@cispa.de

Divyanshu Bhardwaj
CISPA Helmholtz Center for Information Security, *and* Saarland University
Saarbrücken, Germany
divyanshu.bhardwaj@cispa.de

Maria Victoria Hellenthal
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
hellenthal@cispa.de

Alexander Hart
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
hart@cispa.de

Katharina Krombholz
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
krombholz@cispa.de

Sven Bugiel
CISPA Helmholtz Center for Information Security
Saarbrücken, Germany
bugiel@cispa.de

Figure 1: A conceptual depiction of the mobile user journey as a series of sequential steps that shape expectations before the permission prompt appears, such as need recognition, app type, reviews, and rationales.

Abstract

Mobile permission decisions are often studied at the moment a permission request appears. However, our study shows that users' choices are shaped much earlier, across a multi-stage journey that begins with app-need recognition and unfolds through app discovery, exploration, selection, installation, and first use. Drawing on interviews with 19 U.S. Android users, we map this process and identify four archetypal journeys that explain how early cues, such as discovery sources, app type, and social trust, shape later permission behavior. These insights align with theoretical models like Privacy Calculus, showing how users weigh perceived benefits and risks at each step, and complement Contextual Integrity theory, explaining how social norms and information flows shape expectations and constrain privacy agency across steps. We contribute an empirically grounded framework that clarifies why permission outcomes vary across contexts. Our results reframe mobile privacy as a sequential, path-dependent process, offering implications for future design and research.

CCS Concepts

• **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → **Empirical studies in HCI**; **User centered design**.

Keywords

mobile privacy, permission-granting decision, user journey, android permissions, human-centered security

CHI '26, Barcelona, Spain

ACM ISBN 979-8-4007-2278-3/2026/04
https://doi.org/10.1145/3772318.3790430

ACM Reference Format:
HTMA Riyadh, Divyanshu Bhardwaj, Maria Victoria Hellenthal, Alexander Hart, Katharina Krombholz, and Sven Bugiel. 2026. From Discovery to Decisions: Archetypal Journeys of Mobile App Users and Their Implications on Privacy. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 25 pages. https://doi.org/10.1145/3772318.3790430

1 Introduction

When users *allow* or *deny* a mobile app permission request, what really drives that decision? Is it the design of the permission dialog, the trust they built long before while browsing app descriptions, scanning reviews and comparing alternatives, or perhaps something else?

This question highlights a central issue in designing and studying permission-granting, for which we still lack a clear answer. Researchers have examined fragments of this problem, typically studying how individual factors shape permission decisions. Works in this space [6, 8, 9, 13, 17, 18, 64] have focused on understanding how demographic or cultural differences, interface design, and communication cues (e.g., rationale messages, app ratings) influence permission responses. While these studies provide valuable insights, they tend to treat each factor in isolation, such as the permission prompt, rationale, or demographic influence. However, they do not account for *how* these factors accumulate and interact across the sequence of steps that culminate in a permission decision. As such, *we lack a holistic understanding of the journey users take to form permission-granting decisions for mobile applications.*

This limitation motivates our work to connect these fragmented insights into a coherent framework that explains how permission decisions evolve throughout the app adoption process. Answering this question requires empirically investigating how decisions unfold across the user journey and how experiences and contextual factors shape subsequent choices. Our approach aligns with theoretical models such as Privacy Calculus [15], situating cost–benefit evaluations within the broader user journey. It also complements Contextual Integrity [51] by explaining how expectations about appropriate information flows form and shift across sequential steps. Prior work hints that such a journey exists by identifying structured decision points in app adoption [22, 34], but these studies stop short of capturing how these points connect into a sequential, cumulative process.

In the current mobile privacy landscape, users encounter privacy information at two distinct points in the app adoption process: pre-installation cues provided in app marketplaces, and post-installation mechanisms that activate during app use. Before installation, app developers provide users with tools such as the Data Safety Section (DSS) and privacy nutrition labels [5]. These tools reveal how an app collects, uses, and shares personal data, allowing users to assess its credibility and potential privacy risks. After installation, the decision paradigm shifts to the runtime permission model [4], where users are prompted at first use to either 'allow' or 'deny' access to resources, such as location or camera. App developers sometimes provide a brief explanation, called a rationale, to help users understand why certain permissions are required. Taken together, these decentralized privacy tools create a complex landscape through which users must navigate.

Our study builds on these process-oriented perspectives by examining how early cues, such as information sources, peer trust, and incentives, shape the permission decisions that occur downstream. To the best of our knowledge, no study has systematically investigated the entire journey a user undertakes from need recognition to app discovery, evaluation, installation, and permission response. Our work makes an important step in addressing this gap by empirically mapping this end-to-end process. Developing this understanding requires first uncovering how users themselves describe the journey from app need to permission response. To capture this holistic view, we draw on the concept of *user journey mapping* [25], a method widely used in user experience [20, 62], human–computer interaction [50, 52, 53], and sales and marketing [40, 46, 61, 69] for studying multi-stage decision processes.

We conducted semi-structured interviews with 19 Android users to explore how they describe the steps, perceptions, and decisions that shape their permission choices. We focus on Android because its diverse app sources and granular permission model better expose pre-installation cues and sideloading practices. Our investigation is based on the following research questions:

- **RQ1** *What are the distinct stages in the user journey from app need to permission decision?*
- **RQ2** *How do these stages vary depending on the type of app?*
- **RQ3** *What privacy-related strategies do users apply as they move through this journey?*

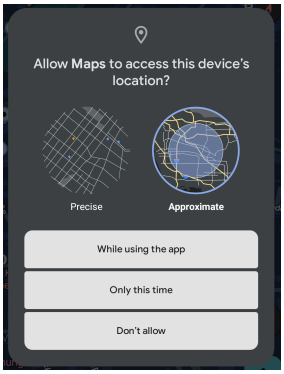
Our findings indicate that understanding mobile privacy decisions requires looking beyond the immediate cues (i.e., rationale messages) presented in apps. Users' permission-granting decisions emerged from a combination of personal context, individual traits, peer influence, and past encounters with data security. This journey is not linear; rather, it is a combination of these elements to shape permission choices. For example, a peer-trust driven journey often begins when a participant adopts an app recommended by friends or family. This early endorsement builds confidence that later overrides hesitation when the permission prompt appears. As our analysis reveals, users follow patterned trajectories, which we describe as *archetypes*. These archetypes are characterized by early motivations, such as peer trust, external mandates, incentives, or alternative information sources, which systematically influence their perceived trade-offs, privacy thresholds, and contextual expectations. Based on these findings, our paper makes the following contributions:

1. **First**, we reconceptualize permission granting as a sequential, path-dependent process rather than a discrete interaction at the prompt. We empirically map how *discovery, exploration and selection, installation, and permission granting* unfold in practice (addresses *RQ1*). We also show how earlier cues, such as *peer recommendations, incentives*, or *app type*, shape later privacy expectations and narrow possible choices. This offers a structured account of how users arrive at permission decisions, addressing gaps in prior work that treated permissions as moment-level events.
2. **Second**, we introduce a set of *archetypal user journeys* that reveal distinct mechanisms through which privacy decisions form. These archetypes illustrate how different combinations of contextual factors (e.g., social trust, institutional mandates, economic

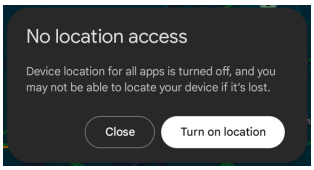
incentives, community vetting) generate predictable trajectories of evaluation and permission granting. The archetypes address *RQ1–RQ3* by demonstrating how cross-stage influences and pre-installation perceptions converge into final privacy choices.

3. **Third**, we contribute a process-oriented framework for sequential privacy decision-making that operationalizes how cost–benefit evaluations unfold across stages of the mobile user journey. By situating users' permission responses within the motivations and expectations formed earlier in the process, this framework clarifies *why* permission outcomes often diverge from the logic assumed by existing privacy instruments. While grounded in qualitative data, these insights identify points in the journey where interventions may hold promise and suggest directions for research methodologies that better capture the full spectrum of the user experience.

Taken together, this paper presents a journey-based account of mobile permission granting that connects fragmented findings into a coherent, process-oriented framework of decision-making. Our archetypal journeys provide a concise lens for studying mobile privacy as an evolving user experience, highlighting opportunities for designing privacy interventions that better align with real-world decision-making processes.



(a) Android Runtime Permission



(b) Rationale

Figure 2: a. Android runtime permission prompt requesting location access for the first time the Maps application is used, presenting multiple decision options. b. Rationale message providing additional context to encourage enabling location services.

2 Background

This section outlines the conceptual foundations that inform our study: the notion of the user journey and the Android runtime permission model. Together, they provide the necessary context to understand the stages of mobile app interaction and the associated privacy considerations.

2.1 Concept of User Journey

The user journey, or journey mapping, describes the sequence of steps users take to achieve a goal, combining their actions, thoughts, and emotions into a coherent experience [25, 50]. Originating in marketing and service design [40, 46, 61], the approach was later adopted in HCI to analyze interactions across multiple touchpoints within a system [20, 52, 53]. By visualizing what users do and feel at each stage, journey mapping helps identify key moments that influence engagement, satisfaction, and decision-making [62]. This holistic perspective moves beyond isolated usability issues, offering a structured lens to examine the interconnected steps that shape user experiences.

2.2 Runtime Permission Model

Modern mobile platforms employ a runtime permission model [4, 64, 73], which requests user consent when an app requires access to sensitive data, such as location or the microphone. These prompts often include a brief rationale explaining why access is needed [41]. Figure 2 illustrates an example of this process. The prompt is the final step before the user decides whether to share their data. The runtime permission model is designed to enhance user privacy choice by providing contextual awareness and control over data access decisions.

3 Related Work

Prior studies have identified a range of influences on permission behavior, including demographic factors [6, 9, 64], cultural contexts [13], and the timing and framing of rationales [17, 18, 66] as illustrated in Figure 3. While these studies offer important insights, each focuses on a single element of the decision-making process and offers little insight into how users move from recognizing the need for an app to ultimately responding to its permission request. In the following, we review prior works across key themes, including Android's runtime permission model, factors affecting permission-granting decisions, and existing privacy theories.

3.1 Users

Understanding users is key to examining permission-granting, as individual characteristics often shape how such decisions are made. Prior research [6, 9, 64, 66] has demonstrated that demographic factors, including age, gender, and education, can influence permission-related behavior. Beyond demographic differences, cultural background, personal attitudes toward privacy, and contextual understanding also influence how users respond to permission requests [13, 42]. In a large-scale study, Cao et al. [13] found that denial rates varied by country (e.g., 12% in the U.S. versus 25% in Argentina), highlighting that cultural factors play a significant role in shaping user behavior. In addition to cultural effects, individual privacy attitudes and education also affect user judgments around permissions [9, 64]. Together, these findings indicate that permission-granting decisions are shaped by a range of individual factors rather than being uniform across users. However, prior work examines these influences in isolation, leaving open the question of how such user characteristics interact with the broader sequence of steps leading to a permission decision.

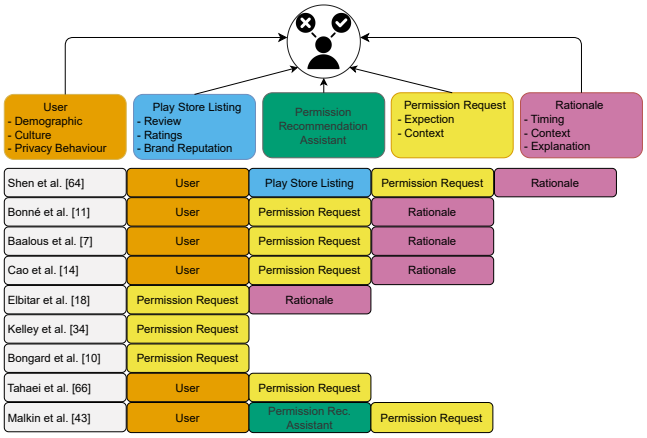


Figure 3: A summary of factors considered in prior research on mobile app permission decisions. The top row provides an overview of factors identified in previous research that influence a user's decision to grant or deny a permission request. The table below visually demonstrates that a significant portion of existing research has predominantly focused on the Permission Request and Rationale factors.

3.2 External Factors

In addition to user characteristics, permission decisions are shaped by external factors—information sources and cues that originate outside the app interface itself. Android encourages developers to include app descriptions, data safety sections, and privacy policies in Play Store listings to promote transparency. Yet, Liu et al. [41] observed that rationales often do not match app descriptions, creating inconsistencies with real permission requests. Such discrepancies may undermine trust in developer-provided information and push users to seek alternative guidance. In line with this, Shen et al. [64] demonstrated that users consider external factors, such as reviews, app ratings, and brand reputation, which lie outside the app interface but shape perceptions of credibility, trustworthiness, and privacy risk when deciding on a permission request. Furthermore, these external cues not only influence users but also affect developer behavior. For instance, Nguyen et al. [49] reported that 60.77% of privacy updates were driven by feedback contained in user reviews. While these works reveal the importance of external signals, they do not examine how users integrate these cues across the broader sequence through which users reach a permission decision.

3.3 Permission Request

Mobile applications must request permission from the user when a feature requiring such access is used for the first time. Earlier studies [6, 9, 13] have shown that permission-granting decisions can depend on the type of permission requested. Baalous et al. [6] found that users were more likely to deny permissions they perceived as sensitive (e.g., microphone, camera, location)—permissions they feared could allow apps to listen, track, or record without consent. Similarly, Cao et al. [13] reported higher denial rates for permissions commonly viewed as dangerous, such as the microphone, calendar, and contacts.

Beyond sensitivity, users' expectations also shape their decisions. Prior work has consistently documented a mismatch between the permissions requested by apps and what users believe these apps should need [8, 9, 13, 22, 33, 74]. This mismatch often leads to discomfort and uncertainty, which in turn reduces user confidence. Importantly, these studies focus on the moment of the request, leaving open how expectations themselves develop earlier in the user journey.

Cao et al. [13] reported that unexpected permissions were twice as likely to be denied as expected ones, indicating the importance of aligning permission requests with user expectations. However, users frequently have limited awareness of the permissions they have already granted [58]. Shen et al. [64] reported that only 6.1% of users accurately understood permission group scopes, with many either overestimating or underestimating their capabilities.

To address these challenges, researchers have explored ways to improve the presentation and comprehension of the permission. Studies show that presenting permissions in a way that feels natural [17] and providing contextual information [74] can enhance understanding. Yet, these interventions focus on the point of interaction rather than on how user assumptions and expectations evolve across earlier stages of app adoption.

3.4 Permission Rationale

Android encourages developers to include rationales— brief explanations alongside permission prompts [4], particularly for sensitive data such as location, microphone, or camera access [2, 13]. Prior work shows that these explanations can meaningfully reduce denial rates (7.1% vs. 15.4%) [13], yet their effectiveness varies with both timing and contextual relevance [18].

A recurring challenge is that many rationales provide only partial information. For instance, developers often emphasize the functional benefits while omitting details about what data is collected or how it will be used [67], leaving users with an incomplete understanding [64]. The linguistic framing also plays a role. Studies [17, 64] highlighted that negatively framed messages that foreground potential risks tend to exert stronger influence than positively framed ones. Timing further shapes outcomes. When rationales appear at the moment an app requires the permission, they yield the highest acceptance rates (around 92%), compared with substantially lower rates (about 74%) when requests are presented upfront without accompanying explanations [17, 18]. However, these studies examine rationales in isolation, rather than situating them within the broader context of the full user journey.

