"I Just Press Allow": Understanding Privacy Practices of New Internet Users in Urban India

Priyanka Popuri
BITS Pilani, Hyderabad
p20210022@hyderabad.bits-pilani.ac.in

Srishti Sanghi
The University of Sydney
ssan0823@uni.sydney.edu.au

Sri Lekha Mondreti
BITS Pilani, Hyderabad
f20190783h@alumini.bits-pilani.ac.in

Dipanjan Chakraborty
BITS Pilani, Hyderabad
dipanjan@hyderabad.bits-pilani.ac.in

Abstract

In rapidly digitizing countries, like India, many people are adopting the Internet for the first time through smartphones. Such new users, with little prior exposure to digital systems, face applications and services that access personal and private data, often leaving no agency with the users to exercise a choice. This creates an imbalance between the power of data-driven platforms and the limited digital literacy of users, raising urgent privacy and security concerns. While prior research has studied experienced Internet populations, far less is known about how first-time users in the emerging markets think about and act on privacy risks.

We present findings from interviews with 50 new Internet users in India, spanning diverse social and economic backgrounds. Our study shows that privacy is often managed by family members and local intermediaries, with users depending on them for key decisions. Participants held incomplete or inaccurate understandings of data collection, while prioritizing visible threats like fraud and device theft. The findings reveal a mismatch between formal privacy controls and the realities of everyday practice. We outline design and policy directions to support consent and security in ways that reflect the experiences of new Internet users.

Keywords

privacy, new internet users, security, interdependent privacy, resigned consent, tactical agency, pragmatic privacy

1 Introduction

The biggest growth in Internet adoption worldwide is happening through the mobile segment, with a substantial share of new users emerging from countries like India [88]. Between 2014 and 2025, smartphone penetration in India surged from approximately 13.5% to nearly 55.3% [89], driven by affordable handsets, declining mobile data costs, and the expansion of app-based services. This rapid uptake has created a distinct and heterogeneous user group often referred to in prior work as Novice Users [59], Emerging Users [12], New Internet Users [38], or the Next Billion Users [74].

New Internet users typically have little or no formal training with digital devices in academic or work settings, are unfamiliar with text-heavy interfaces, and often do not use English as a working language [86]. Their entry into the digital ecosystem has enabled large-scale innovations in entertainment, digital payments, social networking [52], instant messaging [20], education, and e-commerce [63]. The design of many smartphone-based platforms continues to assume the knowledge, expectations, and decision-making patterns of more experienced users, leaving newcomers to navigate complex privacy and security settings without adequate support.

Smartphone applications and operating systems routinely collect sensitive personal data like contacts, location, financial records, behavioral patterns, and increasingly biometric identifiers [85]. While there is a lot of research focusing on using technical means to protect privacy, such as cryptography [67, 70], far less attention has been paid to the perspectives and practices of first-time users or low-literacy users. A lack of understanding of how these populations interpret privacy and security, can render interventions inaccessible, ineffective, or culturally irrelevant.

When platforms are not designed with the user's context in mind, they create real risks. Previous research shows that poorly tailored protections make users more vulnerable to problems like data breaches [96], financial fraud [94], and identity theft [71]. These risks become even greater in situations where digital and everyday social challenges overlap such as when phones are shared within families, taken to local repair shops, or set up by more knowledgeable relatives or shopkeepers [87]. As more first-time users come online, privacy and security systems need to combine strong technical protections with sensitivity to social and cultural realities.

In this paper, we present findings from a qualitative study with 50 first-time or early-stage smartphone users in India, spanning diverse geographic and socio-economic backgrounds. Our study addresses three key research gaps:

- Limited interpretability of privacy-preserving technologies: Prior work has focused on technical strength (e.g., authentication, encryption, consent mechanisms), but has not adequately examined how these can be made understandable and usable for novice and culturally diverse populations.
- Underexplored role of local practices and trust networks: Existing research often assumes individual decision making,

Proceedings on Privacy Enhancing Technologies 2026(2), 180–197

https://doi.org/10.56553/popets-2026-0043

overlooking how family ties, community beliefs, and interpersonal trust shape privacy and security choices in Global South contexts.
- Lack of socio-cultural fit in privacy frameworks: Current models emphasize technical robustness , but rarely account for challenges faced in low-literacy, shared-device, and informal repair settings, leaving significant gaps in protection for first-time users.

We ground these goals in the following research questions:

RQ1 How do household relationships and reliance on digitally literate family members shape privacy decisions and experiences? (Sections 4.1, 4.3, 4.5)

RQ2 What informal strategies and everyday workarounds do users adopt when formal controls are difficult to understand or use? (Sections 4.2, 4.4, 4.5)

RQ3 Why do users consent to apps despite mistrust, and what does this reveal about the limits of current consent models? (Sections 4.1, 4.2)

Our work bridges privacy and security research with the lived realities of new digital populations, offering empirical insights and design implications for creating digital ecosystems that are more inclusive, trustworthy, and sensitive to context.

The rest of the paper is arranged as follows: The literature survey related to privacy and security around the users of Internet, mobile phone sharing, and digital literacy is discussed in Section 2. The details of the qualitative study are described in Section 3. The findings obtained through the survey and the related discussions are mentioned in Sections 4 and 5. Future work and conclusion are outlined in Section 6.

2 Related Work

This work builds on prior research in four key areas: (1) Privacy and Security Practices on the Internet, (2) Mobile privacy and sharing, (3) Privacy Risks in Refurbished and Shared Devices, and (4) App permissions and digital literacy. We review this literature to highlight gaps that motivate our study, which investigates how new smartphone users in urban India understand and navigate privacy and security. Understanding what privacy means to individuals who will use and be affected by the usage of the technology is a crucial step in designing for privacy [31]. Our study contributes to the expanding body of research examining privacy attitudes within specific regions of India.

2.1 Privacy and Security Practices on the Internet

Privacy perceptions and practices among low-literate users in South Asia have been a growing focus in HCI and privacy research. Naveed et al., [65] showed that in Pakistan, gender bias and device-related constraints shaped privacy concerns differently from W.E.I.R.D. (Western, Educated, Industrialized, Rich, Democratic) contexts. Similarly, Friedman et al., [31] demonstrated cross-cultural variation in privacy norms, finding that Swedish participants expressed stronger privacy concerns than U.S. participants, with women in both contexts reporting higher sensitivity. Kumaraguru and Sachdeva et al., [51] found that Indian mobile users with lower literacy placed high trust in service providers despite limited understanding of privacy implications.

These studies show that privacy concerns are shaped by culture, gender, and literacy levels, but most examine what people think about privacy rather than how they handle it in everyday digital life. Our study builds on this foundation by examining how these factors materialize in the everyday smartphone experiences of first-time adopters in urban and peri-urban India, highlighting how privacy understanding develops through interaction, social learning, and experimentation rather than formal instruction.

In Bangladesh, Mahidi et al., [7] reported that privacy leakage was a common problem among urban app users who recognized risks but lacked coping strategies. Ahmed et al., [5, 6] explored tensions between collective and individual privacy within families, while Habib et al., [36] found that low awareness, social norms, and family guidance shaped how users navigated permissions, often resulting in consent fatigue.

These works highlight that privacy in South Asia is socially negotiated and contextually learned, but they examine user groups whose experiences differ from those at the earliest stages of adoption. By focusing on early-stage users, our work reveals how such negotiation begins when users are still forming norms of trust, ownership, and control, thereby extending understanding of privacy not as a fixed practice but as an evolving process.

Recent research, such as the SoK: Safer Digital Safety Research Involving At-Risk Users [14], has emphasized ethical engagement with participants facing literacy, dependency, or surveillance-related constraints. Building on this guidance, our study provides grounded empirical insights into how these constraints influence digital safety behaviors in everyday settings, highlighting the importance of contextualized, user-centered methods for emerging smartphone populations.