3.5 Process Oriented Perspective on Privacy

Scholars have long theorized that privacy decision-making is a dynamic and context-dependent process, rather than a single discrete act. The Privacy Calculus (PC) [15] theory highlights how individuals weigh perceived risks and benefits when making privacy-related decisions. While it captures the essence of this privacy decision process, it offers limited insight into how such judgments evolve over time or across different stages of interaction. Likewise, Nissenbaum's theory of Contextual Integrity (CI) [51] conceptualizes privacy through the norms governing information flows, emphasizing that expectations depend on social and institutional context.

However, it provides little guidance on when these expectations form, how they shift as users encounter new cues, or how earlier interpretations constrain later decisions. Related work in HCI echoes this process-oriented view (see Section 2.1). Morton and Sasse describe privacy as a layered, ongoing practice shaped by users' interpretations at successive moments [47], while Wang et al. apply privacy calculus theory to users' intentions to disclose information via mobile apps in a bounded decision context [72]. However, neither perspective has been operationalized to examine how users navigate the full sequence of app adoption, starting from finding an app to evaluating it, installing it, and ultimately responding to permission prompts.

Existing studies in mobile privacy also have rarely aligned with these two theoretical models as they only consider isolated factors or steps like the timing and framing of rationale messages or the permission requests (see Section 3.1- 3.4).

This leaves two notable gaps: the absence of an empirically grounded work that links pre- and post-installation decisions into a unified process, and the lack of work that situates PC and CI across the full progression of app adoption. Our study makes the first important steps to address these gaps by examining privacy decision-making as a sequential, cross-stage process and how early cues (PC) accumulate and inform later choices (CI).

4 Method

To explore our research questions, we conducted semi-structured interviews with Android smartphone users to collect detailed insights into their app user journey, while keeping the conversation open enough to explore emerging themes. Our approach was exploratory, given the limited understanding of how users move from an initial app need to ultimately making a permission-granting decision.

We recruited participants who primarily use Android devices, as this aligns with our study's focus on permission-granting practices within Android's ecosystem. Android's open ecosystem enables granular data collection and analysis of user behaviors, permissions, and security practices, unlike iOS, where restrictive APIs and sandboxing limit observational research [19, 71]. Additionally, Android's dominant global market share (≈72% as of 2025) [65] and diverse device landscape also provide a more representative sample for privacy research [9, 13], since findings are grounded in the ecosystem where the majority of mobile permission interactions take place. We discuss the limitations of our method in Section 6.6. Our overall study setup is outlined in Figure 4.

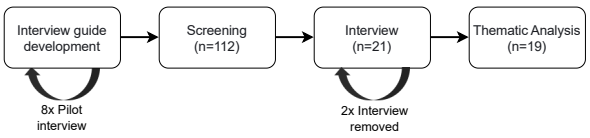


Figure 4: Overview of our recruitment and analysis approach

4.1 Interviewing procedure

We developed an interview guide as a flexible protocol to guide the data collection process. The guide was iteratively refined throughout the study, incorporating insights from earlier interviews and shifting the focus toward newly emerging topics as they arose. When participants introduced issues spontaneously, we followed their lead and adjusted the sequence of questions to explore these areas in depth. Despite this flexibility, the guide retained a consistent core set of topics that was explored with all participants. These topics covered their general smartphone use; what they typically do when they need a new app, both in general and for different app categories (e.g., banking vs. shopping apps); where they usually obtain apps; what information they review before downloading an app; and any concerns they have about app-related privacy. We ensured that participants described their user journeys in their own words without being prompted with specific steps. Only when a topic did not arise spontaneously did we introduce gentle cues to explore it further. This combination of structure and adaptability aligns with qualitative research best practices, which emphasize responsiveness as a means of enhancing data richness and validity [37, 75].

4.2 Pilot Study

We conducted two iterative pilot rounds to refine the interview guidelines and ensure comprehensive coverage of the user journey. The first pilot involved five participants recruited from university lists and internal student workers who were not involved with the project. During these initial interviews, we observed that participants were frequently unfamiliar with the app store's Data Safety Section and seldom mentioned secondary phone use or sideloading apps without prompting. To better capture these potentially relevant but less spontaneously reported behaviors, we incorporated brief demonstrations of the Data Safety Section and added explicit, neutrally phrased prompts about secondary phone use and sideloading in the revised interview guide.

A second pilot with three Prolific [59] participants confirmed that these refinements improved the interview flow and clarity without leading to biased responses. Importantly, these prompts were designed to encourage recall rather than guide opinions, preserving participants' original perspectives. Data from both pilot phases were excluded from analysis to maintain the integrity of the main dataset. The finalized interview guidelines are provided in Appendix C.

4.3 Sampling and Recruitment

To sample and recruit interview partners, we first distributed a screening survey via Prolific [59]. In this survey, we 1. asked for participants' willingness to take part in an online interview session and 2. collected information relevant to selecting suitable interview partners. In addition to demographic information, we collected self-reported data on participants' app download frequency, their tendency to download apps or APKs outside of the Google Play Store, the frequency of such downloads, and the approximate number of APKs they had downloaded. We also measured participants' security attitude using the SA-6 scale [21].

All participants were recruited from the United States to ensure a more homogeneous context for examining the mobile user journey.

Table 1: Participant Demographics

PID	G	Age	Education	IT	SL	SLN	SA-6
P1	M	35	HS Diploma	❍	●	3	4.33
P2	F	56	HS Diploma	❍	●	3	3.33
P3	M	28	HS Diploma	❍	●	1	2.66
P4	F	48	HS Diploma	❍	❍	0	3.00
P5	M	36	Bachelor's	❍	❍	0	2.16
P6	M	75	HS Diploma	❍	●	8	4.66
P7	F	61	HS Diploma	❍	❍	0	3.83
P8	M	68	Master's	●	●	6	3.83
P9	M	52	Associate	●	●	10	4.83
P10	M	38	HS Diploma	❍	●	2	3.66
P11	F	34	Doctoral	❍	●	200	3.50
P12	F	50	HS Diploma	❍	❍	0	1.66
P13	M	58	Bachelor's	❍	❍	0	4.50
P14	F	50	Bachelor's	❍	❍	0	2.33
P15	F	53	Master's	❍	●	3	4.33
P16	M	37	Bachelor's	❍	❍	0	3.66
P17	M	25	HS Diploma	●	●	50	2.66
P18	N	23	Bachelor's	❍	❍	0	1.66
P19	N	25	HS Diploma	❍	●	6	1.83

Legend:
G: Gender (M=Male, F=Female, N=Non-binary); **IT**: IT background (●=Yes, ❍=No); **SL**: Sideload (●=Yes, ❍=No); **SLN**: Number of Sideloaded apps; **SA-6**: Security Attitude Score [21]; **HS Diploma**: High School Diploma or Equivalent.
SA-6 Interpretation (U.S. population sample): < 3.57 = much lower than average; 3.57–3.99 = close to average; > 3.99 = much higher than average.

Limiting the study to one country minimized confounds related to device availability, platform popularity [1], and cultural variations that could influence privacy perceptions [13]. Prolific users were eligible only if they held a U.S. account, had a minimum approval rate of 95%, and were fluent in English.

We first applied Prolific's standard sampling filters based on our recruitment criteria (see Appendix A) to identify suitable participants. Respondents then completed a prescreening survey (see Appendix B) via Qualtrics [60], yielding 112 responses. After data quality checks, we excluded iPhone users and responses flagged by Qualtrics as duplicates or potentially fraudulent, resulting in 74 eligible participants. Although an "Android mobile OS" filter was used on Prolific, 38 respondents reported using iPhones, likely due to outdated profile information. Interview invitations were then distributed iteratively across four recruitment pools, and 6 participants withdrew before scheduling could occur. Applying our inclusion criteria—aiming for diversity in security attitudes [21], education, technical background, and sideloading behavior—yielded 21 qualified participants. Two interviews were later excluded due to connectivity issues, resulting in a final dataset from 19 interviewees (10 male, 7 female, and 2 non-binary). See Table 1 for the demographics of our final dataset.

4.4 Data Collection

We conducted 19 interviews, each lasting between 22 minutes and 66 minutes, totaling 737 minutes (with an average duration of 38.8 minutes). Variation in interview duration primarily reflected individual communication styles and levels of elaboration. Some participants offered concise responses, resulting in shorter sessions (*P19, duration 22 min.*), but all interviews followed the same semi-structured guide, and every core topic was covered in full, ensuring data completeness. Interviews were conducted via Zoom, with both audio and video recorded. However, only the audio files were transcribed and analyzed. Video recording served two purposes: first, it enhanced participants' engagement, created a sense of social presence and credibility through eye contact, and second, it allowed us to verify that no disruptions or technical issues affected data quality, consistent with online interview best practices [26, 54]. Participants could choose whether to enable their camera, and three participants opted to keep it off. Only the interview session was captured, and all recordings were managed in accordance with our ethical procedures (see Section 4.6).

4.5 Data Analysis

We analyzed the interviews using thematic analysis [11, 70], which is well-suited for exploratory studies that aim to capture end-users' perspectives and has been widely applied in related works [7, 10, 24, 28]. Our process followed the six-phase framework introduced by Braun and Clarke [11].

First, the audio recordings were transcribed verbatim by a GDPR-compliant transcription service [57]. To begin coding, three researchers independently analyzed the same four transcripts using an inductive, bottom-up approach inspired by open coding. Afterward, they met to compare their coding outcomes and discuss differences in interpretation. Subsequently, the two primary researchers continued by coding two more transcripts, then met to reconcile any discrepancies and jointly constructed an initial version of the codebook. This preliminary codebook was applied to two additional interviews, with the researchers meeting weekly to review disagreements and refine code definitions. Iterative refinements led to the finalized codebook used for the remaining transcripts.

During the analysis process, the researchers created analytic memos and summaries to document reflections and track emerging ideas. Codes were then organized and connected axially to explore their relationships, facilitating the development of broader themes and subthemes using thematic analysis [11, 70]. Throughout this stage, we repeatedly revisited the transcripts to ensure that interpretations remained grounded in participants' accounts. Data saturation was assessed through ongoing weekly team discussions during analysis. Saturation was operationalized as the point at which coding successive interviews yielded no new codes or subthemes beyond those already represented in our evolving codebook (i.e., not a relabeling or refinement of an existing code). We declared saturation when the codebook remained stable across successive interviews; this point was reached after coding 13 interviews. Coding disagreements were resolved through discussion until consensus among coders, with decisions documented by updating the shared codebook and revisiting affected transcripts. To verify this observation, six additional interviews were coded and analyzed, confirming codebook stability and that no new codes or subthemes emerged, which indicated that saturation had been reached. In total, our analysis produced six main themes and eighty-nine subthemes (*see Codebook in Appendix D*).

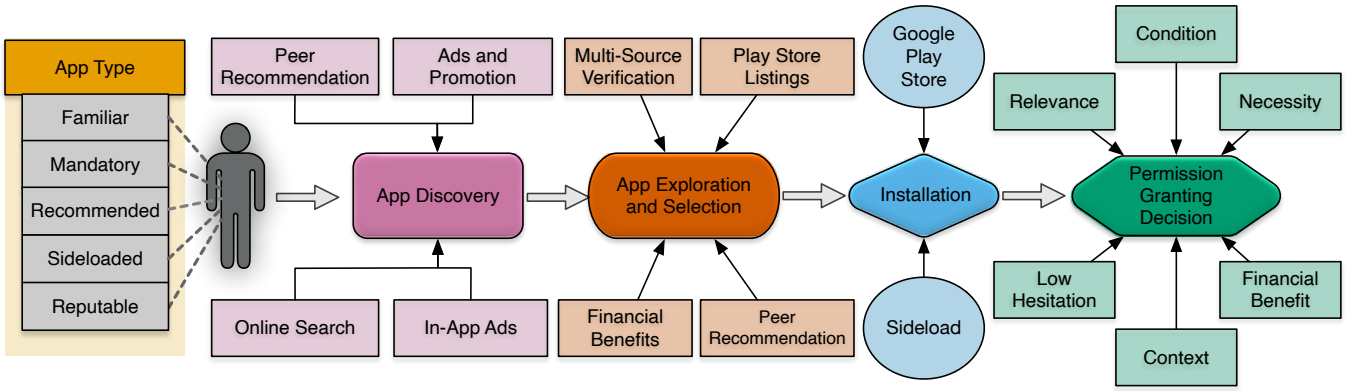


Figure 5: The mobile user journey from app discovery to permission-granting decision. This diagram highlights four stages: discovery through peer recommendation, search, or promotion; exploration and selection via multisource verification, Play Store listings, or financial benefits; installation through the Play Store or sideloading; and finally, permission decisions shaped by relevance, necessity, financial benefits, or contextual considerations. The app type is not directly linked to the user journey, but it is one of the catalysts that drive the journey.

These themes informed the structure and emphasis of the *Results* and *Discussion* sections. While not every theme appears as a standalone topic in the final narrative, the majority contributed to the interpretation of key findings and arguments, for example, themes related to the user journey, sideloading practices, and app types. Other themes, such as those capturing individual user traits, supported contextual understanding and analytic depth but were not treated as central analytical points. This selective integration reflects established qualitative practice, where themes serve as analytic scaffolding rather than a one-to-one outline for reporting. We did not calculate inter-rater reliability; instead, the two main researchers held weekly meetings to resolve differences and update the codebook until a consensus was reached, consistent with best practices in qualitative research [35, 43, 55].

4.6 Ethical Considerations

Interviews were conducted via Zoom. Participants received compensation at a rate of £9.60/hour for completing the brief pre-screening survey and £20.00/hour for participation in the interview.

Both audio and video were recorded during the sessions to support clear communication and maintain an accurate record of the interview; however, only the audio recordings were used for transcription and analysis. Video files were permanently deleted immediately after each interview. Audio recordings were transcribed, anonymized, and subsequently deleted once transcription was complete. Throughout the research process, we minimized the collection of personally identifiable information (PII), restricted access to non-anonymized data to a small number of researchers, and ensured that all data storage and processing complied with GDPR requirements.

The study posed minimal risk to participants, focusing solely on general smartphone usage patterns. Participants were encouraged to express any discomfort with particular topics and could withdraw at any time. No participants chose to discontinue their participation, and all appeared comfortable discussing their experiences. All participants provided informed consent prior to the interview and were debriefed at the end.

All procedures in this study received approval from our university's Ethical Review Board (ERB), which reviewed and approved the study design, survey materials, and interview guide. The study adhered to the ethical principles set forth in the Menlo Report [16].

5 Result

We present the themes that emerged from our thematic analysis. These themes illustrate how participants interpreted the available information, navigated alternative options, and made choices across the user journey. To indicate the prevalence of each theme, we use qualitative frequency descriptors tied to participant counts in our sample of 19 interviews.[1] Our aim is not to generalize beyond our study context but to surface patterned dynamics that characterize how participants encountered, evaluated, and ultimately responded to permission requests.

Our analysis shows that decisions around *'Allow'* or *'Deny'* do not emerge at a single moment but unfold across a journey with distinct yet interlinked phases: ***app discovery, app exploration and selection, app installation, and permission-granting decision (PGD)***.

We begin by examining how this journey starts and how participants first encounter mobile applications. We then describe each step of the journey, followed by the privacy strategies participants adopted and the factors that influenced their decisions. Finally, we describe archetypal variations that highlight alternative pathways shaped by contextual factors. Figure 5 provides a visual overview of the user journey and its core components.

5.1 Factors Shaping the User Journey

The user journey starts with the desire for an app. This initial motivation, whether functional, social, or situational, served as a catalyst that pushed users to seek out applications that could fulfill

[1]We define the descriptors as follows: *a few* (0–3 participants), *some* (4–7), *about half* (8–11), *many/most* (12–15), and *almost all/all* (16–19). This mapping follows prior qualitative research [27, 29, 30].

their goals. Participants consistently emphasized the centrality of mobile phones in their everyday lives and described a wide range of app-dependent activities from work and shopping to navigation and entertainment.

> *"I do everything with my phone. Literally everything. Work, social media, crypto, you name it."-P9*

Across interviews, distinct types of apps emerged as influential entry points that shaped how the journey unfolded. For instance,

- **Familiar Apps –** applications that the user already knows or has used before.
- **Mandatory Apps –** applications that users feel obligated to install due to the necessity to take the service, i.e., Banking App.
- **Recommended Apps –** applications suggested by others (friends, experts, systems) for specific purposes.
- **Reputable Apps –** applications with strong reputations, often from well-known developers or companies.
- **Sideloaded Apps –** applications installed from outside the official Google Play Store, typically in APK format.

These app types did not constitute steps in the journey but acted as early frames that conditioned expectations, trust, and the degree of scrutiny participants applied later. We discuss each type below. We further examine the implications of these app types in Section 5.4.

5.1.1 Familiar Apps. About half of the participants (n = 9; P1, P3, P9, P10, P13-P15, P18, P19) described relying on apps they had previously used. They highlighted that familiarity served as a shortcut, simplifying choice, reducing uncertainty, and diminishing the need to reevaluate the app's legitimacy or permissions, as they already trusted the app from previous experience.

> *"Since I've already used it in the past and I typically won't really read the description of the apps when I have already used them before."-P3*

Familiar apps illustrate how trust can accumulate over time and carry forward, effectively pre-structuring later stages of the journey.

5.1.2 Mandatory Apps. Some participants (P4–P6, P12, P13, P15, P17) adopted apps because external institutions required them to do so. These included banking, workplace, school, or service-provider applications (e.g., youth sports communication platforms). In such cases, participants framed installation as obligatory rather than elective. For example, P15 noted, *"Sometimes they'll say download our app or some things you can't do on the website [...], you have to download that."* Mandatory apps constrained their decision space. Participants described compliance as the only viable option, which later reduced resistance at the permission-decision stage.

> *"A lot of times with our kid for like sports, youth sports and stuff they'll have specific communication apps we need to download to get information updates."-P5*

5.1.3 Recommended Apps. Social recommendations played a significant role for almost half of the participants (n=9). Friends, family, colleagues, or trusted communities influenced app choices, with recommendations functioning as a transfer of trust. For instance, P11 recalled, *"Admittedly, I do get a little bit more relaxed with it. Like I don't do as crazy checks because I assume that my husband, or my friend, has gone through the same process I do."* Almost half of our participants (n=9; P2, P5, P8, P11, P13-15, P18, P19) echoed this pattern.

> *"Similarly, the people I know on the mailing list, I have years of depth of interaction with them. [...] And I typically am installing apps only that have been recommended by someone that I feel I have some personal connection to."-P8*

These social recommendations offered a perceived safety layer, demonstrating how interpersonal trust can serve as a substitute for technical scrutiny.

5.1.4 Reputable Apps. Some participants (n=7; P2, P3, P10-13, P15) emphasized app reputation, often equating it with recognizable companies or established brands. Reputation operated as another heuristic for quality and safety. Apps associated with well-known companies or strong brand recognition were often described as reputable.

> *"Well, before I download, I have to make sure that it's a reputable site. I have to make sure that I'm not going to download anything that's like a brand new company that nobody's heard of."-P2*

Here, brand recognition substituted for detailed evaluation, revealing how institutional trust shapes early filtering.

5.1.5 Sideloaded Apps. About half of our participants (n=8; P1, P3, P6, P9, P10, P15, P17, P19) described situations where they needed apps that were not available in the official Play Store. Motivations included missing features, unavailable services, or avoiding payment for premium apps. According to P6, some premium apps that cost money on the Play Store were freely available elsewhere, prompting him to sideload. Participants acknowledged the security risks involved in sideloading apps but justified the practice as a calculated trade-off.

> *"[...] I couldn't like a function that I just wasn't offered on the play store at all. So I kind of had to just trust that it was going to be okay, just because I took the gamble and just decided I needed that function. So I took a risk."-P1*

Sideloading reflects a different logic of decision-making where functional needs override security norms, and risk is reframed as an acceptable trade-off.

Key Takeaway

The need for an app initiates the journey, but identifiable app types, such as familiar, mandatory, recommended, reputable, and sideloaded apps, quickly shape how the journey unfolds. These types function as early heuristics that influence trust, scrutiny, and risk tolerance. Familiarity and reputation provide a sense of safety, recommendations transfer trust from peers, mandatory apps constrain choice into compliance, and sideloading reflects calculated risk-taking for access. As a result, **many permission decisions are effectively pre-conditioned long before the prompt appears, underscoring how initial contexts structure downstream behaviors.**

5.2 The User Journey

The following themes, derived from our interview analysis, illustrate how participants' experiences gradually connect across the user journey. Each block represents a stage in the journey where users interact with different facets of mobile apps and privacy decisions. The journey unfolds across four primary stages: *App Discovery, App Exploration and Selection, Installation, and Permission-Granting Decisions (PGD).* Within each stage, we also identified several subthemes that represent specific pathways or factors shaping users' actions. Depending on the app type, some stages may be skipped. For example, users sometimes move directly from *app discovery* to *installation*, as we illustrate later in the *archetypal journeys* (in Section 5.4). We conceptualize these stages as connected moments of sensemaking, where earlier assumptions, needs, and contextual cues shape what users notice and prioritize next. The findings reveal that these moments build upon one another, forming consistent patterns that shape how participants ultimately approach permission decisions.

- **App Discovery** captures how users first become aware of applications. Key subthemes include peer recommendations, website searches, in-app advertisements, and promotional campaigns, among others. These subthemes reflect the diverse ways users encounter apps before any evaluation or engagement.
- **App Exploration and Selection** represents the evaluative phase where users assess app details, security factors, and make informed choices. Key subthemes include review analysis, app descriptions, ratings, and reputation, among others. These elements shape users' confidence, perceived risk, and overall decision-making before installation.
- **Installation** is the practical step of downloading and installing the chosen application.
- **Permission-Granting Decisions (PGD)** reflects the stage where users respond to runtime permission requests and decide whether to grant or deny access to sensitive resources. Key subthemes include perceived necessity of permission request, trust in the app, privacy concerns, and risk assessment, among others. This stage exposes how earlier expectations and heuristics surface during privacy-relevant choices.

We discuss each theme in detail in the following sections.

App Discovery

In our study, participants described various ways they discovered applications, often starting with peer recommendations, social media advertisements or campaigns, and browsing online sources. These encounters marked the starting point of their journey toward further evaluation. App discovery, therefore, emerged as a socially and digitally mediated process, where exposure through different means often prompted participants to explore apps further. Across participants' narratives, the discovery functioned less as a neutral starting point and more as an initial filter, shaping which apps users perceived as trustworthy, familiar, or worth further effort.

Peer Recommendation. Participants often learned about new apps from friends, family members, or colleagues. P8 noted, *"I am slow to download. I do it infrequently. Mostly it's on word of mouth. It's personal recommendation from someone whom I know."* About half (n=10; P5, P7-9, P11-15, P18) of our participants reported this pathway. These accounts illustrate how interpersonal trust can substitute for technical scrutiny and set the tone for subsequent exploration. When the recommender is trusted, participants often proceed to the next stage with heightened confidence and a lower perceived risk.

Online Search. Participants also used online searches, such as Google Search and Reddit, to find new apps. P5 described a process shared by half of our participants (n=11; P1-3, P5, P6, P8-10, P12-14), *"If I want something more specific, I typically utilize a Reddit search, [...] because I feel there are threads in there, people discussing more specific apps [...]."* These searches often reflected active information seeking, especially when participants had specific functional needs or desired community validation.

Some participants found apps directly through services they previously used on other platforms, including cases where apps were unavailable on the Play Store. As one participant shared:

> *"I had used Adult Friend Finder on a browser [...] they said, we've got an app now. But it wasn't in Google Play. [...] We'll send you the link."– P12*

Similar experiences were reported by half of the participants (n = 8; P1, P3, P6, P9, P10, P15, P17, P19). While some participants were encouraged by the service provider to download an external app, a few reported finding apps independently on websites when they were unavailable on the Play Store, for instance, to access a free version or a specific older release. These examples show how platform absence did not deter motivated users. Instead, prior familiarity with a service often justified bypassing conventional safeguards to use third-party downloads.

Ads and Promotions. Participants also discovered new apps through social media, TV ads, and promotions. They reported that regular exposure to these ads often led them to download the advertised apps. P4 noted, *"Sometimes I'll see like new apps through different types of social media or even on TV. And if it looks interesting, I'll download it."* Half of the participants (n=10; P1, P7, P9-12, P14, P15, P18, P19) described similar experiences.

These pathways demonstrate how repeated exposure can normalize apps that participants had no prior intention of exploring. Ads functioned as background cues that gradually shifted perceptions of relevance and further exploration.

In-app Ads and Play Store Browsing. Participants reported being exposed to new apps through in-app ads.[2] Some noted that these ads appeared while using other applications, particularly games, and often sparked their curiosity to try something new. As P14 explained, *"I generally find new games through ads. They'll send me in because I play the games that have ads in them. [...] And then from there, all I do is just click install."* Participants also browsed categories on the Play Store to find apps. For example, one participant shared that they used a random search by category to find a new app to try out, and noted that,

[2]In-app ads are targeted advertisements within mobile applications that use user data to display relevant promotions and generate revenue for developers. [48]

> *"I'm just wanting to find a fun game to download and install. So I'll just kind of scroll through and look at the different games in the category of game apps that are on the Google Play Store [...] then download it.-"P3*

This reflects a self-guided approach, where participants actively browsed categories to discover apps, while some (n=7; P5-7, P9, P10, P12, P13) engaged in a try-and-test approach rather than relying on ads or promotional recommendations. This exploratory behavior suggests that some users treat app discovery as a low-stakes, iterative process guided by experimentation rather than deliberate evaluation.

Key Takeaway

App discovery operates as an early filter that shapes how users approach all subsequent stages of the journey. Social recommendations often transfer trust directly into the process, online searches support targeted problem-solving, and advertisements create repeated cues that normalize unfamiliar apps. These discovery pathways do more than introduce options; **they form initial expectations that influence later scrutiny, trust formation, and ultimately permission decisions.**

App Exploration and Selection

After discovering new applications, participants described employing various strategies to determine whether the app was worth installing. This stage reflected a process of diverse considerations and involved a mix of verification, reassurance, and motivation before making a final decision to proceed with the app. Across participants, this stage served as a critical filtering point, determining which discovered apps progressed toward installation, and addressing how early exposures shape later steps **(RQ1, RQ2)**.

Multisource Verification. Participants often used online communities such as Reddit, YouTube, tech blogs, or discussion forums to verify an app's credibility before selecting it. They described this cross-checking as a way to validate trustworthiness and align with their expectations, as P5 highlighted: *"If I'm wanting to download an app that's already in the Google play store, sometimes I'll watch YouTube videos and see what other people are saying about the apps."* Many reported rarely relying on a single source of information. Instead, they compared opinions across platforms to make more confident choices. As P6 explained:

> *"Look for reviews of that from reputable sources, PC Magazine in the US, or there's other internet sites, and Android reviewers that do reviews of apps and see if they have that same logo and then make sure that I've got the right one from a trusted source."-P6*

This pattern was echoed by most participants (n=15). Such cross-checking became more pronounced for unfamiliar or higher-risk apps, indicating that exploration intensity scaled with perceived sensitivity. In contrast, everyday or well-known apps required minimal verification, demonstrating how familiarity reduced cognitive effort during exploration.

Play Store Listings. Our thematic analysis showed that the Play Store played a central role in shaping exploration and evaluation before participants considered app selection. User reviews, star ratings, and download counts served as quick indicators of quality and trust, which helped participants filter out less reliable apps. Many of our participants (n = 15; P1-9, P11, P13-15, P18, P19) reported that they routinely checked these cues before making a decision to download the app. They also noted that low download counts or a run of negative reviews were taken as signals of poor quality, with P4 remarking: *"There's nothing more truthful than listening to people's actual complaints in the reviews."* In such cases, participants reported that they preferred to move on and look for alternative options, as remarked by P15, *"I definitely am not going to download anything with low reviews, low star rating."*

Participants also differentiated between heuristics used for simple utilities and those used for sensitive apps. For high-risk categories (e.g., VPN apps), they combined multiple Play Store cues to reduce uncertainty, illustrating how exploration becomes a risk management process rather than a simple preference matching process.

Some participants followed workplace requirements or service obligations even when ratings were low, treating the installation as a matter of compliance rather than a personal choice. These exceptions show how contextual constraints can override the usual selection logic, which helps explain why certain apps advance despite low trust signals.

A few participants (n=3; P3, P6, P11) also paid attention to Play Store credibility cues, such as app icon, verified badge, or 'Editor's Choice' label, before considering an app among the available options. For example, P11 emphasized: *"I always like when it comes to any type of app that I download, I always want to double check to make sure that it's verified and it's not a scam."*

Many participants reported limited understanding of technical terms in privacy policies, leading them to ignore these cues. About half (n = 9) reported skipping them due to a lack of understanding or excessive length. As P7 noted, *"I don't know what to do about it because I don't know that much about it. It would be good to have like a basic education on data privacy and how to use your technology without exposing yourself."*

Furthermore, almost all (n=18) participants also tended to skip the DSS, either because they overlooked it or found it too dense to act on. Consequently, they relied far more on ratings and reviews than on privacy-specific DSS embedded in the Play Store.

This limited comprehension ultimately narrowed their ability to critically assess security claims, pushing them toward readily interpretable surface-level indicators rather than deeper assessments of security or data practices.