2.2 Mobile Phone Privacy and Sharing in South Asia

Studies across India, Bangladesh, and Pakistan emphasize that device sharing shapes privacy expectations and constraints for many users [45, 73]. Prior work highlights that privacy is not always an individual pursuit but often a collective and relational process shaped by social ties, shared responsibilities, and interdependent digital practices. Research on interdependent and networked privacy shows that people often rely on others to configure settings, manage visibility, and interpret digital risks, especially in shared-use environments [29, 40, 57]. Studies of family-mediated privacy further demonstrate how privacy boundaries are negotiated within households through trust, obligation, and hierarchical roles [1]. These perspectives shift privacy from an individual choice model toward a socially embedded phenomenon, emphasizing how visibility and control are shaped by interpersonal relationships rather than isolated decision-making.

Ahmed et al., [4] examine how biometric SIM registration policies expose surveillance concerns and identity negotiations in Bangladesh, while Hussain et al., [41] show that youth often trust mobile networks despite limited awareness of digital risks. Gender also plays a crucial role where women frequently manage visibility through deletion, avoidance, and app hiding rather than

relying on permissions [73]. Broader structural factors complicate these practices, as device obsolescence, repair, and reuse shape privacy in low-resource communities [44], with Pew Research [21] quantifying how phone-sharing correlates with income and gender in India. Vulnerable populations, such as queer men using geosocial apps, face additional risks of stigma and exposure due to shared-device contexts [69].

Studies in rural South Asia show that device sharing and limited autonomy shape privacy experiences: Iqbal et al., [43] report how rural Indian youth's smartphone autonomy is gendered; Komen et al., [49] reveal how phone sharing in rural Kenya influences privacy concerns; Wijetunga et al., [91] examine how under-privileged youth in Sri Lanka access mobile services and how design neglects their literacy and sociocultural constraints. These studies demonstrate that phone sharing, gendered autonomy, and structural inequality are key factors in shaping the experience of privacy in low-resource settings. The prior work highlights these challenges and proposes design interventions, it offers little understanding of how people navigate privacy in day-to-day digital use.

Prior work also connects privacy, literacy, and user experience in important ways. Schwind et al. [76] show that ethical consent principles often fail to ensure comprehension among diverse users, while Soheil et al. [39] find that uneven digital literacy in India leaves low-literate groups vulnerable to privacy risks. Botha et al. [18] emphasize that mobile usability depends not only on technology but also on users' ability to interpret interactions, echoing broader UX work such as Park et al. [68] who define UX as balancing usability and user value, and Fernando et al. [28] who propose methods to capture accessibility and ease of interaction. These studies link privacy to literacy and design, yet few explore how users with limited digital skills practice privacy in daily life.

Our study addresses this gap by examining how low-literate mobile users in India perceive and experience privacy through their everyday actions. Focusing on lived practice rather than attitudes, we show how users negotiate privacy through delegation, coping with fear, and improvised workarounds. This ground view reveals privacy as a process continuously shaped by digital literacy, gender, cultural norms, and emotional safety in South Asian contexts.

2.3 Privacy Risks in Refurbished and Shared Devices

Refurbished and pre-owned mobile phones constitute a sizable market in South Asia; however, little is known about how users perceive the associated privacy risks. Existing research has largely focused on adjacent domains. Tu et al., [83] examine consumer attitudes toward second-hand luxury goods in Southeast Asia, where trust, sustainability, and value shape adoption. Ben Yahya et al., [16] show that perceived data security modestly influences recycling and reuse intentions. Broader studies highlight technical risks: Haris et al., [37] survey mobile data leakage across apps, while Shen et al., [80] map global patterns of private information collection, noting regional variation. In financial contexts, Mgiba and Shukla et al., [62] find that perceived invasiveness and trust jointly shape mobile banking adoption.

These studies show that privacy concerns shape how people reuse or recycle devices and whom they trust. Most of this work focuses on perceptions or technical risks, not the day-to-day experiences of users handling second-hand phones. The everyday realities of reused phones, especially in low-literacy settings, remain underexplored.

Our findings address this gap by showing that for low-literate users in India, privacy risks are experienced through practical challenges, depending on shopkeepers or relatives to set up phones, not knowing if old data was erased, and fearing misuse during repair or resale. Looking at refurbished phone use within social and economic dependencies, our work highlights how privacy vulnerabilities persist in informal repair, resale, and shared-use practices. For participants, second-hand phones offered affordability but also created reliance and vulnerability, underscoring the need for context-sensitive privacy safeguards.

2.4 App Permissions & Digital Literacy

Prior research has examined both technical and human dimensions of mobile privacy. Tahaei et al., [82] show that developers often over-request permissions due to uncertainty in third-party libraries, while users grant them with a limited understanding of the consequences. Shrivastava et al., [81] similarly highlight mismatches between user expectations and android's permission scope. Remedies such as translating permissions into service-based labels [23] or providing privacy education [53] have shown promise. Previous work also explores how clearer risk signals or glanceable notices support informed consent [47, 93]. These approaches presume that users themselves interpret and act on such signals, which does not align with shared-device contexts where intermediaries often make privacy decisions. Industry data indicate that 58% of apps request sensitive data beyond core functionality [92].

Research on dark patterns and coercive interfaces reveals that apps often require permissions as a condition for access, undermining meaningful refusal [84]. Denial of permissions can also disrupt core functionality, prompting users to comply regardless of their understanding or trust [48]. These studies demonstrate how platform control and infrastructure constraints limit users' ability to make informed consent decisions.

Regional work extends these insights by linking privacy to culture, literacy, and usability. Saeed et al., [72] find that usable privacy controls build trust in Saudi Arabia, while Vaidehi et al., [90] uncover caste-based divides in India shaped by education and income. Digital literacy initiatives such as Internet Saathi [33] attempt to bridge these gaps, echoing Jackson et al.'s argument that privacy needs in developing regions are constrained by culture and cost [46]. Technical studies [37, 80] further stress the need for context-aware protections, and human-centered work proposes more accessible models such as culturally grounded privacy design [32] and layered policies that reduce cognitive load [58].

These studies show that technical and educational interventions often treat privacy as an individual cognitive task. In contrast, our work examines how low-literate Indian users navigate privacy through delegation, improvisation, and emotional negotiation in daily life. By focusing on lived routines rather than isolated prompts, we show that privacy is collectively managed and relationally sustained, extending previous work by highlighting the trust-based and fear-driven practices that shape consent in the Global South.

3 Methodology

We undertook a qualitative investigation to understand how new and less digitally literate users engage with mobile app privacy and security. In this section, we describe the study design, ethical considerations, participant recruitment, data collection, data analysis, and researcher positionality.

3.1 Study Design

India has one of the world's fastest-growing Internet user bases, with millions of individuals coming online for the first time through affordable smartphones and low-cost mobile data plans. However, the rapidity of this adoption means many users have minimal prior experience with digital devices, online platforms, or associated risks to privacy and security. At the same time, many mobile applications request extensive permissions and collect sensitive personal information.

Our goal was to explore how new Internet users in urban India perceive, negotiate, and respond to privacy and security challenges while using smartphones. Towards this end, we recruited participants through convenience and snowball sampling and conducted a qualitative study comprising semi-structured interviews followed by thematic analysis.

3.2 Ethical Considerations

In the absence of a formal ethics board for human subjects research in our university, we followed established ethical guidelines for ICTD research, as layed out by Dearden et al., [26]. All participants provided informed consent before participation. Given the varying digital literacy levels among participants, we developed a verbal consent script in local languages, supplemented with simple visual aids to explain study aims, procedures, and rights. Participants were informed that:

- They could withdraw at any time without consequence.
- Their responses would be anonymised and used only for research purposes.
- No personally identifying information would be linked to published findings.

We obtained verbal informed consent before starting each interview, given many participants' lower digital literacy levels. Interviews were recorded with permission, and all identifying details were anonymized in transcripts. We offered no monetary incentive to the participants for participating in the study, as it might have added a bias to the convenience sampling we used for the study.