Peer Recommendation. In several cases, participants noted that the same peer recommendation that triggered discovery also governed exploration and selection, with participants choosing the recommended app without further comparison. About half of our participants (n=11; P5, P7-9, P11-13, P15-18) described knowing about apps through friends or acquaintances and ultimately downloading and using them. P7 recalled: *"I looked up calorie counters on google and then it gave me a list of ones [...] then a friend was like have you tried this one? And I was like oh and I downloaded it. I like the way it worked. I've been using it ever since."* These cases show that peer trust can effectively compress the exploration stage,

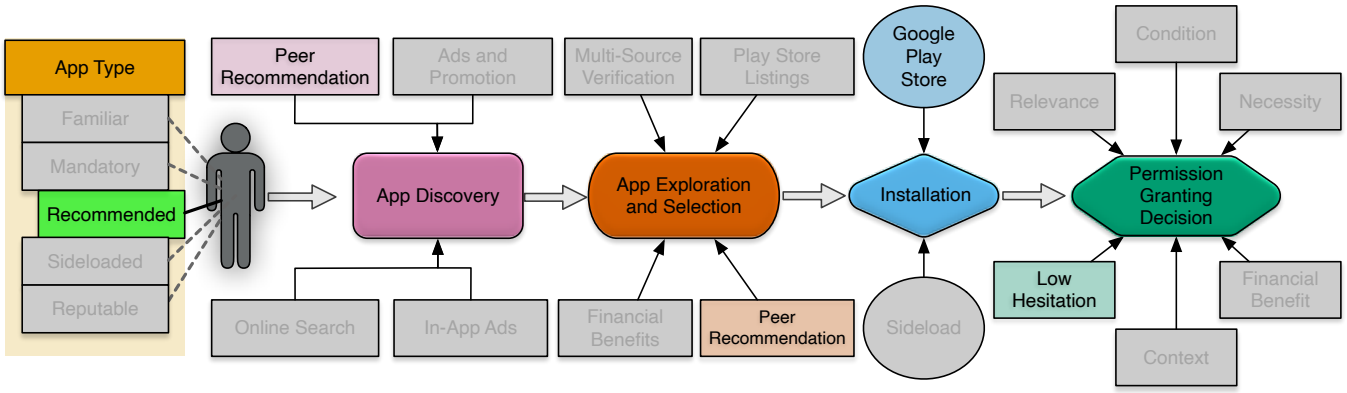


Figure 6: Archetypal Journey Type 1: "Recommended App" with Peer Recommendation. This figure illustrates a journey where the focal app type is a Recommended App, as indicated by the app type on the left. The journey is initiated through peer recommendations, which shape both the Discovery phase and the Exploration and Selection stage. Because the recommendation already provides a trusted basis for evaluation, users move through Exploration with minimal comparison or verification. Installation typically occurs via the Google Play Store, reinforcing expectations of legitimacy. By the time users reach the Permission-Granting Decision, the prior social endorsement reduces hesitation, resulting in a relaxed and largely uncritical acceptance of permissions. Greyed-out elements indicate stages or factors inactive in this journey.

illustrating how social cues can bypass more systematic evaluation. This dynamic also clarifies why discovery mechanisms influence later stages of the journey

Financial Benefits. Exploration was also shaped by potential financial benefits. Many participants (n = 12; P2, P3, P7, P8, P10-13, P15-17, P19) were motivated to try apps that offered coupons, rewards, or promotional points, framing these as added incentives for their selection. One participant explained downloading a shopping app mainly for points that could be redeemed for discounts, noted with

> *"Thing about Target I got their app because they had like a lot of coupons and discounts and special things [...] They'll give you a free carton of ice cream for your birthday [...] so that made me think like why not?"-P10*

Financial benefits served as strong motivators that could override concerns or reduce scrutiny, highlighting how non-privacy factors influence which apps advance toward installation.

Key Takeaway

Participants relied on cues such as ratings, reviews, and app descriptions, but combined them with personal heuristics, including comparing alternatives and seeking trust signals. **Exploration operated as an active filtering stage where users assembled multiple forms of evidence to reduce uncertainty, selectively ignored harder-to-interpret elements like the DSS, and at times moved quickly toward installation when strong social or financial cues were present.** These patterns clarify how exploration mediates the influence of earlier discovery mechanisms on installation decisions.

Installation

Installation emerged as a universal and unavoidable step in the user journey, marking the transition from app selection to use. For all participants, the Google Play Store was the default and most familiar source of downloads. However, participants also described instances where they turned to sideloading when an app was unavailable in the Play Store, when seeking a free alternative to a paid version, or when needing an older release (see Section 5.1.5). In these cases, participants mentioned sources such as F-Droid or other third-party repositories, as echoed in P17's remark:

> *"I get a typical application from the app store. It wants me to pay money. It's going to put ads in my face. It wants me to, it's just gonna, it's like, I'm being marketed to at all times. I get these F-Droid things."-P17*

While the Play Store was perceived as the safer and more convenient option, sideloading reflected a practical workaround when specific needs could not be met through official channels. These deviations demonstrate how installation choices are influenced by earlier exploration constraints, such as affordability or availability, highlighting the interconnected nature of the journey.

Permission-Granting Decisions (PGD)

Our analysis revealed that participants employed a range of strategies when confronted with permission requests. This included evaluating relevance to app functionality, weighing necessity against potential risks, and tailoring accept or deny choices to situational needs. Across accounts, permission decisions reflected a negotiation between practical demands and privacy concerns, illustrating how users move from earlier exploratory heuristics to explicit risk–benefit judgments.

Evaluating Permission Relevance. Participants described several techniques they used to assess whether a permission request aligned with their understanding of the app's purpose. When a requested permission seemed unrelated to the app's intended function, they often became suspicious and were more likely to deny it. This pattern appeared in most of our sample (n=14), as P15 noted:

"When I looked at the permissions, what the permissions made sense, they wanted access to my contacts, which makes sense because I'm going to be texting. I look at it, does it make sense for this app to be asking to have access to this data?" This reasoning demonstrates how participants drew on intuitive models of app functionality to evaluate legitimacy, thereby filling the interpretive gaps left by technical language or explanations.

Necessity. Participants also assessed whether permissions were required for the app to function properly. About half (n = 11; P2-4, P6, P7, P9, P10, P13, P14, P18, P19) accepted permissions they viewed as essential, even when they had underlying concerns. They framed these decisions as constrained choices in which utility outweighed discomfort. As P7 explained:

> *"I don't like it when it does that, but sometimes I let it anyway if I really want to use the app. If I have to do it to be able to use the app and I really want to use the app, I'll let it anyway, even though I don't like it."-P7*

Some (n=4) participants rejected or deleted apps when the permissions seemed excessive or unjustified. As P14 noted, *"I know I needed the camera but it also asked for my contacts and all that. So I ended up deleting that [...] because there's no reason for an ear cleaner or ear scope to need my contact information."* These accounts illustrate a threshold dynamic; once a request crosses a perceived boundary of necessity, users are willing to abandon the app entirely.

Conditional Acceptance based on Context. Participants reported adjusting their decisions based on context, such as whether the app was used for work, leisure, or a specific one-time task. Many described granting permissions temporarily and revoking them afterward, using contextual logic to retain a sense of control. For instance, P6 recalled, *"I did get one of those picture frames [...]. And I had to let them have access to my photos so I could put photos. [...] And if I ever want to put a photo back in the frame again, I'll give them permission for that 10 minutes and then cancel the permission,"* and half of the participants (n=11) expressed similar experiences. A few participants described a flexible or inconsistent pattern, where permission decisions were shaped primarily by the immediate context rather than stable rules. As P3 explained:

> *"Sometimes I'll press allow, sometimes I'll press the other option just basically just to get past that section of what it's asking me so I can use the app."-P3*

These accounts show that permission decisions are not fixed rules but adaptive responses shaped by immediate goals, effort minimization, and perceived reversibility.

Financial Benefits. Some participants (n=7; P3, P10-13, P17, P19) expressed willingness to grant permissions if the app offered tangible rewards, such as coupons, loyalty points, or gift cards. In these cases, the trade-off was considered worthwhile, even if the permissions otherwise felt invasive. One participant noted,

> *"There are receipt apps where you take pictures of your receipts and they give you points. That asks for those permissions so they can analyze everything and then give you credit for cash or gift cards. [...] I've already been through a breach and still I'm out here doing this."-P12*

These cases highlight how financial incentives can recalibrate privacy boundaries, shifting the evaluation from risk avoidance to opportunity maximization.

Low Hesitation. A few participants (n=3, P2, P3, P19) described paying little attention to permissions, treating the prompt as a routine step, and skipping it quickly in order to start using the app. These participants described granting permissions almost automatically, without reflection. P2 shared *"There are times where I'm just like, I use this app all the time. Okay, allow, allow, allow. And then I don't think about it too much."* Several associated this low hesitation with trust in well-known companies or brands. For these participants, familiarity effectively replaced scrutiny, collapsing the permission stage into a near-automatic step.

Key Takeaway

Participants' permission decisions ranged from careful scrutiny to rapid, habitual acceptance. While many evaluated relevance and necessity, others prioritized functionality, contextual convenience, or financial incentives. A small subset treated permissions as trivial, relying on trust in familiar apps or companies. Overall, these accounts demonstrate how users balance privacy concerns with the practical demands of continued app use, revealing **substantial variation in their approach to this final decision point**.

Summary of Insights

In response to **RQ1**, the analysis identifies four main stages in the user journey: app discovery, exploration and selection, installation, and permission granting. These stages are shaped by diverse influences, including app type, social cues, prior experiences, and contextual factors, addressing **RQ2**. Regarding **RQ3**, throughout the journey, participants employed a range of privacy strategies, including verification and selective acceptance, as well as contextual decision-making and routine compliance. **The stages of the user journey are best understood as interconnected rather than strictly linear, forming a cumulative decision context that shapes the final permission outcome.**

5.3 Privacy Strategy

Participants employed a range of privacy strategies across the journey. Examining these strategies reveals the underlying logics that guide decision-making and shows how early cues shape later choices in systematic ways.

5.3.1 Trust in the Company and Brand. Participants frequently grounded their decisions in trust in the company or brand. Well-established organizations, particularly banks and financial institutions, were perceived as inherently safer because participants already trusted them with sensitive information. Many participants (n = 13) highlighted that brand familiarity, a large user base, and positive past experiences reduced their perceived privacy risk. For instance, P5 noted that

> *"I'm trusting this financial institution with my money already and handling my money. So going into it, there's already a large layer of trust with that institution there.*

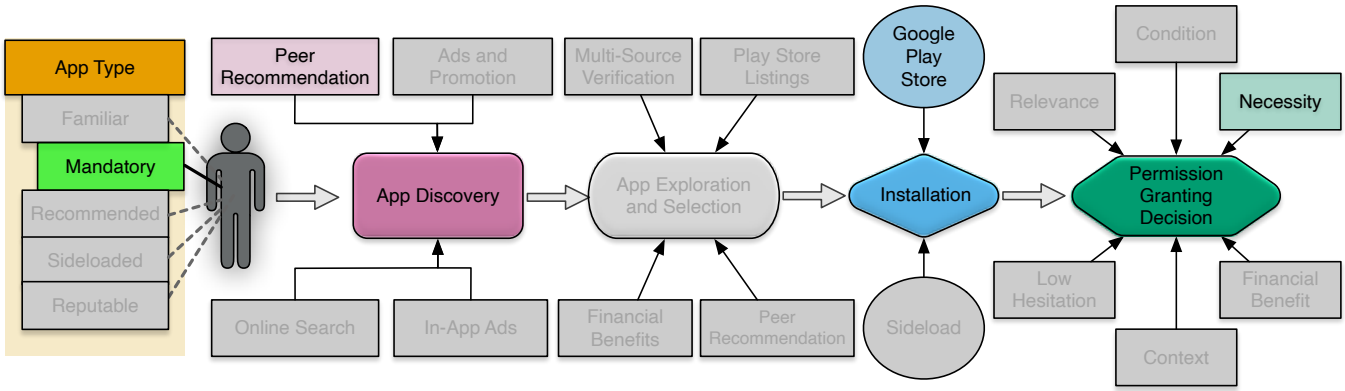


Figure 7: Journey Type 2 — "Mandatory App." This figure illustrates a journey centered on a Mandatory App, marked in the app-type on the left. Users first encounter the app through institutional or workplace requirements, which define the Discovery stage and effectively remove autonomy in the Exploration and Selection phase. Because alternatives are absent, Exploration is bypassed entirely. Installation takes place through the Google Play Store, but the key determinant is obligation rather than choice. At the Permission-Granting Decision, users proceed with acceptance out of necessity, often viewing permissions as unavoidable preconditions for fulfilling institutional tasks. Greyed-out elements indicate stages or factors inactive in this journey.

> *So I feel like their app isn't going to make or break my trust with them."-P5*

This trust had a tangible impact on the journey. It lowered scrutiny during exploration, reduced the need for external verification, and diminished hesitation at installation or permission prompts. This pattern illustrates how institutional trust serves as a heuristic that streamlines decision-making and establishes a relatively high baseline for acceptance before users encounter the permission interface.

5.3.2 Trade-off between Privacy and Access. Some participants (n=5) explicitly described weighing privacy concerns against the need to access a feature or service. They mentioned that sometimes they prioritized necessity over privacy, such as when they had no other options or a specific service was only available via a mobile app. Reputation again played a role in mitigating perceived risk, allowing users to accept permissions they would otherwise reconsider, as P7 admitted that, *"I wanted to be able to see the news in the morning. [...] I hadn't read anywhere that CBC was doing massive data accumulation or there was any kind of security risk. So it is a trade-off that I was willing to take the risk because of the reputation of the company."* A few participants also mentioned that they didn't want to share their information, but they accepted the condition in order to use the app. Tangible benefits, such as loyalty rewards, also shifted participants toward acceptance (see Section *Financial Benefits* in 5.2). These accounts reflect a pragmatic orientation in which privacy is negotiable when essential functionality or clear benefits are at stake, highlighting how contextual pressures narrow the decision space long before users reach a permission request.

5.3.3 Play Store Listings. Participants commonly used Play Store cues, such as app ratings, reviews, and download counts, to gauge credibility and assess potential privacy risks. Half of our participants (n=11; P1, P4, P6-7, P9, P11, P13-16, P19) relied on these metrics as quick filters during *exploration and selection*, interpreting strong ratings or high adoption as indirect evidence of safety. For instasnce, P1 noted,

> *"In terms of like security and the permissions I try to find things that are, like they have a lot of downloads where other people have already gone through and had no problems."*

At the same time, some participants (n = 6) viewed reviews with suspicion, and half of the participants (n = 9; P3, P4, P6, P8-9, P11, P12, P15, P17) distrusted app descriptions due to their promotional nature. This distrust often led users toward external sources for validation.

> *"The developer can say anything he wants. He can say that it's safe and he could actually pull that off until Google or Apple catches them."-P4*

This pattern demonstrates that store-level cues provide an accessible but imperfect layer of privacy reasoning, often sending participants to external sources before shortlisting an app.

5.3.4 Trust in External Community. Many participants (n=12) relied heavily on online communities such as blogs, Reddit, and review groups as trusted sources for privacy-relevant assessments. These spaces were valued for perceived authenticity, technical expertise, and reduced commercial influence. P10 explained obtaining a VPN app recommendation from Reddit:

> *"[...] So going to Reddit, you'll likely get something genuine. You don't get people that are paid to promote things on Reddit."*

Community-vetted recommendations functioned as shortcuts, for example, when participants encountered an app already endorsed in these spaces, exploration became minimal, and installation felt safer. This shift toward community-based trust highlights how privacy judgments are socially constructed and often delegated

to collective vetting processes, rather than being formed through individual inspection.

5.3.5 Multi-device and Shared-account Routines. A few participants (n = 3; P10, P12, P14) described managing privacy risk across devices by maintaining a "primary" phone for essential tasks and a secondary device for experimentation or less-trusted applications. This strategy effectively sandboxed risk and offered a structural means of separating sensitive data from uncertainty. As P10 mentioned, *"I'm not really downloading things that I'm not familiar with for the most part on my main phone. But I may get and just go on the second phone."* Only one participant (P11) reported sharing a routine account with a spouse to access apps and content together. While a corner case in our sample, this household practice may be more common in the wild and can blur individual consent and complicate permission management, consistent with findings in prior work [38, 56]

Summary of Insights

Addressing **RQ3**, our findings show that users apply diverse, stage-sensitive privacy strategies influenced by accumulated experiences, trust relationships, and contextual constraints. Brand trust and large user bases reduced scrutiny early in the journey; skepticism toward store materials led users to triangulate information with external communities; and perceived necessity, incentives, or device-level routines shaped how they ultimately approached permission requests. These strategies illustrate that **many permission decisions emerge from patterns set well before the prompt appears, reinforcing that privacy choices are formed cumulatively rather than at a single decision point.**

5.4 Archetypal journey

Drawing on participants' detailed accounts, we traced how individuals moved from discovery to evaluation, selection, installation, and ultimately permission decisions. By comparing these sequence maps across the dataset, we identified recurring patterns that illustrate how different combinations of needs, contexts, and information sources shape the flow of the journey. The archetypes highlight not only the steps participants passed through but also the mechanisms that influenced how privacy considerations emerged or faded across stages. We identified several archetypal journeys and report four that were most prevalent and analytically distinct in our data.

Journey Type 1: Recommended App Use. A distinct journey unfolded when app discovery was rooted in peer recommendation. Rather than conducting an extensive evaluation, participants deferred to the judgment of friends, family, or colleagues, assuming that trusted peers had already vetted the app's credibility and usefulness (see Section 5.2). This substitution of social trust for personal scrutiny shortened the exploration stage considerably. Participants described feeling more assured during selection and moved to installation with relatively little hesitation. Permission prompts were approached with lower attention and weaker scrutiny, as participants framed the app as already *"safe"* based on who recommended it. The resulting pathway reflects a compressed journey: a need emerged, discovery occurred through peer endorsement, exploration became minimal, and permission evaluation shifted from risk assessment to routine confirmation. Figure 6 illustrates this sequence.

Journey Type 2: Mandatory App Use. A second archetype was identified when app use was non-optional. Participants encountered mandatory apps in workplace settings, institutional processes, or essential service interactions (see *Mandatory app* in Section 5.1.2). In these cases, participants exercised little agency in selecting the app; the organization dictated which app to use and provided the discovery path. Participants described a linear and externally driven progression: they received instructions, located the required app, and proceeded directly to installation. When asked about permissions, they noted reluctance or concern but emphasized that declining was not feasible without losing access to the service. Figure 7 illustrates this journey. This journey demonstrates how institutional requirements effectively override deliberation. The path shifted from decision-making to compliance, with minimal opportunity for negotiation or alternative evaluation.

Journey Type 3: Financial Benefits. A third archetype was characterized by discovery through promotional campaigns, targeted advertisements, or reward-based marketing (see *Ads and Promotion*, in Section 5.2). Participants who encountered apps in this way often moved quickly toward installation, motivated by the prospect of coupons, loyalty points, or other financial returns. While some participants cross-checked reviews or ratings, especially those with prior negative experiences, financial incentives generally accelerated the journey. Even participants who expressed privacy concerns at other times reported accepting permission requests to secure the reward. This pattern demonstrates how economic incentives reorganize the journey by reducing scrutiny and increasing willingness to accept data access conditions. Figure 8 illustrates a recommended app journey where ads and promotion spark discovery, financial benefits motivate exploration and later permission acceptance, and demonstrate how incentives can outweigh prior privacy concerns.

Journey Type 4: Sideloaded Apps. A fourth archetype surfaced when participants acquired apps from outside the Play Store ecosystem (see *Sideloaded App* in Section 5.1.5). These cases typically arose when desired apps were unavailable in official stores (e.g., older versions), offered premium functionality elsewhere, or circulated within specialized communities (see Section 5.2). In this journey, community trust replaced formal platform vetting. Participants relied heavily on developer forums, tech communities, or word of mouth from experienced users. Although participants acknowledged high risk, they proceeded based on confidence in these external sources and the perceived value of the app. This journey demonstrates how alternative trust infrastructures, such as community expertise rather than platform governance, shape privacy decisions. Users weighed risks differently when benefits were clear and when external actors fulfilled the role typically played by app stores, as illustrated in Figure 9.

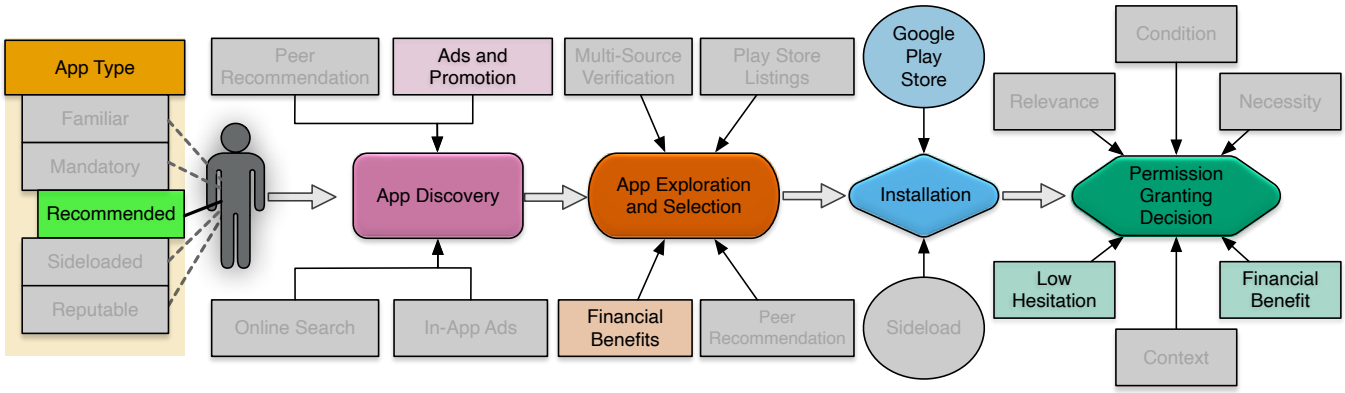


Figure 8: Archetypal Journey Type 3 — "Recommended App" with Financial Benefits. This figure illustrates a user journey in which the focal app type is a Recommended App (highlighted in green within the app-type on the left). The journey proceeds from App Discovery to Permission-Granting Decision. Participants first encounter the app through ads or promotional recommendations, which anchor the discovery stage. During App Exploration and Selection, users are primarily motivated by financial benefits, making the incentive a decisive factor in choosing an app. Installation typically occurs through the Google Play Store, reinforcing perceptions of legitimacy. By the time users reach the Permission-Granting Decision, the earlier financial incentives continue to shape their judgments, often making them more comfortable granting permissions they might otherwise scrutinize. Greyed-out elements indicate stages or factors inactive in this journey.

Summary of Insights

Addressing **RQ2**, user journeys varied substantially by app type, with four archetypal pathways—recommended apps, mandatory apps, financially motivated apps, and externally sourced (sideloaded) apps—showing distinct patterns across discovery, exploration and selection, installation, and permission handling. Recommended apps compressed evaluation through peer trust and reduced attention to permissions. Mandatory apps constrained choice and made permissions effectively non-negotiable. Financially motivated apps accelerated installation and shifted acceptance toward incentives. Sideloaded apps relied on community vetting while accepting an elevated permission risk. **These archetypes demonstrate that app type not only shapes the order of stages but also conditions when, how, and why privacy decisions occur.**

6 Discussion

Our findings advance the study of mobile privacy by shifting attention from isolated permission prompts toward the *processual dynamics* through which users arrive at those decisions. Across our analyses, we observe that the determinants of permission choices emerge not at the moment of disclosure but cumulatively throughout the user's app journey, a perspective that directly addresses the research gap raised in **RQ1–RQ3**. This section synthesizes our main theoretical contributions, elaborates how our results extend prior work, and outlines implications for design and future research.

6.1 From Fragmented Decisions to a Sequential Framework of Privacy Choice

Our study reframes app permission decisions as the *culmination of a longer sequence*, integrating app *discovery, exploration and selection, installation,* and *permission-granting* into a coherent behavioral process (Section 5.2). This responds directly to **RQ1**, which asks what the journey looks like, and **RQ2**, which examines how information flows across these stages.

Prior research has typically focused attention on the immediate prompt context (e.g., rationales, timing) [8, 17, 18], treating the permission dialogue as the central unit of analysis, while ignoring how the user arrives at this permission decision. However, our results show that many participants had effectively made their decisions long before reaching the prompt. For instance, in *Journey Type 3*, the discovery context, such as financial incentives, collapsed subsequent exploration and set expectations for acceptance at the permission stage, aligning with previous work [72]. Similar sequential patterns appeared across other archetypes, suggesting that early cues serve as epistemic anchors[3] that shape how later information is interpreted or disregarded.

This sequential patterning also complicates the assumption made by prior works [17, 18] that permission decisions are shaped primarily by the prompt's timing, framing, or justification. Instead, our data show that decision inertia is formed through early heuristics, such as *perceived necessity, trust in recommenders,* or *app type*, which often determine outcomes. This insight calls for a theoretical shift: permission decisions should be conceptualized as *path-dependent* rather than *moment-dependent*. This opens up a direction for future work to explicitly examine cross-stage dependencies, test causal mechanisms between stages, and identify where the interventions would have a meaningful impact on the user journey.

By integrating journey mapping, a method previously used in other domains [31, 36, 44, 45, 68] such as HCI, sales and marketing, and UX guidance [20, 25, 62], into *mobile privacy*, we demonstrate that journey thinking is not merely descriptive. It offers a structured

[3] early cues that stabilize expectations and reduce the perceived need for later scrutiny

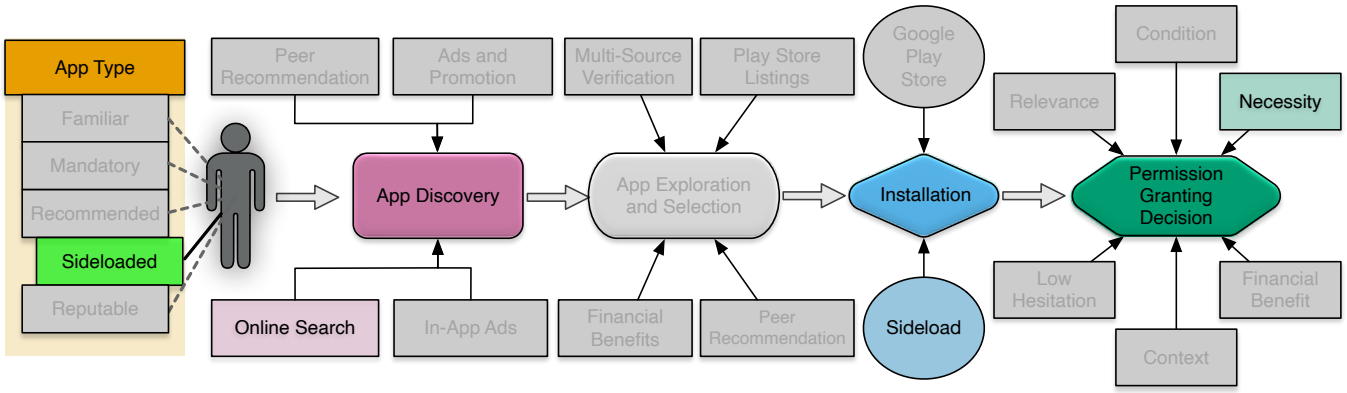


Figure 9: Journey Type 4 — "Sideloaded App" with Calculated Risk. This figure represents a journey where the app type is a Sideloaded App, highlighted on the left. Discovery typically occurs through online searches or recommendations from tech-savvy communities, setting expectations for a more hands-on, technical process. Because users pursue a specific app for a specific purpose, the Exploration and Selection stage is minimal or predetermined. Installation occurs through sideloading, outside the Google Play Store, which introduces additional security considerations. At the Permission-Granting Decision, users engage in a calculative assessment of risk, accepting permissions they believe are necessary while remaining aware of the security trade-offs inherent to sideloading. Greyed-out elements indicate stages or factors inactive in this journey.

explanatory framework that clarifies *why* permission outcomes vary across contexts. For instance, in *Journey Type 2*, the early framing of apps as *"mandatory"* established a binding trajectory that downstream stages could not meaningfully alter.

6.2 Broader contexts shape choices

Our findings further show that permission decisions are embedded within broader contextual frames, such as *prior experiences, social influences, discovery pathways,* and *app type*, that shape the extent of user agency. This directly addresses **RQ3**, which inquired about how perceptions from pre-installation stages influence subsequent decisions.

Where users exercised full choice (e.g., *Journey Type 3*), permission decisions reflected personal heuristics, such as trust in store reviews or recollections of past positive or negative experiences. In contrast, for *mandatory apps* (e.g., *Journey Type 2*), users described permissions as unavoidable, revealing that the concept of *"user decision"* is structurally constrained in many cases. Here, privacy tools such as the DSS or permissions rationale have minimal influence; not because users are uninformed, but because their autonomy is limited by institutional context.

This raises an important theoretical tension: privacy instruments assume a model of user choice that does not always exist in practice. Across our data, participants treated privacy tools inconsistently, for instance, sometimes as informational aids during comparison when choice existed, and sometimes as bureaucratic formalities when choice was constrained. This suggests that such tools may not serve as universal privacy interfaces, but rather as contingent devices whose influence depends on the user's position within the journey and the structural conditions that shape their agency.

This broader contextualisation helps explain inconsistencies reported in prior literature [17, 18], such as the same prompt design being effective for some users and ineffective for others, because the prompt interacts with expectations shaped earlier in the journey. Thus, understanding permission behavior requires examining not only the micro-context of the prompt but also the macro-context of user agency, app type, and motivational framing.

These insights call for renewed attention to the situated nature of privacy decisions. They also point toward a richer theoretical understanding of contextual privacy behavior that incorporates not only micro-level cues but also macro-level constraints such as institutional mandates and app types.

6.3 Designing for Journey-Aligned Privacy Interventions

Existing critiques of mobile permissions often center on the usability limitations of prompts [22]. In response, platforms introduced upstream privacy tools such as the Data Safety Section (DSS). However, our findings show that interventions remain limited if they are not aligned with the temporal structure of the user journey (see Section 5.2). Participants often weighted *peer trust, app type, ratings, perceived necessity* or *brand reputation* far more strongly than DSS content. Because DSS appears during the *exploration* stage, which is situated well before the permission prompt's appearance. Thus, it often becomes background information rather than an active decision aid. In cases like *peer-recommended* or textitmandatory apps, DSS was functionally irrelevant because users had already committed to installing and using the app.

These results suggest that platforms may overestimate the effect of providing privacy information at a single point in the journey. This also highlights the need for future research to investigate not only *what* privacy information is provided but also *when* and *where* it is introduced in the journey, exploring whether hybrid or staged interventions can enhance practical impact. A more effective approach in future studies may involve: 1. repositioning privacy cues [3] to moments of heightened relevance, such as integrating DSS summaries into the permission screen, 2. synchronizing

privacy affordances across multiple touchpoints, enabling users to revisit relevant information when decisions evolve. 3. tailoring the placement and framing of privacy tools to different journey archetypes and structural conditions (e.g., mandatory apps, peer-driven discovery, or sideloading), rather than assuming a single, universal flow.