3.3 Participants

We recruited 50 participants through a combination of convenience and snowball sampling, across urban and peri-urban areas in India until we reached data saturation. Initial recruitment took place via local community centres, mobile phone retailers, educational institutions, and informal word-of-mouth referrals. The inclusion criteria were:

- First-time or early-stage smartphone users, who own and regularly use a smartphone, but do not know what happens in the background.
- Aged 18 years or older.
- Able to participate in an interview in one of the languages spoken by the research team (Hindi, Telugu, or English).

The study involved 50 participants (26 women and 24 men) aged between 19 and 58 years, recruited through convenience and snowball sampling across urban and peri-urban areas in India. The sample included a diverse range of ages, genders, and occupations, reflecting early-stage smartphone adopters with varying levels of digital literacy. Educational backgrounds ranged from no formal schooling to postgraduate degrees, and occupations included informal labour (e.g., domestic work, street vending), students, and service-sector employees. Notably, even participants with higher educational qualifications were new Internet users with limited experience in smartphone use. The sample also reflected a range of device types, from low-cost entry-level models to mid-range smartphones, with several participants using pre-owned or shared devices. Detailed demographic information is provided in Appendix B.

Because participants were recruited through convenience and snowball sampling, the study does not aim to statistically represent all new Internet users in India. Instead, it offers an in-depth, qualitative understanding of how early-stage smartphone adopters experience privacy and digital use in their everyday lives. The participant group aligns with national patterns of new Internet adoption. According to recent reports by the Internet and Mobile Association of India (IAMAI 2024) [42] and the Telecom Regulatory Authority of India (TRAI 2025) [66], first-time Internet users in India are predominantly from lower and middle-income groups, with increasing adoption among women and adults in peri-urban regions. Our participants reflect these emerging segments, including early-stage smartphone adopters who are learning to navigate mobile technologies for communication, entertainment, and social media. This situates our qualitative sample within the broader context of India's expanding and diversifying connected population.

3.4 Interview Guide and Data Collection

We developed a semi-structured interview guide with open-ended, scenario-based prompts. Questions focused on how participants installed and set up apps, who helped them with phone settings and updates, what they knew about app permissions and data sharing, fears or experiences with privacy breaches, and how they protected personal content. The guide was pilot-tested with ten participants and refined for clarity and flow.

Interviews lasted 45–60 minutes and were conducted in participants' preferred languages (Hindi, Telugu, or English). To ensure accessibility, we avoided technical jargon, for example, instead of asking, "How do you manage application permissions?", we asked, "When your phone asks to use your camera or location, what do you do?". All interviews were audio-recorded with permission and later transcribed and translated into English where necessary. The complete interview guide and protocol is provided in Appendix A.

3.5 Data Analysis

The interviews were conducted by a multilingual team of undergraduate engineering students and a Ph.D. scholar. Thematic analysis was carried out following Braun and Clarke's six-phase approach [19].

The process involved:

- **Familiarisation:** The research team read and re-read transcripts to gain an overall understanding of participants' narratives.
- **Initial coding:** Segments of text related to privacy, security, technology use, and decision-making were labelled with descriptive codes derived inductively from the data.
- **Theme development:** Related codes were clustered into broader themes such as "delegation of decisions to trusted others," "invisible data collection," "trade-offs between convenience and safety," and "privacy as a social rather than individual concept."
- **Iterative refinement:** Themes were refined through team discussions, ensuring both common patterns and outliers were captured, while preserving socio-cultural context.

The initial codebook was developed on a pilot set of 10 participants and iteratively refined as more transcripts were coded, with definitions and inclusion/exclusion criteria updated for consistency. Our analysis aimed to capture both surface-level practices (e.g., locking the phone, accepting permissions) and underlying rationales (e.g., trust in family members, resignation to technology's demands). Privacy and security perceptions were treated not as static beliefs, but as dynamic, situated understandings shaped by lived experience and social interactions. The final codebook used for the analysis is available in Appendix C.

3.6 Positionality

Given the interpretive nature of qualitative research, we recognise that our positionality as researchers, educated, digitally literate, and institutionally affiliated, may have influenced both the framing of questions and the interpretation of data. We attempted to mitigate these effects by:

- Using local language to build relationships and reduce perceived power imbalances.
- Encourage participants to use their own examples and metaphors to describe experiences.
- Discussing emerging interpretations within a multidisciplinary team to challenge assumptions and avoid overly techno centric readings of participants' accounts.

We acknowledge that our study captures a snapshot in time of participants' perceptions, which may evolve as they gain more digital experience. Nevertheless, the findings offer valuable insights into the initial phases of technology adoption and the privacy-related challenges faced in these early stages.

4 Findings

Our analysis revealed five major themes that capture participants' perceptions, behaviors, and coping strategies related to mobile app privacy and security. These themes demonstrate how privacy is not only shaped by technical understanding, but also by social roles, family dynamics, infrastructural constraints, and everyday negotiation. We present these themes as:

(1) Perceived Lack of Control
(2) Eschewal of Terms and Policies
(3) Delegating Digital Decisions
(4) Everyday Privacy Workarounds
(5) Fear of Exposure and Harm

4.1 Resigned Consent: Perceived Lack of Control

A dominant concern expressed by participants was their inability to control what mobile apps collect, store, and share. Even participants who had heard of data misuse incidents felt resigned to the idea that apps "take what they want." This sense of helplessness was closely tied to both technical unfamiliarity and systemic distrust of digital ecosystems. Participants described how attempts to assert control, such as denying permissions or uninstalling apps, often led to service disruptions or had no observable effect, reinforcing a belief that control over personal data is merely symbolic.

> *"I was trying to book a cab using the ride app on my phone, but it kept asking for location, contacts, and even the microphone. At first, I thought I could just deny it, but then the app refused to open. I tried again and again. Finally, I clicked 'Allow' to everything just so it would work. Since then, I just press 'Allow' for all apps; otherwise, they don't work. I feel like I'm not really choosing."* — **P12**, Female, 31, Construction worker, 6th standard education

P12's experience shows how permission requests often function as coercion rather than true consent. The interface appeared to offer a choice, but refusal meant the app would not work, pushing her to grant all permissions as a survival strategy rather than informed agreement. Many participants echoed this sense that saying "no" was not a real option, since denial often broke key features. This mirrors findings from smart home studies, where attempts to revoke consent also disabled functions, making privacy control feel symbolic. Furthermore, when devices were repurposed for parenting or entertainment, they introduced new risks and household tensions around privacy [22, 61].

This perceived lack of control extended beyond active app usage to the belief that data, once collected, remains permanently accessible to companies, even after an app is removed.

> *"One day, my daughter told me to delete a game app that she thought was using too much data. I deleted it, but then I kept getting offers and ads from the same game on Facebook. That's when I realized these apps still keep something, even after uninstalling. Now I believe nothing can really be erased from the phone."* — **P6**, Male, 45, Rikshaw driver, 10th standard education

P6's account highlights growing distrust in systems that claim to offer control. Even after uninstalling apps, participants felt their data remained accessible, and repeated permission prompts deepened this anxiety, leading to reluctant compliance. Over time, such experiences weakened trust further and reinforced the sense that privacy controls offered little real protection [35]. Others reported becoming wary when apps repeatedly prompted for the same permissions, interpreting this as a sign of potential harm.

> *"Some apps ask me every time I open them: location, photos, contacts. Even if I deny, they ask again. I don't know what happens if I say no too many times. Maybe*

> *the app will stop working or my phone will stop working, or hang."* — **P28**, Female, 35, Tailor, 6th standard education

P28's concern reveals that unclear, repeated permission prompts cause anxiety and fearful compliance, particularly among less confident users.

A few participants disengaged entirely from reviewing permissions after encountering mismatches between an app's purpose and its data requests.