Designers should therefore consider privacy as a distributed, journey-wide process, requiring continuity rather than isolated interventions. Future research can build on this by evaluating how timing, repetition, and placement of privacy tools influence outcomes across different *archetypes* and by reevaluating whether the effects of contextual cues (i.e., timing, framing of rationale) reported in prior work [17, 18, 66] are in fact contingent on earlier stages of the journey rather than arising solely at the prompt.

6.4 Toward a Theory of Sequential Privacy Decision-Making

Our findings underscore the importance of situating existing privacy theories within a temporal and sequential framework of mobile app adoption. Privacy Calculus (PC) [15] accounts for the content of users' evaluations (e.g., perceived risk-benefit trade-offs) but does not explain *how* these assessments develop as users move across the stages that precede a permission request. Similarly, Contextual Integrity (CI) [51] highlights the role of contextual norms and information flows, yet offers limited guidance on when these expectations form, shift, or become constrained during the adoption process.

The *archetypal pathways* identified in our study address these gaps by showing *how* evaluations and expectations accumulate across the journey. Participants' decisions at the moment of a permission request often reflected commitments formed much earlier, shaped by discovery signals, perceived necessity, social trust, or the type of app. For instance, in our *"Mandatory App"* pathway (see Section 5.4), institutional framing at the discovery stage established both the perceived legitimacy of the app (CI) and the acceptable trade-off structure (PC), leaving little room for reconsideration when the permission prompt appeared. These mechanisms illustrate how risk–benefit judgments (PC) and appropriateness expectations (CI) co-evolve over time, narrowing or expanding users' sense of agency as they progress toward permission decision.

By grounding these dynamics in participants' narratives, our analysis offers a process-oriented account of privacy decision making that connects the rational evaluations emphasized by PC with the contextual factors central to CI. This synthesis advances a clearer understanding of how users navigate the pre- and post-installation ecosystem and provides empirical traction on **RQ1–RQ3**, laying the conceptual foundation for interventions aligned with the realities of journey-based decision-making.

6.5 Implications

Implications for Research. Our findings suggest a need for a methodological shift in mobile privacy research. Because permission decisions emerge cumulatively across stages, we encourage researchers to move beyond prompt-centric studies and adopt journey-based, longitudinal approaches that capture how early signals (*e.g., discovery pathways, social influences*) shape later privacy behavior. Addressing this requires new empirical and analytical methods capable of tracing decision formation over time, such as staged diary studies, cross-stage experimental designs, or mixed-method journey reconstructions.

Additionally, our archetypal journeys point to the need for a more explicitly sequential theory of privacy decision-making, one that explains how choice structures evolve across stages, how early cues constrain or expand user agency downstream, and where different intervention types are most effective along the journey. Such theorizing would help reconcile fragmented findings in the privacy literature and provide a shared foundation for evaluating privacy interventions, while offering clearer entry points for combining qualitative journey reconstructions with log-based or experimental work.

Implications for Designers and Platforms. Our findings suggest that privacy tools should be redesigned to align with the temporal structure of the user journey, rather than assuming that users engage with privacy uniformly across stages. Participants often encountered the DSS and app store materials at moments when they were not yet orienting toward privacy (see Section 5.2). For example, during discovery or early exploration, where heuristics such as peer trust (see Section 5.2), brand familiarity (see Section 5.1.1), or externally sourced guidance (see Section 5.1.5) dominated decision-making. As a result, these upstream cues were frequently overlooked or interpreted only as quality signals (see Section 5.2).

To better support meaningful decisions, platforms should surface privacy information closer to consequential transitions. Integrating key DSS elements into the permission interface and presenting concise privacy summaries at installation would align privacy cues with the moments when participants evaluate the relevance or necessity of permissions (see *Evaluating Permission Relevance and Necessity* 5.2). Treating each stage as a distinct design surface allows information to be matched to users' goals, attention, and agency at that point.

A multi-touchpoint approach is also necessary to accommodate compressed or constrained pathways seen in our archetypes. For example, mandatory app users exercised little discretion (*Journey Type 2*, see Section 5.1.2), while recommended app users deferred to social trust (*Journey Type 1*, see Section 5.2).

Reintroducing brief, contextually relevant summaries at first launch or when activating sensitive features would help ensure that privacy cues remain accessible even when earlier stages are skipped.

Finally, platforms should support contextual and time-limited permission modes, reflecting patterns of conditional acceptance and post-use revocation observed in our data (see Section 5.2). Such interventions would more closely align with how users actually navigate privacy throughout their journeys. Developing validated design solutions will require targeted, user-centered evaluation (see also Section 6.6).

6.6 Limitations

Our study, while providing a detailed account of mobile user journeys, has several limitations that guide the interpretation of our

findings. First, our data is based on self-reported experiences reconstructed through interviews, which may involve over- or under-reporting of experiences [63]. This risk is heightened in privacy-focused studies, where participants may respond in socially desirable ways [23]. All participants were recruited via Prolific, which may bias the sample toward those familiar with online research. Some participants might also have prior interview experience, which could influence how they described their experiences. Although these interviews enabled us to capture cross-stage reasoning that is rarely observable through log data or prompt-level studies, they may underrepresent unconscious or automatic elements of decision-making. Complementary methods such as longitudinal logging or in-situ experiments would strengthen future causal claims.

Second, while our sample reflects a diverse range of everyday Android users, it does not aim for statistical representativeness. Our goal was to uncover mechanisms rather than measure population-level prevalence. As such, the archetypes we identify should be interpreted as analytically meaningful patterns rather than exhaustive categories. We focused on U.S. participants, who have also been the primary population in prior mobile privacy research [1, 32, 39, 58] and to limit confounding variation introduced by cross-cultural privacy norms and regulatory regimes (e.g., the GDPR), which are known to shape mobile privacy attitudes and decision processes differently across regions [12–14]. This allowed us to examine journey-level mechanisms within a relatively coherent regulatory and cultural context. Future work may extend this analysis to other populations, platforms, and cultural settings.

Third, our design implications (see Section 6.5) are intentionally exploratory and should be interpreted as theoretically grounded directions rather than ready-to-deploy solutions. Because they are derived from a qualitative analysis of 19 interviews, future work should subject these ideas to targeted evaluation through user-centered design studies (e.g., prototyping, field experiments, or A/B tests) to assess their effectiveness and generalizability across app categories, user groups, and platforms.

Fourth, our study focuses on the user's journey from app need recognition to the permission-granting decision. Although this is where permission choices occur, some downstream behaviors, such as revisiting permission settings, may reveal additional dynamics. Extending the journey to include sustained use would enable a more comprehensive framework of sequential privacy behavior.

Despite these limitations, our approach provides a theoretically grounded account of how permission decisions form over time, offering a framework for future work to build upon and empirically validate across larger and more diverse contexts.

7 Conclusion

This paper provides a new perspective on mobile privacy-granting decisions by empirically mapping the user journey from app need to permission response. Our findings show that users' decisions about granting app permissions are not made in isolation but unfold across interconnected stages, in which app need, discovery, selection, and installation are interdependent and influence one another. These findings collectively address our research questions by outlining how the distinct stages of the mobile user journey unfold (**RQ1**), how these stages vary across different app types (**RQ2**), and how users apply evolving privacy strategies shaped by early cues such as peer trust, mandates, and incentives (**RQ3**). Together, these insights consolidate fragmented understandings of permission behavior into a coherent, empirically grounded framework of the end-to-end decision process. By mapping app privacy-granting as a journey, we highlight opportunities for designers to intervene early, embed privacy safeguards strategically, and build trust throughout the process. In doing so, our work provides a foundation for privacy-focused cognitive walkthroughs that enable stakeholders to identify pain points and better support users' informed decisions regarding permission granting.

References

[1] Desiree Abrokwa, Shruti Das, Omer Akgul, and Michelle L. Mazurek. 2021. Comparing Security and Privacy Attitudes Among U.S. Users of Different Smartphone and Smart-Speaker Platforms. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Vancouver, B.C., Canada (Virtual), 139–158. https://www.usenix.org/conference/soups2021/presentation/abrokwa

[2] Ashwaq Alsoubai, Reza Ghaiumy Anaraky, Yao Li, Xinru Page, Bart Knijnenburg, and Pamela J. Wisniewski. 2022. Permission vs. App Limiters: Profiling Smartphone Users to Understand Differing Strategies for Mobile Privacy Management. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI '22)*. Association for Computing Machinery, New York, NY, USA, Article 406, 18 pages. doi:10.1145/3491102.3517652

[3] Android Developers. 2023. Data Safety Information Is More Visible in Android 14. https://developer.android.com/about/versions/14/changes/data-safety. Last updated May 16, 2023. Accessed September 10, 2025..

[4] Android Developers. 2025. Request runtime permissions. https://developer.android.com/training/permissions/requesting. Retrieved July 30, 2025.

[5] Apple. 2025. Privacy – Labels. https://www.apple.com/privacy/labels/. Accessed August 26, 2025.

[6] Rawan Baalous and Ronald Poet. 2020. Factors Affecting Users' Disclosure Decisions in Android Runtime Permissions Model. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE, Guangzhou, China, 1113–1118. doi:10.1109/TrustCom50675.2020.00147

[7] Divyanshu Bhardwaj, Sumair Ijaz Hashmi, Katharina Krombholz, and Maximilian Golla. 2025. Understanding How Users Prepare for and React to Smartphone Theft. In *USENIX Security Symposium (SSYM '25)*. USENIX, Seattle, Washington, USA, 5987–6005.

[8] Kerstin Bongard-Blanchy, Jean-Louis Sterckx, Arianna Rossi, Verena Distler, Salvador Rivas, and Vincent Koenig. 2022. An (Un) Necessary Evil-Users'(Un) Certainty about Smartphone App Permissions and Implications for Privacy Engineering. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, IEEE, Genoa, Italy, 01–08. doi:10.1109/EuroSPW55150.2022.00023

[9] Bram Bonné, Sai Teja Peddinti, Igor Bilogrevic, and Nina Taft. 2017. Exploring decision making with {Android's} runtime permission dialogs using in-context surveys. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 195–210. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/bonne

[10] Robert Bowman, Camille Nadal, Kellie Morrissey, Anja Thieme, and Gavin Doherty. 2023. Using Thematic Analysis in Healthcare HCI at CHI: A Scoping Review. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 491, 18 pages. doi:10.1145/3544548.3581203

[11] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[12] France Bélanger and Robert E. Crossler. 2011. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly* 35, 4 (2011), 1017–1041. http://www.jstor.org/stable/41409971

[13] Weicheng Cao, Chunqiu Xia, Sai Teja Peddinti, David Lie, Nina Taft, and Lisa M. Austin. 2021. A Large Scale Study of User Behavior, Expectations and Engagement with Android Permissions. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Virtual (Vancouver, B.C., Canada), 803–820. https://www.usenix.org/conference/usenixsecurity21/presentation/cao-weicheng

[14] Hichang Cho, Milagros Rivera-Sánchez, and Sun Sun Lim. 2009. A multinational study on online privacy: global concerns and local responses. *New media & society* 11, 3 (2009), 395–416.

[15] Mary J Culnan and Pamela K Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science* 10, 1 (1999), 104–115.

[16] D Dittrich and E Kenneally. 2012. *The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research*. Technical Report. U.S.

Department of Homeland Security. https://catalog.caida.org/paper/2012_menlo_report_actual_formatted

[17] Yusra Elbitar, Alexander Hart, and Sven Bugiel. 2025. The Power of Words: A Comprehensive Analysis of Rationales and Their Effects on Users' Permission Decisions. In *Proceedings of the 32nd Annual Network and Distributed System Security (NDSS) Symposium* (San Diego, CA, USA) *(NDSS Symposium 2025)*. NDSS, San Diego, CA, USA, —. doi:10.14722/ndss.2025.230544

[18] Yusra Elbitar, Michael Schilling, Trung Tin Nguyen, Michael Backes, and Sven Bugiel. 2021. Explanation Beats Context: The Effect of Timing & Rationales on Users' Runtime Permission Decisions. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Vancouver, B.C., Canada, 785–802. https://www.usenix.org/conference/usenixsecurity21/presentation/elbitar

[19] William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, and Anmol N. Sheth. 2014. TaintDroid: an information flow tracking system for real-time privacy monitoring on smartphones. *Commun. ACM* 57, 3 (March 2014), 99–106. doi:10.1145/2494522

[20] Anja Endmann and Daniela Keßner. 2016. User journey mapping–a method in user experience design. *i-com* 15, 1 (2016), 105–110.

[21] Cori Faklaris, Laura A. Dabbish, and Jason I. Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 61–77. https://www.usenix.org/conference/soups2019/presentation/faklaris

[22] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: user attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (Washington, D.C.) *(SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, Article 3, 14 pages. doi:10.1145/2335356.2335360

[23] Robert J Fisher. 1993. Social desirability bias and the validity of indirect questioning. *Journal of consumer research* 20, 2 (1993), 303–315.

[24] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. 2022. "Like Lesbians Walking the Perimeter": Experiences of U.S. LGBTQ+ Folks With Online Security, Safety, and Privacy Advice. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 305–322. https://www.usenix.org/conference/usenixsecurity22/presentation/geeng

[25] Sarah Gibbons. 2018. Journey Mapping 101. https://www.nngroup.com/articles/journey-mapping-101/. Accessed August 16, 2025.

[26] Lisa M Gray, Gina Wong-Wylie, Gwen R Rempel, and Karen Cook. 2020. Expanding qualitative research interviewing strategies: Zoom video communications. *The qualitative report* 25, 5 (2020), 1292–1301.

[27] Greg Guest, Kathleen M MacQueen, and Emily E Namey. 2011. *Applied thematic analysis*. sage publications, California, 91320, US.

[28] Jonas Hielscher, Uta Menges, Simon Parkin, Annette Kluge, and M. Angela Sasse. 2023. "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 2311–2328. https://www.usenix.org/conference/usenixsecurity23/presentation/hielscher

[29] Clara E Hill, Sarah Knox, Barbara J Thompson, Elizabeth Nutt Williams, Shirley A Hess, and Nicholas Ladany. 2005. Consensual qualitative research: an update. *Journal of counseling psychology* 52, 2 (2005), 196.

[30] Clara E Hill, Barbara J Thompson, and Elizabeth Nutt Williams. 1997. A guide to conducting consensual qualitative research. *The counseling psychologist* 25, 4 (1997), 517–572.

[31] Tharon Howard. 2014. Journey mapping: a brief overview. *Commun. Des. Q. Rev* 2, 3 (May 2014), 10–13. doi:10.1145/2644448.2644451

[32] Hsiao-Ying Huang, Soteris Demetriou, Muhammad Hassan, Güliz Seray Tuncay, Carl A. Gunter, and Masooda Bashir. 2023. Evaluating User Behavior in Smartphone Security: A Psychometric Perspective. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. USENIX Association, Anaheim, CA, 509–524. https://www.usenix.org/conference/soups2023/presentation/huang

[33] Patrick Gage Kelley, Sunny Consolvo, Lorrie Faith Cranor, Jaeyeon Jung, Norman Sadeh, and David Wetherall. 2012. A conundrum of permissions: installing applications on an android smartphone. In *International conference on financial cryptography and data security*. Springer, Springer, Berlin, Heidelberg, 68–79. doi:10.1007/978-3-642-34638-5_6

[34] 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* (Paris, France) *(CHI '13)*. Association for Computing Machinery, New York, NY, USA, 3393–3402. doi:10.1145/2470654.2466466

[35] Sabrina Klivan, Sandra Höltervennhoff, Nicolas Huaman, Alexander Krause, Lucy Simko, Yasemin Acar, and Sascha Fahl. 2023. "We've Disabled MFA for You": An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (Copenhagen, Denmark) *(CCS '23)*. Association for Computing Machinery, New York, NY, USA, 3138–3152. doi:10.1145/3576915.3623180

[36] Carine Lallemand, Jessie Lauret, and Luce Drouet. 2022. Physical Journey Maps: Staging Users' Experiences to Increase Stakeholders' Empathy towards Users. In *Extended Abstracts of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) *(CHI EA '22)*. Association for Computing Machinery, New York, NY, USA, Article 344, 7 pages. doi:10.1145/3491101.3519630

[37] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. 2017. *Research methods in human-computer interaction*. Morgan Kaufmann, Cambridge, MA, 02139 US.

[38] Junchao Lin, Jason I Hong, and Laura Dabbish. 2021. " It's our mutual responsibility to share" The Evolution of Account Sharing in Romantic Couples. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–27.

[39] Jialiu Lin, Bin Liu, Norman Sadeh, and Jason I. Hong. 2014. Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*. USENIX Association, Menlo Park, CA, 199–212. https://www.usenix.org/conference/soups2014/proceedings/presentation/lin

[40] Martin Lindstrom. 2012. *Buyology: How everything we believe about why we buy is wrong*. Random House, 1745 Broadway, New York, NY 10019, United States.

[41] Xueqing Liu, Yue Leng, Wei Yang, Wenyu Wang, Chengxiang Zhai, and Tao Xie. 2018. A large-scale empirical study on android runtime-permission rationale messages. In *2018 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*. IEEE, IEEE, Lisbon, Portugal, 137–146.

[42] Nathan Malkin, David Wagner, and Serge Egelman. 2022. Runtime Permissions for Privacy in Proactive Intelligent Assistants. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA, 633–651. https://www.usenix.org/conference/soups2022/presentation/malkin

[43] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 72 (Nov. 2019), 23 pages. doi:10.1145/3359174

[44] Yihan Mei, Zihang Liu, Shengyang Xu, Zhao Wu, and Zhibin Zhou. 2025. GeneyMAP: Designing GenAI-empowered User Journey Mapping Tool. In *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '25)*. Association for Computing Machinery, New York, NY, USA, Article 307, 11 pages. doi:10.1145/3706599.3720075

[45] Yihan Mei, Zhao Wu, Junnan Yu, Wenan Li, and Zhibin Zhou. 2025. GeneyMAP: Exploring the Potential of GenAI to Facilitate Mapping User Journeys for UX Design. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25)*. Association for Computing Machinery, New York, NY, USA, Article 270, 22 pages. doi:10.1145/3706598.3713479

[46] Christopher Meyer, Andre Schwager, et al. 2007. Understanding customer experience. *Harvard business review* 85, 2 (2007), 116.

[47] Anthony Morton and M. Angela Sasse. 2012. Privacy is a process, not a PET: a theory for effective privacy practice. In *Proceedings of the 2012 New Security Paradigms Workshop* (Bertinoro, Italy) *(NSPW '12)*. Association for Computing Machinery, New York, NY, USA, 87–104. doi:10.1145/2413296.2413305

[48] Suman Nath. 2015. MAdScope: Characterizing Mobile In-App Targeted Ads. In *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services* (Florence, Italy) *(MobiSys '15)*. Association for Computing Machinery, New York, NY, USA, 59–73. doi:10.1145/2742647.2742653

[49] Duc Cuong Nguyen, Erik Derr, Michael Backes, and Sven Bugiel. 2019. Short text, large effect: Measuring the impact of user reviews on android app security & privacy. In *2019 IEEE symposium on Security and Privacy (SP)*. IEEE, IEEE, San Francisco, CA, USA, 555–569.

[50] Nielsen Norman Group. 2020. User Journeys vs. User Flows. Online article. https://www.nngroup.com/articles/user-journeys-vs-user-flows/ Accessed: 2025-07-31.

[51] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[52] Don Norman. 2003. *Emotional Design: Why We Love (or Hate) Everyday Things*. Basic Books, New York.

[53] Don Norman. 2013. *The design of everyday things: Revised and expanded edition*. Basic books, New York, US.

[54] John L Oliffe, Mary T Kelly, Gabriela Gonzalez Montaner, and Wellam F Yu Ko. 2021. Zoom interviews: Benefits and concessions. *International journal of qualitative methods* 20 (2021), 16094069211053522.

[55] Anna-Marie Ortloff, Matthias Fassl, Alexander Ponticello, Florin Martius, Anne Mertens, Katharina Krombholz, and Matthew Smith. 2023. Different Researchers, Different Results? Analyzing the Influence of Researcher Experience and Data Type During Qualitative Analysis of an Interview and Survey Study on Security Advice. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 864, 21 pages. doi:10.1145/3544548.3580766

[56] Cheul Young Park, Cori Faklaris, Siyan Zhao, Alex Sciuto, Laura Dabbish, and Jason Hong. 2018. Share and Share Alike? An Exploration of Secure Behaviors in Romantic Relationships. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, Baltimore, MD, 83–102. https://www.usenix.org/conference/soups2018/presentation/park

[57] European Parliament and Council of the European Union. 2016. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive

95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679 OJ L 119, 4.5.2016, p. 1–88.

[58] Sarah Prange, Pascal Knierim, Gabriel Knoll, Felix Dietz, Alexander De Luca, and Florian Alt. 2024. "I do (not) need that Feature!" – Understanding Users' Awareness and Control of Privacy Permissions on Android Smartphones. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. USENIX Association, Philadelphia, PA, 453–472. https://www.usenix.org/conference/soups2024/presentation/prange

[59] Prolific. 2025. Prolific - Participant recruitment for research. https://www.prolific.com/ Accessed: 2025-07-29.

[60] Qualtrics. 2025. Qualtrics XM: The Leading Experience Management Software. https://www.qualtrics.com/. Accessed August 14, 2025.

[61] Adam Richardson. 2010. Using customer journey maps to improve customer experience. *Harvard business review* 15, 1 (2010), 2–5.

[62] Kerry Rodden, Hilary Hutchinson, and Xin Fu. 2010. Measuring the user experience on a large scale: user-centered metrics for web applications. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. Association for Computing Machinery, New York, NY, USA, 2395–2398. doi:10.1145/1753326.1753687

[63] Christie N Scollon, Chu Kim-Prieto, and Ed Diener. 2003. Experience sampling: Promises and pitfalls, strengths and weaknesses. *Journal of Happiness studies* 4, 1 (2003), 5–34.

[64] Bingyu Shen, Lili Wei, Chengcheng Xiang, Yudong Wu, Mingyao Shen, Yuanyuan Zhou, and Xinxin Jin. 2021. Can Systems Explain Permissions Better? Understanding Users' Misperceptions under Smartphone Runtime Permission Model. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Vancouver, B.C., Canada, 751–768. https://www.usenix.org/conference/usenixsecurity21/presentation/shen-bingyu

[65] StatCounter Global Stats. 2025. Mobile Operating System Market Share Worldwide. https://gs.statcounter.com/os-market-share/mobile/worldwide. Accessed August 14, 2025.

[66] Mohammad Tahaei, Ruba Abu-Salma, and Awais Rashid. 2023. Stuck in the Permissions With You: Developer & End-User Perspectives on App Permissions & Their Privacy Ramifications. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 168, 24 pages. doi:10.1145/3544548.3581060

[67] Joshua Tan, Khanh Nguyen, Michael Theodorides, Heidi Negrón-Arroyo, Christopher Thompson, Serge Egelman, and David Wagner. 2014. The effect of developer-specified explanations for permission requests on smartphone user behavior. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto, Ontario, Canada) *(CHI '14)*. Association for Computing Machinery, New York, NY, USA, 91–100. doi:10.1145/2556288.2557400

[68] Zofija Tupikovskaja-Omovie. 2025. Digital Art Gallery in Metaverse: Eye Tracking Digital Visitors' Visual Attention, Engagement and User Journey when Interacting with Digital Artworks on Smartphones. In *Proceedings of the 2025 Symposium on Eye Tracking Research and Applications (ETRA '25)*. Association for Computing Machinery, New York, NY, USA, Article 96, 9 pages. doi:10.1145/3715669.3725874

[69] Amos Tversky and Daniel Kahneman. 1974. Judgment under Uncertainty: Heuristics and Biases: Biases in judgments reveal some heuristics of thinking under uncertainty. *science* 185, 4157 (1974), 1124–1131.

[70] Mojtaba Vaismoradi and Sherrill Snelgrove. 2019. Theme in Qualitative Content Analysis and Thematic Analysis. *Forum: Qualitative Social Research* 20, 3 (2019), 23. doi:10.17169/fqs-20.3.3376 Article 23.

[71] Haoyu Wang, Hao Li, and Yao Guo. 2019. Understanding the Evolution of Mobile App Ecosystems: A Longitudinal Measurement Study of Google Play. In *The World Wide Web Conference* (San Francisco, CA, USA) *(WWW '19)*. Association for Computing Machinery, New York, NY, USA, 1988–1999. doi:10.1145/3308558.3313611

[72] Tien Wang, Trong Danh Duong, and Charlie C Chen. 2016. Intention to disclose personal information via mobile applications: A privacy calculus perspective. *International journal of information management* 36, 4 (2016), 531–542.

[73] Ying Wang, Yibo Wang, Sinan Wang, Yepang Liu, Chang Xu, Shing-Chi Cheung, Hai Yu, and Zhiliang Zhu. 2022. Runtime permission issues in android apps: Taxonomy, practices, and ways forward. *IEEE Transactions on Software Engineering* 49, 1 (2022), 185–210.

[74] Primal Wijesekera, Arjun Baokar, Ashkan Hosseini, Serge Egelman, David Wagner, and Konstantin Beznosov. 2015. Android Permissions Remystified: A Field Study on Contextual Integrity. In *24th USENIX Security Symposium (USENIX Security 15)*. USENIX Association, Washington, D.C., 499–514. https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/wijesekera

[75] A. Witzel and H. Reiter. 2012. *The Problem-Centred Interview: Principles and Practice*. SAGE Publications Ltd, London.

A Participant Recruitment Filters

To ensure participants aligned with the study's objectives and maintained consistency across cultural, linguistic, and technical contexts, we applied the following pre-screening filters on Prolific.

(1) **Age 18 or above:** Ensures participants can provide informed consent independently.
(2) **Currently living in the United States:** Maintains consistency in cultural, regulatory, and market contexts.
(3) **Born in the United States:** Focuses on those with long-term experience in the U.S. mobile ecosystem.
(4) **First language - English:** Supports clarity in communication and understanding of the interview.
(5) **Phone OS - Android 6.0 or higher:** Ensures participants have experience with runtime permission prompts.
(6) **Primary mobile device - Android:** Keeps focus on Android specific app behaviors and settings.

B Pre Screening Survey

The pre-screening survey was used to verify participant eligibility based on the inclusion criteria. It collected demographic details, mobile usage patterns, and confirmation of Android device ownership to ensure that selected participants matched the study's target profile.

(1) **Age** - Please enter your age in years: *(Use numeric format only, e.g., 18)*
(2) **Gender** - What is your gender identity?
  (a) Male
  (b) Female
  (c) Non-binary
  (d) Prefer to self describe *(text entry)*
(3) **Education** - What is the highest degree or level of education you have completed?
  (a) No degree
  (b) Primary School Degree
  (c) High School Diploma or Equivalent
  (d) Associate Degree
  (e) Bachelor's Degree
  (f) Master's Degree
  (g) Doctoral Degree (PhD, EdD, etc.)
(4) **Mobile Brand** - Please specify the brand name and model of your primary smartphone. (*e.g., Google Pixel 9 Pro, Samsung Galaxy A54*) *(text entry)*
(5) Mobile Phone Usage Period - How long have you been using your primary smartphone mentioned in the previous question?
  (a) Less than 6 months
  (b) 6–12 months
  (c) 1–2 years
  (d) 2–4 years
  (e) More than 4 years
(6) **IT Skills** - Which of the following describes you best *(multiple answer possible)*?
  (a) I am majoring a degree in IT security
  (b) I have a degree in IT security
  (c) I am majoring a degree in Computer Science or a closely related field
  (d) I have a degree in Computer Science or a closely related field
  (e) I work as an IT security professional, Software Engineer, or Software Developer
  (f) None of the above
(7) Would you describe yourself as Tech Savvy? **(Yes/No)**
(8) Do you agree with the following statement? *If I want a specific app for a specific task, I put a lot of time into finding the right application.* **(Yes/No)**
(9) **Mobile app download frequency** - How often do you download new applications?
  (a) At least once a day
  (b) At least once a week
  (c) At least once a month
  (d) At least once a year
  (e) More rarely than once a year
(10) Did you ever install and/or manage apps beyond just downloading from the official Google Play Store? *(e.g., alternative app store such as Galaxy Store, Mi Store; direct download from third-party websites, testing beta versions, or using developer mode)* **(Yes/No)**
(11) (**If Q10 was selected as yes**) How often do you install and/or manage mobile applications from sources other than the official Google Play Store? (e.g., alternative app store such as Galaxy Store, Mi Store; direct download from third-party websites, testing beta
  (a) I only did it once or twice
  (b) I do it once or twice a year
  (c) I do it once or twice a month
  (d) I do it almost every month or more often
(12) (**If Q10 was selected as yes**) Approximately how many mobile apps have you installed and/or managed from sources other than the official Google Play Store? *(Only numerical values allowed)* (text entry)

B.1 Security Attitude (SA-6)

In the following questions, "security" refers to how cautious or concerned you are about protecting your personal information, data, and device from threats such as hacking, malware, or unauthorized access when using mobile apps.

Please indicate your agreement with the following statements.

(1) I seek out opportunities to learn about security measures that are relevant to me.
(2) I am extremely motivated to take all the steps needed to keep my online data and accounts safe.
(3) Generally, I diligently follow a routine for security practices.
(4) I often am interested in articles about security threats.
(5) I always pay attention to experts' advice about the steps I need to take to keep my online data and accounts safe.
(6) I am extremely knowledgeable about all the steps needed to keep my online data and accounts safe.