> *"I installed a torch (flashlight) app once and later saw it had access to my call logs and camera. It made no sense. After that, I stopped checking permissions because I didn't understand how it all works. I just assume they do what they want."* — **P34**, Female, 40, Tailor, 3rd standard education

P34's experience describes a situation where functionality and permission requests appeared incongruent. The mismatch between the app's stated purpose and its data access reinforced his decision to disengage entirely from privacy settings. Similar experiences show that people often trade privacy for convenience, choosing to keep apps working even if the data access feels excessive. Many weighed the benefits of using a service against the risks of sharing information, a process shaped by necessity rather than comfort. When the balance felt unfair, they stopped engaging with privacy settings, focusing instead on getting the functionality they needed [75].

Beyond language barriers and social reassurance, many participants also experienced privacy decisions as mentally exhausting. The repeated prompts and complex choices demanded time and effort they were unwilling to spend. This cognitive burden, while not specific to our user group, further explains why users often skip details and accept permissions just to continue using the app.

We refer to these collective experiences as *resigned consent*: situations where users comply not out of agreement or understanding, but because they perceive no viable alternative. This sense of *no exit* from data collection was particularly acute for those dependent on apps for transportation, work, or communication. The cost of denial was too high, leading participants to normalize invasive behaviors than to resist them.

Unlike other studies where people weigh privacy risks against benefits, our participants felt they had no real choice at all. Consent was less about making a trade-off and more about going along out of necessity, since refusing often meant losing access to essential apps and services. Such findings challenge widely held assumptions embedded in digital consent frameworks [76], which presume autonomy, understanding, and the ability to revoke consent. For many participants, none of these conditions held true. Instead, consent functioned as a form of symbolic compliance, an act carried out to keep essential services running, even when users knew their choices had little real effect. This perceived lack of control reflects deeper systemic gaps in app design, business models, and policy enforcement rather than individual digital literacy alone.

4.2 Eschewal of Terms and Policies

Most participants admitted to skipping privacy policies, disclaimers, and permission prompts without reading them. This behavior was not due to lack of interest or indifference towards privacy, but stemmed from the perception that these materials were difficult to understand. Participants cited multiple barriers, including unfamiliar technical language, dense layouts, and English-only content. These factors led users to develop routine practices of ignoring such disclosures, often reinforced by social norms or peer advice.

> *"A message popped up when I installed the photo editing app. It was written in English, and there was a lot of text. I couldn't make sense of anything, so I scrolled and pressed 'Agree'. That's what I do for every app just agree and move ahead. I once asked my younger cousin what it meant, and he said 'Nobody reads that anyway.'"* — **P19**, Female, 35, Homemaker, 5th standard education

P19's experience highlights how language barriers and perceived irrelevance lead to consent fatigue [36]. Even interested users avoid policies when reading them feels too difficult or irrelevant. Prior studies show that users skip privacy policies not just due to their length and complexity, but because they see little value or trust in them. Policies are often perceived as corporate legal protections rather than useful information, making reading them feel pointless. This further normalizes habitual non-engagement, even among those concerned about their data [54].

Some participants initially attempted to engage with privacy settings, but found the process too opaque to continue.

> *"I once tried to look at app permissions after a friend told me some apps can record secretly, but when I opened the settings, there were so many confusing terms, like, 'background access' and 'save app data to cloud'. I got scared and worried that I might mess up something."* — **P27**, Male, 35, Shopkeeper, 12th standard education

P27 initially tried to explore privacy settings but was soon discouraged by technical jargon and confusing options. Unfamiliar terms like "background access" and "save app data to cloud" felt intimidating, and fear of breaking something made him give up. Prior studies similarly show that complex language and unclear settings discourage users from managing their privacy. Instead of showing a lack of interest, this reflects a fear of making mistakes, leading users to rely on guessing or advice from others rather than a clear understanding [17] [79].

These experiences emphasize that it is not a lack of concern, but a lack of comprehensible design, that prevents users from making informed choices. For many participants, the very structure of digital consent in the form of long documents, complex settings, or abstract permissions is exclusionary. What appears to be user inattention is often a rational adaptation to interfaces that demand high levels of digital and linguistic literacy. As a result, privacy decisions are made based on peer heuristics, guesswork, or trial and error rather than genuine understanding.

This theme highlights a fundamental flaw in current consent infrastructures: the assumption that all users can read, interpret, and evaluate complex disclosures. In reality, many users, especially those operating in second or third languages, or with limited technical backgrounds are structurally unable to participate in such consent processes. Consequently, digital consent becomes more of a performative ritual than a meaningful exercise in autonomy. Addressing this challenge requires not just simplified language, but

reimagined interaction models that prioritize clarity, context, and linguistic inclusion.

4.3 Delegating Digital Decisions

A recurring pattern, especially among older and less digitally literate participants, was the outsourcing of digital decisions to more knowledgeable family members, often male children, nephews, or neighbors. These intermediaries served as informal digital caregivers who installed apps, enabled permissions, and managed privacy-related prompts. For many participants, trust in these individuals substituted for understanding the technology itself.

> *"My son gave me this phone. He installed everything and told me how to open YouTube and WhatsApp. When something new comes, I give him the phone and he handles it. Once, a message came asking for access to contacts, and I gave the phone to him. He clicked something and gave it back. I don't know what he did exactly, but I trust him."* — **P1**, Female, 36, House Helper, 3rd standard education

P1's case highlights how dependence on her son for navigation transferred control over both functionality and consent. Not knowing what he clicked reflects limited technical understanding and reliance on trust rather than informed decision-making. Similar patterns appear in other research, where many users rely on family or friends to set up devices and manage permissions, effectively shifting privacy decisions away from individuals toward more knowledgeable others, resulting in trust-based rather than informed consent [10, 11, 27, 56].

A similar pattern emerged in cases involving second-hand phones, where uncertainty about residual data compounded reliance on others.

For example, P38 described giving his pre-owned phone to his nephew, who formatted it on his behalf. Like P1, he did not fully grasp what was being done, but trusted the family member to ensure safety.

> *"When I gave my pre-owned phone to my nephew, he formatted it. I didn't know that a second-hand phone could still have data from the previous user. At that time, I only removed the SIM card. Later, I learned there is something called a 'reset,' so next time I will ask for that before giving it away."* — **P38**, Male, 42, Bus conductor, 8th standard education

We also observed that trust in others often served as the primary measure of an app's safety, replacing any direct evaluation of settings or policies.

> *"I wanted to talk to my sister who lives in another town, and my nephew installed an app for video calls. I asked him if it was safe, and he said it's what everyone uses. Now I use it daily, but I've never looked into the settings or privacy. I assume he made it safe for me."* — **P42**, Female, 56, House helper, No education

In P42's case, the app's safety was judged not through technical checks but through her nephew's reassurance and its perceived popularity. Her reliance on his setup decisions, without reviewing privacy settings herself, shows how interpersonal trust often replaces personal verification. Other studies also find that people trust apps because relatives recommend them or many others use them, rather than by checking the settings themselves. This kind of social reassurance replaces individual scrutiny, making privacy a shared assumption. As a result, permissions are accepted by habit, not careful choice [34, 95].

Delegation also extends beyond familial relationships to include local businesses and service providers.

> *"When I wanted to install a loan app, the shopkeeper helped me. He took my phone and did everything quickly. I saw some messages asking for a camera and SMS, but he said it's normal., I didn't ask again."* — **P18**, Female, 34, Tailor, 8th standard education

P18's account illustrates how delegation of digital decisions extends into community and commercial settings. A local shopkeeper managed the app installation and permissions, presenting consent requests as *just how apps work*. This normalization discouraged further questioning and highlights the risks of relying on intermediaries who may not prioritize user privacy. Recent work on privacy-enhancing technologies shows efforts to protect data while still allowing its use, but these solutions remain complex and far from everyday practice. In contrast, participants often relied on intermediaries, accepting permissions as routine without questioning how their data would be handled [8].

Even when participants attempted to engage directly, guidance from trusted individuals could discourage exploration or intervention.

> *"I get help from my grandson to set up everything. I saw a lock symbol once and asked what it was. He said 'don't touch it, it's for safety.' So I never opened it. I don't know what it does, but I assume it's protecting something."* — **P23**, Female, 50, Homemaker, 5th standard education

P23's account illustrates how trusted advice can unintentionally discourage engagement with privacy features. The lock icon, likely a security setting, became off-limits following second-hand warnings. Such dependency limits user confidence and reinforces findings that family guidance often overrides personal judgment in privacy decisions. This dependence can unintentionally limit exploration and learning, leaving settings untouched. Over time, privacy becomes something managed by others rather than by the user themselves [25] [64].

These accounts demonstrate that privacy and security decisions in such contexts are deeply social processes. Rather than being made in isolation, they are embedded in networks of trust and dependency, where digital authority is ceded to those perceived as more competent. While these arrangements can reduce immediate barriers for novice users, they also obscure the transparency and intentionality expected in conventional consent frameworks. Once configured by someone else, settings and permissions were rarely revisited, creating persistent blind spots in users' understanding of their own devices.

4.4 Everyday Privacy Workarounds

Despite significant barriers to understanding or controlling digital systems, many participants developed inventive, context-specific strategies to safeguard their privacy. These workarounds, ranging from using pseudonyms and symbolic profile images to locking specific apps or avoiding certain types of sharing, were not always technically robust, but they gave participants a tangible sense of control. Such actions represent what we term tactical agency: adaptive behaviors that constitute meaningful resistance to perceived risks of digital exposure.

One common approach involved shifting online behavior to reduce unwanted attention. Some participants replaced personal photos with non-identifiable images and limited their content to neutral or socially safe topics.

> *"I had posted a picture of myself in a new dress, and comments started coming from unknown people, some were not nice. I felt uncomfortable, so I removed the picture and decided to change my profile photo to a flower. Since then, I only post poems or festival messages. My friends understand, and it keeps things simple."* — **P21**, Female, 42, Construction worker, 5th standard education

P21's choice to share poems and greetings instead of personal photos shows how users consciously manage visibility and safety online. By setting boundaries through selective sharing, she balances participation with protection. Similar patterns appear in prior work, where people use symbolic or non-personal content to stay connected while safeguarding privacy. These adjustments allow continued social participation without increasing risks. Such practices highlight how privacy management is woven into everyday acts of self-expression [2, 60].

Another strategy was to create separate online identities to control who could view certain content. This tactic allowed participants to segment audiences, reducing exposure to undesirable interactions while maintaining selective social engagement.

> *"I created a second Facebook account under a different name after my cousins kept tagging me in silly posts. In my new account, I only have close friends. That way, I control what people see and who I talk to. I don't post much, just follow pages for news and offers."* — **P22**, Female, 22, Student, B. Tech education

P22 manages privacy by separating accounts to control content and audience boundaries. This segmentation allows her to curate interactions and visibility on her own terms, demonstrating a nuanced awareness of online exposure even outside platform norms. Such repurposing of platform affordances illustrates how users creatively adapt design features to meet their privacy needs. Prior research similarly shows that people seek inventive ways to manage privacy through design cues and feedback—ranging from making data use more transparent to using simple user reviews to uncover hidden privacy risks early. Both point to the importance of designs that support user control and trust [24, 47].

In shared-device contexts, participants often turned to technical features such as app locks or hidden folders to safeguard personal content from co-users.

> *"I share my phone with my younger brother, and I don't want him to see my chats or photos. So I use the app lock that asks for a pattern. I also keep some apps in a hidden folder, which I learned about from a YouTube video. It's not perfect, but it gives me peace of mind."* — **P7**, Female, 19, Student, B-Com (pursuing).

P7 describes a layered strategy for protecting personal content on a shared device. By combining an app lock and hidden folders, she asserts control over what others can access. She learned these methods through YouTube, showing how informal networks foster privacy literacy. Her approach reflects a blend of caution and creativity. Research on monitoring devices shows that even when privacy is considered in design, it is often treated as secondary and not fully built in. This leaves users to find their own ways of protection, much like P7's creative use of locks and hidden folders [9, 50]. Such gaps highlight how everyday strategies often fill the space left by weak design safeguards.

For others, privacy strategies revolved around symbolic anonymity and routine content clearing, reflecting a desire to manage visibility while minimizing traces of activity.

> *"My DP is always a flower or cartoon image. I also clear my browser history regularly because I don't want others to see what I searched. I don't know if it deletes everything, but it makes me feel better."* — **P17**, Female, 27, Tailor, 6th standard.

P17 maintains privacy through symbolic anonymity and routine digital hygiene. She uses a flower or cartoon as her display picture and regularly clears browser history to prevent others from seeing her activity. Though unsure of its technical effectiveness, these actions offer her a sense of control and psychological comfort, showing how privacy is felt as much as it is practiced. Studies in similar contexts show that people often use parallel accounts, selective sharing, and culturally shaped practices to manage privacy on shared devices. These tactics are less about technical control and more about creating a safe balance between social expectations and personal boundaries. Together, they show how privacy is shaped as much by context and necessity as by technology itself [6, 65].

These practices demonstrate that even with limited technical understanding, users negotiate their digital presence. Personal experiences and perceived risks of the participants shape their attitudes and practices towards privacy. Their actions are not passive or accidental, but represent intentional, situated responses to specific risks and social dynamics. These strategies are often grounded in personal experiences, peer learning, and cultural norms about modesty, respect, and visibility.

4.5 Fear of Exposure and Harm

Many participants, especially women, described fears of harassment, blackmail, or reputational damage stemming from the misuse of their personal data. Details like phone numbers, personal photos, and location details were consistently viewed as sensitive, not just for privacy reasons, but because of the potential for social and physical harm. These fears were not hypothetical; participants recounted personal experiences or community stories that had lasting impact on their behavior and sense of safety.

> *"I had taken a ride using an app. The driver seemed fine at the time, but after the trip ended, he messaged me and said he had saved my number. I never gave it to him. He kept calling at odd times. I was scared and told my brother, who blocked the number. Since then, I don't use that app after dark."* — **P3**, Female 58, Home-maker, 12th standard education

P3's account illustrates how routine app use can expose personal data in unexpected ways. After a ride-hailing driver obtained her phone number without consent and began harassing her, she stopped using the app at night. The incident shows how privacy breaches directly affect users' sense of safety and reshape everyday behavior.

Other participants recounted being misled by messages or forms that mimicked official communications. These scams often leveraged visual and linguistic cues of legitimacy, such as government symbols or promises of public benefits, to trick users into voluntarily surrendering sensitive data.

> *"A relative once forwarded a message that promised cash rewards if we filled in a form. I entered my name, phone number, and Aadhaar number, thinking it was from the government, but later I found out it was fake. Now I'm very careful, but sometimes I still wonder where that data went."* — **P25**, Male, 28, Delivery boy for e-commerce, 10th standard education

P25's story reveals how trust in official looking messages and forms can lead to involuntary data sharing. His uncertainty about where the data ended up and the lack of any clear recourse which reflects the long tail of fear that follows such incidents. It also signals a broader challenge in distinguishing legitimate platforms from scams, particularly in environments where digital literacy may be uneven.

For many women, cautionary tales from the community had as much influence as personal experience. Stories of reputational damage, particularly involving photo misuse, circulated widely and served as warnings that shaped daily digital habits.