The options for the SA-6 questionnaire:

- Strongly Disagree
- Somewhat Disagree
- Neither Agree nor Disagree
- Somewhat Agree

- Strongly Agree

C Interview Guideline

- **Introduction and Oral Consent**
  - Researcher briefly introduces themselves
  - Inform participants about confidentiality and data handling.
  - Obtain consent to record the interview and assure them they can skip questions or end the interview at any time.
- **Warm Up Phase**
  - What smartphone do you currently use?
  - Do you have multiple phones?
    - If yes:
      - Can you tell me why do you have multiple phones?
      - If it is primary and work or secondary phone?
  - What are the main things you do with your smartphone each day?
- **Exploratory Phase**
  - Can you recall the last time you installed a new app on your phone?
    - If yes:
      - Can you tell me what it is?
    - What is it about the need that makes you install the app?
  - What do you usually do when you need a new app?
  - Where do you get your apps from?
    - Follow up: *(If they used Google Play Store)*
      - What do you typically look at or consider first?
      - **Probes**: app description, rating, screenshots, reviews, permissions.
    - Follow up: *(If they don't use the Google Play Store:)*
      - What made you decide to get apps from other sources?
      - How do you know about this source?
      - Why do you prefer using that particular source?
      - What led you to do that?
      - How did you feel about the safety or trustworthiness of the source?
- **Focused Phase**
  - What information do you usually check before downloading an app?
    - Do you check the info provided in the App store?
      - Last resorts: e.g., description, reviews, permissions, data safety section
  - Have you ever changed your mind about installing an app after seeing certain information?
    - If yes
      - What influenced your decision?
  - Have you ever seen an app ask for permission to access things like your camera?
    - Can you describe what you did?
    - What made you do this?
- **Concluding Questions**
  - Is there anything about apps- privacy that worries you these days?
    - If yes, what is it?
    - What precautions did you take?
    - What led you to think about that?
      - **Probe**: Before even installing the app; after installing the app
  - Is there anything we have not discussed that you think is relevant to this topic, or any suggestions?
- **Closing and Thanks**
  - Thank the participant sincerely.
  - Explain how their input contributes to understanding app privacy behaviours.
  - Provide follow-up information: "We will anonymize your responses and use them only for research purposes. If you have any questions later, feel free to contact us at firstname.lastname@organisation.org."
  - Confirm how compensation will be processed.

D Codebook

The codebook presents the final set of codes and subcodes developed through thematic analysis. It includes definitions and examples that guided the consistent coding of interview transcripts and the identification of key themes across participants.

(1) **Multiple Phones** - *Use of more than one phone to manage work and personal activity; risk, and privacy.*
   (a) **Multiple Phones::App Download Attitude** - *How users' decisions about downloading apps differ across multiple phones.*
   (b) **Multiple Phones::Different App Usage Per Device** - *Assigning apps to specific phones based on perceived risk or purpose.*
   (c) **Multiple Phones::Security Behaviour** - *Different security and usage habits depending on which phone is used.*

(2) **Privacy Strategy** - *This theme encompasses the user's planned attitudes and principles regarding data privacy when interacting with apps. It reflects their underlying trust or distrust in various entities and their strategies for managing access to their data.*
   (a) **Privacy Strategy::Distrust in Developer Intent** - *Skepticism about whether app developers act in the users' best interest or primarily for their own benefit. Users suspect that developer goals may not align with user privacy.*
   (b) **Privacy Strategy::Distrust in External Review** - *Lack of trust in third-party review platforms or online sources.*
   (c) **Privacy Strategy::Distrust in New/ Less Known Company** - *Reluctance to trust companies that are new, small, or have little public reputation.*
   (d) **Privacy Strategy::Distrust in Play Store Review** - *Belief that reviews on Google Play may be fake or unreliable.*
   (e) **Privacy Strategy::Phone Privacy Settings** - *Customizing phone settings (permissions, tracking, etc.) to protect privacy.*
   (f) **Privacy Strategy::Trade-off between Privacy and Access** - *Balancing data protection with app functionality or access needs.*
   (g) **Privacy Strategy::Trust in Company/Brand** - *A willingness to install apps from brands or companies that are perceived as trustworthy, reputable, and established.*

(h) **Privacy Strategy::Trust in External Community**- *Relying on recommendations and advice from trusted external communities like Reddit, specialized forums, or social media groups. Users value the perceived authenticity of peer experiences.*
(i) **Privacy Strategy::Trust in Familiarity** - *Trusting apps that are already known to the user.*
(j) **Privacy Strategy::Trust in Play Store No. of Download**- *Using a high download count on the Play Store as a heuristic or signal for an app's legitimacy, popularity, and safety.*
(k) **Privacy Strategy::Trust in Play Store Ratings** - *Believing star ratings reflect app quality or privacy.*
(l) **Privacy Strategy::Trust in Play Store Review** - *Trusting user reviews in the Play Store as honest indicators.*

(3) **Sideload** - *Practices and concerns related to installing apps from unofficial sources.*
(a) **Sideload::How to Find Alternative Sources**- *Online searches, forums, or peer recommendations.*
(b) **Sideload::Reasons for Alternative Sources** - *Why users look beyond the Play Store (e.g., unavailability, censorship).*
(c) **Sideload::Security Concerns about Sideloading**- *Worries about app safety and phone vulnerability from sideloaded apps.*
(d) **Sideload::Trust Factors in Alternative Store** - *Trust and security factors for apps installed from third-party stores (sideloading).*

(4) **Use Case** - *Contexts or domains where users use apps, shaping their privacy expectations.*
(a) **Use Case::Analogy example from Participant** - *Participants use metaphors or real-life comparisons to describe their behavior.*
(b) **Use Case::Bank** - *Apps related to financial services, where privacy and security are critical.*
(c) **Use Case::Delivery Service** - *Apps for food or package delivery, involving location and transaction data.*
(d) **Use Case::Fitness Tracker (Smart band, calory tracker, sleeping monitor)**- *Apps that collect personal health data.*
(e) **Use Case::Game** - *Gaming for recreation and focused apps where users may take more risks.*
(f) **Use Case::Smart Devices** - *Apps for controlling or connecting smart home or IoT devices (e.g., smart bulbs, thermostats, wearables).*
(g) **Use Case::Specific Need for an App** - *Unique situations or one-time requirements for which an app is installed.*

(5) **User Traits** - *This category captures relatively stable tendencies, dispositions, and orientations that shape how individuals approach mobile apps and privacy-related decisions.*
(a) **User Traits::Admits Relax Security Practices** - *Users acknowledge lowering their security guard in certain cases.*
(b) **User Traits::Data Breach Shapes Future Actions** - *Past experiences with data breaches or incidents cause the user to adopt stricter privacy and security practices in the future.*
(c) **User Traits::Fear of Identity Theft** - *A strong and specific concern that using apps could lead to identity theft or the compromise of sensitive credentials.*
(d) **User Traits::High Trust in Banking Apps** - *A specific trait of placing a high degree of trust in banking or financial apps, often viewing them as inherently secure regardless of general privacy concerns.*
(e) **User Traits::Ignore Data Safety Section** - *Does not pay attention to the app's "Data Safety" information provided in the Play Store.*
(f) **User Traits::Indirect Negative Experiences** - *The user's privacy practices are influenced by knowing someone else who faced a privacy or security issue, even if they haven't experienced one personally.*
(g) **User Traits::Low Hesitation in Downloading Apps** - *A tendency to quickly download and install apps without spending much time on prior evaluation or research.*
(h) **User Traits::Neglects Looking for Any Information (Review, Ratings etc.)** - *Tends to install apps without checking available background information like reviews, ratings, or developer details.*
(i) **User Traits::Neglects Privacy Policies** - *Avoids or ignores reading detailed privacy statements.*
(j) **User Traits::Only download doesnt give any data** - *The user holds the perception that merely downloading an app does not share any data with the developer, believing data is only shared upon opening and using the app.*
(k) **User Traits::Past Victim of Online Fraud** - *The user's current behaviors are directly influenced by having been a victim of online fraud, scams, or data theft in the past.*
(l) **User Traits::Personal Data Concern** - *Worries about how apps collect, use or share personal information.*
(m) **User Traits::Policy Comprehension Barrier** - *A feeling of difficulty or inability to understand the complex legal and technical language commonly used in privacy policies and terms of service.*
(n) **User Traits::Proactively Checks Security Factors** - *A tendency to intentionally and diligently review permissions, developer information, and ratings before making a decision about an app.*
(o) **User Traits::Relies on Peer Recommendation** - *A habitual reliance on advice from friends, family, or colleagues as a primary source for deciding which apps to download.*
(p) **User Traits::Relies on Tech Communities (Reddit)** - *Heavily depending on opinions and recommendations from technology-focused online communities like Reddit for app-related decisions.*
(q) **User Traits::Security Mindset** - *General tendency to prioritize safety and data protection.*
(r) **User Traits::Skeptical of Developer Claims** - *Disbelieves developers' promises, especially about privacy.*
(s) **User Traits::Trial and Error Approach to Apps** - *A learning strategy where the user prefers to install and test apps themselves, forming opinions based on direct experience rather than prior research.*

(6) **User Journey** - *This theme captures the sequence of steps and decisions a user takes when engaging with a mobile app, from the first time they discover an app to permission granting decision. It highlights how choices evolve across stages and influence later privacy-related decisions.*

(a) **App Needs** - *The user's initial motivation or purpose for seeking an app, based on a specific need or problem they want to address. This comes before discovery and guides what kind of apps they search for in the marketplace or on specific websites.*
  (i) **App Type::App Cost::Free - Apps available at no monetary cost, often monetized through ads or data collection.**
  (ii) **App Type::App Cost::Paid** - *Apps that require purchase or subscription, often perceived as higher quality or more privacy-respectful.*
  (iii) **App Type::Familiar** - *Apps that the user already knows or has used before.*
  (iv) **App Type::Mandatory** - *Apps that users feel obligated to install due to necessity or external pressure i.e.Online Bank App.*
  (v) **App Type::Optional** - *Apps that users can choose to install based on preference.*
  (vi) **App Type::Recommended** - *Apps suggested by others (friends, experts, systems) for specific purposes.*
  (vii) **App Type::Reputable** - *Apps with strong reputations, often from well-known developers or companies.*
  (viii) **App Type::Sideloaded APKs** - *Apps not available on Play Store and installed from sources outside the official Play Store, usually in APK format.*
  (ix) **App Type::Specific but not Mandatory** - *Apps that user looking for something specificity in mind and free to choose from tha available options.*

(b) **App Discovery** - *How the user first becomes aware of or comes across an app. This can happen through multiple channels, such as app store recommendations, advertisements, social media, company websites, or peer recommendations. Discovery represents the entry point into the user journey.*
  (i) **App Discovery::Brand/Company Website** - *Discovering an app by visiting the official website of the developing company to learn about it directly from the source.*
  (ii) **App Discovery::External Research other Than Play Store (Reddit, Google, YouTube)** - *Actively seeking information and recommendations from independent online sources like search engines, Reddit, or YouTube before downloading.*
  (iii) **App Discovery::Google Play Store Search** - *Finding apps by searching directly in the Play Store.*
  (iv) **App Discovery::In app ads** - *Discovering new apps from ads embedded in other apps.*
  (v) **App Discovery::Recommendation from Peer**- *Learning about an app through advice and suggestions from friends, family, or colleagues.*
  (vi) **App Discovery::Social Media/TV ads, Promotion** - *Becoming aware of an app through mass media channels, including social media ads, television commercials, or other promotional campaigns.*
  (vii) **App Discovery::Trial and Test Features** - *Discovering an app's value by exploring its features through a trial version, just out of curiosity or limited functionality before making a decision.*

(c) **App Exploration & Selection** - *The process that follows discovery, where users engage in evaluating potential apps. This includes exploring the app store page (e.g., reviews, description, screenshots, ratings), verifying information from multiple sources, and comparing alternatives. The outcome of this stage is the user's final decision to select and install (or reject) an app.*
  (i) **App Selection::App Description for App Selection** - *Evaluates the content and clarity of the app's description to decide whether to install it.*
  (ii) **App Selection::App Icon, Thumbnails or Verified Sign for Selection** - *Using visual indicators like the app icon, screenshots, and developer verification badges to assess professionalism and build trust.*
  (iii) **App Selection::Avoids Negatively Reviewed Apps** - *Actively skipping or rejecting apps that have a significant number of negative user reviews or low aggregate scores.*
  (iv) **App Selection::Based on Familiarity** - *Prioritizing and selecting apps that they are already familiar with from past use or exposure.*
  (v) **App Selection::Based on Number of Downloads** - *Using a high number of downloads on the Play Store as a key factor in selecting an app, equating popularity with safety and quality.*
  (vi) **App Selection::Based on Peer Recommendation** - *Choosing to install an app primarily because it was personally recommended by someone they know.*
  (vii) **App Selection::Based on Permission, Privacy Policy requirements** - *Reviewing the permissions an app requests and its privacy policy before downloading to assess potential privacy risks.*
  (viii) **App Selection::Based on Play Store Reviews** - *Reading user reviews on the Play Store and using them as a primary factor in the decision to install an app.*
  (ix) **App Selection::Based on User Ratings** - *Chooses apps based on user ratings i.e. higher ratings means "good app"*
  (x) **App Selection::Getting Financial Benefits, Coupons , Points**- *Selecting an app because it offers direct monetary incentives, coupons, reward points, or other financial benefits.*
  (xi) **App Selection::Online Community Recommendation (via Multisource Verification)** - *Being influenced by and trusting recommendations from online tech communities, forums, or blogs during the selection process.*
  (xii) **App Selection::Trust in known Brands** - *Preferring and readily selecting apps from well-known and familiar companies or developers, often with less hesitation.*

(d) **App Installation** - *The action of installing the selected app onto the device, which can occur through different methods.*
  (i) **App Install::Default from Google Play Store** - *Installing an app directly from the official Google Play Store, which is the standard for most users.*
  (ii) **App Install::Sideload (If Unavailable at Play Store)** - *Installing an app from an alternative source (outside the Play Store) by sideloading an APK, typically only when the app is not available officially or when specifici features comes with a payment, user goes for unofficial apps.*

(e) **App Permission** - *The user's interaction with and response to permission requests. This includes runtime permissions, and post-installation prompts. Users may grant, deny, or reconsider permissions depending on perceived necessity, relevance, or trust in the app.*
  (i) **App Permission::Accept Based on Trusted Source** - *Granting permissions because the app came from a source they trust, such as a recommended or reputable developer.*
  (ii) **App Permission::Accept Conditionally Based on Context** - *Granting a permission based on the immediate context or need, and may revoke it later if the context changes.*
  (iii) **App Permission::Accept Due to Financial Benefits** - *Approving permissions specifically to gain access to financial incentives, rewards, or coupons offered by the app.*
  (iv) **App Permission::Accept for Necessity for App Functionality**- *Granting a permission because it is absolutely required for the core functionality of the app to work, even if hesitant.*
  (v) **App Permission::Allow Based on Data Sensitivity** - *Permits access only if data involved isn't sensitive.*
  (vi) **App Permission::Allow Low-Risk Permissions (They thought low risks)**- *Readily allowing permissions that are perceived as non-intrusive or low-risk (e.g., network access) without much deliberation.*
  (vii) **App Permission::App Running in Background** - *Permission decisions based on whether the app operates continuously in the background.*
  (viii) **App Permission::Ask Each Time** - *Requests the app to ask permission each time before accessing a feature.*
  (ix) **App Permission::Default Deny Strategy** - *Employing a mindset of denying permission requests by default unless the app provides a compelling reason to grant access.*
  (x) **App Permission::Deny Excessive & Irrelevent Permissions** - *A user's refusal to grant permission requests that are perceived as either too numerous (excessive) or not logically required for the app's core functionality (irrelevant).*
  (xi) **App Permission::Don't think much of App permission** - *Granting app permissions routinely without much thought, evaluation, or concern for the potential consequences.*
  (xii) **App Permission::Evaluate Permission Relevance** - *Actively assessing whether a requested permission makes logical sense for what the app is supposed to do.*
  (xiii) **App Permission::Low Hesitation Accepting Permission** - *Accepting permissions quickly and without significant deliberation, primarily to get the app running and start using it.*
  (xiv) **App Permission::Permit Based on Brand Trust** - *Grants permission if the app comes from a trusted company/brand.*