> *"I heard of a woman in our area whose photo was taken from Facebook and used on a fake profile. People thought it was her, and she faced a lot of insults. That story scared me. I don't share photos anymore, and I've made my profile private with just a few friends."* — **P13**, Female, 38, Construction worker, 8th standard education

P13's account reflects how community-level incidents inform personal privacy practices. The fear of impersonation and reputational harm, especially for women, is not an abstract concern, but a socially mediated one. Her response, including tighter privacy settings and limiting photo sharing, illustrates a proactive, but constrained approach to managing risk. Other research finds that people often avoid apps that ask for sensitive data, like location or activity, even if they're useful, showing that privacy concerns strongly influence app choices. Visual tools that show data sharing at a glance can help users understand what apps are doing, making privacy feel more transparent and manageable. Together, these insights show how clear data signals and sensitive practices shape user trust and cautious behavior [77, 93].

Even seemingly safe spaces, such as class or community WhatsApp groups, were sometimes sources of unwanted exposure. Along with that the familiar digital spaces, such as school or community WhatsApp groups, participants encountered risks of unwanted exposure. The overlap of personal and semi-public communication channels meant that sensitive information could easily reach unintended audiences.

> *"A boy from my coaching class once messaged me something strange. I asked how he got my number, and he said he saw it on a class WhatsApp group. After that, I stopped putting my number in any group where I don't know everyone."* — **P2**, Female, 19, Student, B.Tech (pursuing).

P48's experience reveals the risks of casual data exposure in social groups, especially mixed-gender ones. The incident made her re-evaluate how and where she shares her contact information, even within seemingly safe contexts like academic groups. It illustrates how users develop new norms of caution after breaches of trust or boundary violations. Other studies show that people often follow group norms to decide what privacy behaviors are acceptable, even if this reduces their caution. Over time, feelings of discomfort with apps become normalized, as users keep using them despite unease. These patterns highlight how privacy choices are shaped by habit and social influence rather than real control [48, 78].

In some cases, risk awareness came through family advice, which participants initially dismissed, but later embraced after hearing corroborating stories from friends or neighbors.

> *"My husband told me not to post selfies online because someone could misuse them. At first, I thought he was being too strict, but later I heard from a friend that her picture was used in a WhatsApp status by someone she didn't know. I deleted most of my photos and now I only use my account to read news."* — **P36**, Female, 36, Home maker, No education.

P36's account shows how cautionary advice and peer experiences influence privacy behavior. Initially dismissing her husband's warning, she changed her stance after hearing about a friend's photo misuse. This led her to delete her pictures and shift from active sharing to passive browsing, reflecting how users manage perceived risks through withdrawal rather than technical controls. Similar work with survivors of digital abuse shows that with the right guidance, people adapt by limiting risky activities and regaining a sense of safety. Choices, like disengagement, highlight how withdrawal can become a protective strategy when trust in technology feels fragile [30].

These fears are rooted in real harms. For many women, privacy is not a legal abstraction, but a daily concern tied to safety, dignity, and social standing. The consequences of data misuse can include harassment, emotional distress, reputational damage, and the curtailing of digital freedoms. As a result, privacy-protective behavior is often defensive and reactive, shaped by fear and constraint rather than empowerment. These accounts challenge platform-centered assumptions that equate access to controls with actual protection. For many users, especially women, privacy is not about managing settings, it is about avoiding risk in a hostile or indifferent system.

In our study, privacy was often interdependent rather than chosen, with women and elders depending on younger relatives to set up apps, manage accounts, and grant permissions. Unlike other studies that describe active strategies like dual accounts, selective sharing, or privacy-by-design tools, our participants' privacy boundaries were frequently decided for them. This reflects how privacy can be socially distributed and constrained by hierarchy, rather than an outcome of individual choice.

5 Discussion

Our findings illustrate that privacy and security are deeply entangled with everyday life, social expectations, and structural constraints, especially for new Internet users in South Asia. Users navigate privacy not through written policies or legal concepts, but through relationships, experiences, and emotional responses. We reflect on how our study challenges dominant assumptions in digital privacy research and design by foregrounding the limited understanding of privacy-preserving technologies among first-time smartphone users. Rather than a lack of concern, this gap stems from inaccessible interfaces, confusing consent flows, and language barriers that make privacy tools difficult to use or trust.

Our findings align with earlier work by Sambasivan et al., [73] and Naveed et al., [65], which emphasize gendered power, digital literacy, and family mediation in South Asian privacy practices, our study contributes new insights by examining users at an earlier stage of digital adoption. Unlike prior studies focused on experienced or rural users, our participants were first-time smartphone owners in low-literacy urban and peri-urban contexts. This shift reveals novel forms of privacy practice, which we term *interdependent privacy* [29, 40], *pragmatic privacy*, and *compelled consent*, describing how users navigate privacy through dependency, improvisation, and constrained choice. Our finding of *resigned consent* resonates with Turow et al.'s discussion of "digital resignation" [84], but differs in that resignation here stems from social and gendered constraints, limited digital literacy, and asymmetric power in household or shared-device settings. These findings extend prior frameworks by showing how privacy evolves during initial encounters with digital technologies.

5.1 Privacy as Unequal and Interdependent

Our study reveals that privacy is not always an individual choice, but often a condition shaped by relationships of trust, dependency, and digital literacy within the household. Many participants, especially women and older adults, reported deferring important privacy-related decisions, such as app installations, account settings, and permission configurations, to more digitally literate family members. In most cases, these individuals were younger male relatives, such as sons or nephews, who assumed the role of intermediaries between the user and the digital system.

This pattern illustrates what we term *interdependent privacy*: a condition where users do not actively negotiate their digital boundaries, but instead rely on the actions and decisions of more digitally literate family members. In many households, younger relatives, often sons or nephews, install apps, configure settings, and decide what permissions to grant. Users who lack digital literacy depend on these intermediaries, leaving them unaware of the implications of such choices. While earlier studies emphasize that people in constrained settings develop personal tactics to manage privacy risks [6, 65], our findings show that many participants did not make privacy decisions themselves, as these were instead handled by others.

In such contexts, privacy is unevenly distributed. Skills and agency are concentrated in certain family members, while others remain excluded from these processes. Privacy becomes less about individual comprehension and more about interpersonal trust. This dynamic challenges design interventions that assume the end user is the active decision-maker. For instance, work such as Jin et al., [47] and Wilkinson et al., [93] argues that clearer risk cues or glanceable notices can improve informed consent. Our data highlight that these solutions are insufficient when users are not the ones interpreting or acting on such cues in the first place.

Delegation is not always negative; it often provides necessary access for users who would otherwise struggle to navigate complex systems. Yet, this arrangement also obscures consent and reduces awareness. Many participants described confusion when unexpected app behaviors occurred, reflecting the fragility of assuming safety through trust rather than understanding. These patterns were strongly shaped by social hierarchies. Women and older adults were far less likely to be the primary decision-makers, with younger male relatives commonly assuming the role of technological authority. This reinforces both cultural and digital power asymmetries, where privacy is shaped by dependency rather than autonomy.

This interdependent model of privacy challenges dominant frameworks emphasize individual responsibility and rational choice in digital environments. These patterns illustrate how privacy choices are deeply influenced by local contextual norms like family hierarchies, gendered power, and intergenerational trust than isolated individual reasoning. Recognizing these social structures is essential for designing privacy solutions that align with how decisions are actually made in households. It shows that the notion of an independent user making informed decisions does not align with contexts where intergenerational reliance and collective trust govern behavior.

To support these users, platforms and policies must acknowledge the collective and negotiated nature of privacy within households. This could include role-based access systems, shared-use consent mechanisms, or features that provide explanations across multiple levels of literacy.

Understanding privacy as socially constructed and interdependent is critical for inclusive design. Ignoring these realities risks perpetuating exclusion and vulnerability for marginalized groups, who may never gain true control over their digital lives under current system assumptions.

5.2 Tactical Workarounds in the Absence of Power

Although many participants lacked formal privacy knowledge, they still developed tactical workarounds to limit exposure. These included avoiding personal photos, creating duplicate accounts, or locking and hiding apps with simple tools. We term this *pragmatic*

privacy: users were not passive, but active in their own ways, relying on trial, error, and peer advice.

Unlike prior work such as Bemmann et al., [15], which frames privacy as a rational risk–benefit calculation, our participants did not weigh trade-offs before adoption. Their practices emerged reactively, often triggered by negative experiences or peer warnings. Pragmatic privacy, therefore, was a protective adjustment rather than a calculated choice. Wilkinson et al., [93] assume that users act on simplified data-flow explanations. Our participants rarely sought clarity; they improvised informal mechanisms like pseudonyms or app-hiding tricks, even without knowing exactly what data was being collected.

This difference shows that clear design alone is insufficient. Users want tools that adapt to their lived practices, not just explanations. While Alkhatib et al., [9] stresses structural design failures, our findings reveal how users compensate for systemic gaps through everyday strategies. Consistent with Seberger et al. [78], several participants normalized discomfort and continued using intrusive apps. Others responded through adaptive practices, redirecting risky expressions like photos into safer alternatives such as poems or greetings.

These insights highlight pragmatic privacy as a unique form of bottom-up resilience. Where prior work stresses formal policies, rational decisions, or systemic flaws, our participants relied on improvised tactics. These strategies show expertise that is often invisible to designers, but crucial for safety in constrained contexts. Supporting these practices means strengthening, not replacing, user innovations, treating them as valid and valuable forms of privacy management.

5.3 When Consent is Compelled, not Chosen

Our participants' accounts show that consent was rarely an empowered choice, but rather a condition for access. Apps that refused to function without permissions, ride-hailing requiring location, finance apps demanding ID uploads, or social platforms insisting on camera and microphone access, created what we describe as compelled consent. Here, users gave consent not because they trusted the app, but because denial meant exclusion from essential services.

This finding differs from Bemmann et al., where decisions are framed through a privacy calculus: users weighing risks against benefits before consenting [15]. In our study, participants often recognized the risks, but had no viable alternative; refusal was not a calculated choice, but a forced compromise. Similarly, while Kim et al., shows how peer reassurance normalizes consent, our participants described an ecosystem where refusal simply broke the app, leaving no space for negotiation [48].

Our results also extend critiques raised in Seberger et al., that work highlights how discomfort is normalized over time [78]. Our participants likewise internalized discomfort, but under sharper coercion pressed "Allow" not because it felt harmless, but because it was the only way to proceed. Finally, unlike Wilkinson et al., which assumes that clearer feedback can improve decision-making [93], our participants revealed that even with transparency, agency collapses when permissions are tied to basic functionality.

The compelled consent reflects a systemic issue. Prior work often emphasizes misunderstanding, peer norms, or interface design as drivers of compliance. By contrast, our findings reveal situations where users understood the risks, but were structurally coerced into acceptance. This highlights the urgent need for consent models that allow proportional, revisable, and non-punitive controls, so that digital participation does not come at the expense of meaningful choice.

5.4 Privacy is Personal, Cultural, and Emotional

Our findings reinforce that privacy is experienced less as a legal or technical category and more as a deeply personal and emotional construct, negotiated through everyday social interactions. Participants accounts showed that what constituted a "breach" was not the collection of metadata or app tracking: concerns emphasized in Western scholarship [13], but rather the fear of being judged by family, ridiculed by peers, or harassed by strangers. This resonates with Ahmed et al., who describe how Bangladeshi women framed privacy around reputation and modesty rather than abstract notions of consent [3]. Similarly, Madianou et al., show that for Filipino migrant workers, digital privacy is entangled with family obligations and emotional labor, underscoring that privacy cannot be abstracted from cultural and relational contexts [55].

The ways in which our participants curated self-presentation using pseudonyms, neutral profile pictures, or silence in WhatsApp groups, mirror the "everyday boundary work" described in Abokhodair et al., among Arab youth, where small acts of hiding, muting, or selective sharing became strategies to navigate collective surveillance within families [1]. Building on Marwick and Boyd's et al., [57] notion of networked privacy, where users manage visibility among peers and platforms, our participants adopted similar selective sharing practices shaped by local social norms. For women in particular, privacy breaches carried moral and social consequences—threatening dignity, reputation, and even physical safety—rather than being viewed primarily as technical risks. that could harm dignity, social standing, and even physical safety.

Rather than conceptualizing privacy as a universal right or a set of static settings, our findings align with research that sees privacy as dynamic, emotional, and relational. This perspective suggests that design solutions must move beyond notice-and-consent or permission controls toward empathetic features that anticipate fear, enable recovery after incidents, and respect cultural notions of dignity. In doing so, systems would better serve users whose privacy is bound not only by individual preference, but by gender roles, family hierarchies, and collective cultural expectations. Broadly, these findings expose a lack of socio-cultural fit in current privacy frameworks, which assume independent, literate users with full control over devices and data. In contrast, our participants' practices show that privacy must be reimagined as collective, negotiated, and contextually grounded within shared-use environments.

This study does not aim for statistical generalization. The findings primarily reflect the experiences of early-stage, low-literacy smartphone users in urban and peri-urban India. These participants represent a rapidly growing segment of the Indian Internet population—individuals who are first-time adopters of smartphones and rely heavily on social learning and family mediation to navigate digital systems. Their experiences align with national reports from TRAI (2025) and IAMAI (2023), which show increasing Internet

penetration among lower- and middle-income users, particularly women and adults in smaller towns. Consequently, our insights are most applicable to similar contexts where users face linguistic, educational, and social barriers to independent digital participation.

5.5 Implications for Design and Policy

Our study reveals that many users perceive themselves as having limited control over their data, relying on others to make privacy decisions, and are concerned about being exposed when using shared phones. These findings suggest that privacy tools and policies should align with users' everyday realities, rather than assuming they act alone or understand technical terms. Below, we suggest design and policy directions that directly connect to our findings and explain how they can make a tangible difference in real life.

- **Use simple, visual, and multilingual consent screens:** Many participants found the permission messages confusing and hard to read, especially in English. Replacing long text with short steps, icons, and audio or video explanations in local languages can help users understand what they are agreeing to. This would make users more confident and less dependent on others for help.
- **Let users try apps before giving full permissions:** Several participants felt forced to allow all permissions just to open an app. Giving users access to limited features first and then gradually asking for permissions can help build trust. In practice, this would prevent people from clicking "Allow" without understanding its implications. Beyond staged access, apps should also clearly explain why each permission is needed. For example, location access enables navigation or contact access, which supports sharing our location with friends. Such contextual prompts help users differentiate between essential and optional permissions, reducing confusion and improving informed consent.
- **Add options for shared or family phone use:** Many users, especially women and young people, shared their phones with others. Features such as guest modes, separate profiles, or easy account switching can help protect personal data in shared use situations. This would make smartphones safer and more convenient for families who share a single device.
- **Provide local and community-based privacy support:** Participants often asked friends or shopkeepers for help with the app settings. Setting up community tech helpers, local helplines, or in-app guides can make privacy support more accessible. This approach would build local digital literacy and provide users with trusted help when they need it.
- **Include gender-sensitive safety features by default:** The women in the study feared unwanted attention or exposure online. Features such as number masking, restricted profile visibility, and sharing of hidden media can reduce these risks. These defaults would make online spaces safer and encourage more women to participate confidently.

These recommendations translate our findings into actionable pathways for designers, policy makers, and developers. Simplified and language-inclusive consent mechanisms can reduce dependence on intermediaries, while family-aware and community-supported tools recognize privacy as shared and negotiated rather than purely individual. Gender-sensitive defaults further ensure that privacy frameworks address the unequal risks faced by women and other vulnerable users. Effective design and policy must view privacy as collective, situated, and interdependent, requiring inclusive mechanisms that enhance user agency and trust in everyday digital interactions.

6 Conclusion and Future Work

This study shows that for many new Internet users, privacy is not an entirely individual or deliberate act, but arises through relationships of trust, dependence, and shared learning. Participants often relied on more digitally literate family members to interpret permissions or make settings decisions, while others adopted trial-and-error strategies such as hiding apps, deleting photos, or using duplicate accounts to manage risk. These behaviors reveal how privacy is shaped by limited autonomy and social hierarchy rather than conscious control.

Our findings reflect the experiences of first-time and low-literate smartphone users in urban and peri-urban India, where digital adoption is rapid, but digital literacy and confidence remain uneven. These insights are applicable to similar populations who navigate smartphones within shared or constrained environments. Future work will expand this understanding by comparing such contexts with rural populations and second-generation users, who have grown up with mobile access—to explore how privacy practices evolve with sustained exposure, digital familiarity, and infrastructural differences.

Design and policy interventions must therefore move beyond one-size-fits-all consent mechanisms and acknowledge the collective, socially embedded nature of privacy. Potential directions include role-based profiles for shared devices, simplified and layered permission systems, gender-sensitive defaults, and localized support structures such as community technology workers. These shifts would align technical protections with the cultural and social realities of emerging groups.

Future research should build on these insights by involving broader and more diverse user groups, integrating qualitative and quantitative approaches, and testing new design interventions in real-world contexts. Doing so will advance the development of privacy and security frameworks that are not only technically robust, but also socia-culturally responsive, ensuring that the next generation of users can participate safely and equitably in the digital ecosystem.

Acknowledgments

The authors used generative AI-based tools to assist in revising the manuscript text, improving readability and flow, and correcting typographical and grammatical errors. All substantive research design, analysis, and interpretation were conducted by the authors. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

[1] Norah Abokhodair and Sarah Vieweg. 2016. Privacy & social media in the context of the Arab Gulf. In *Proceedings of the 2016 ACM conference on designing interactive systems*. 672–683.

[2] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J Lee. 2020. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–28.

[3] Nova Ahmed, Mahbuba Tasmin, and Sayyed Mohammad Nasim Ibrahim. 2022. Technology for empowerment: Context of urban Afghan women. *Technology in Society* 70 (2022), 102058.

[4] Syed Ishtiaque Ahmed and et al. 2017. Biometric SIM registration in Bangladesh: Users' perceptions and implications for privacy. *ACM Transactions on Computer-Human Interaction (TOCHI)* 24, 3 (2017), 1–33.

[5] Syed Ishtiaque Ahmed, Md Romael Haque, Jay Chen, and Nicola Dell. 2017. Digital privacy challenges with shared mobile phone use in Bangladesh. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–20.

[6] Syed Ishtiaque Ahmed, Md Romael Haque, Irtaza Haider, Jay Chen, and Nicola Dell. 2019. " Everyone Has Some Personal Stuff" Designing to Support Digital Privacy with Shared Mobile Phone Use in Bangladesh. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–13.

[7] Mahdi Nasrullah Al-Ameen, Tanjina Tamanna, Swapnil Nandy, MA Manazir Ahsan, Priyank Chandra, and Syed Ishtiaque Ahmed. 2020. We don't give a second thought before providing our information: understanding users' perceptions of information collection by apps in Urban Bangladesh. In *Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies*. 32–43.

[8] Ayomipo Alademehin. 2025. The Impact of Privacy-Enhancing Technologies (PETs) on Data Governance: A New Era of Digital Trust. *Available at SSRN 5167542* (2025).

[9] Sami Alkhatib, Jenny Waycott, George Buchanan, Marthie Grobler, and Shuo Wang. 2020. Privacy by design in aged care monitoring devices? well, not quite yet!. In *Proceedings of the 32nd Australian Conference on Human-Computer Interaction*. 492–505.

[10] Anurag Aribandi, Divyanshu Agrawal, and Dipanjan Chakraborty. 2022. Note: Evaluating Trust in the Context of Conversational Information Systems for new users of the Internet. In *Proceedings of the 5th ACM SIGCAS/SIGCHI Conference on Computing and Sustainable Societies* (Seattle, WA, USA) *(COMPASS '22)*. Association for Computing Machinery, New York, NY, USA, 574–578. https://doi.org/10.1145/3530190.3534852

[11] Gonul Ayci, Murat Sensoy, Arzucan Özgür, and Pinar Yolum. 2023. Uncertainty-aware personal assistant for making personalized privacy decisions. *ACM Transactions on Internet Technology* 23, 1 (2023), 1–24.

[12] Devanuj Balkrishan, Anirudha Joshi, Chandni Rajendran, Nazreen Nizam, Chinmay Parab, and Sujit Devkar. 2016. Making and breaking the user-usage model: Whatsapp adoption amongst emergent users in India. In *Proceedings of the 8th Indian Conference on Human-Computer Interaction*. 52–63.

[13] Susanne Barth and Menno DT De Jong. 2017. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. *Telematics and informatics* 34, 7 (2017), 1038–1058.

[14] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L Mazurek, Dana Cuomo, et al. 2024. Sok: Safer digital-safety research involving at-risk users. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 635–654.

[15] Florian Bemmann and Sven Mayer. 2024. The Impact of Data Privacy on Users' Smartphone App Adoption Decisions. *Proceedings of the ACM on Human-Computer Interaction* 8, MHCI (2024), 1–23.

[16] Oussama Ben Yahya and et al. 2023. Understanding consumers' intentions to recycle electronic devices: The role of privacy and data security concerns. *Resources, Conservation and Recycling* 187 (2023), 106664.

[17] Carlos Bermejo Fernandez, Petteri Nurmi, and Pan Hui. 2021. Seeing is believing? Effects of visualization on smart device privacy perceptions. In *Proceedings of the 29th ACM International Conference on Multimedia*. 4183–4192.

[18] Adele Botha, Marlien Herselman, and Darelle van Greunen. 2010. Mobile user experience in a mlearning environment. In *Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists*. 29–38.

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

[20] Hancheng Cao, Zhilong Chen, Mengjie Cheng, Shuling Zhao, Tao Wang, and Yong Li. 2021. You recommend, i buy: How and why people engage in instant messaging based social commerce. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–25.

[21] Pew Research Center. 2019. Smartphone ownership is growing rapidly around the world, but not always equally. https://www.pewresearch.org/global/2019/02/05/smartphone-ownership/. Accessed July 2025.

[22] George Chalhoub, Martin J Kraemer, Norbert Nthala, and Ivan Flechais. 2021. "It did not give me an option to decline": A Longitudinal Analysis of the User Experience of Security and Privacy in Smart Home Products. In *Proceedings of the 2021 CHI conference on human factors in computing systems*. 1–16.

[23] Omar Chamseddine and George Candea. 2019. Towards user-centric permission models: A service-based approach. *arXiv preprint arXiv:1906.10873* (2019).

[24] Yu-Ting Cheng, Mathias Funk, Rung-Huei Liang, and Lin-Lin Chen. 2023. Seeing through things: exploring the design space of privacy-aware data-enabled objects. *ACM Transactions on Computer-Human Interaction* 30, 4 (2023), 1–43.

[25] Jiamin Dai and Joanna McGrenere. 2025. Envisioning Financial Technology Support for Older Adults Through Cognitive and Life Transitions. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. 1–24.

[26] Andy Dearden and Dorothea Kleine. 2019. Ethical standards for the ICTD/ICT4D community: A participatory process and a co-created document. In *Proceedings of the Tenth international conference on information and Communication technologies and development*. 1–5.

[27] Mrunal Dhaygude and Dipanjan Chakraborty. 2021. Rethinking Design of Digital Platforms for Emergent Users: Findings from a Study with Rural Indian Farmers. In *Proceedings of the 11th Indian Conference on Human-Computer Interaction* (Online, India) *(IndiaHCI '20)*. Association for Computing Machinery, New York, NY, USA, 62–69. https://doi.org/10.1145/3429290.3429297

[28] Fernando Dias and Ana C. R. Paiva. 2017. Pattern-Based Usability Testing. In *2017 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*. 366–371. https://doi.org/10.1109/ICSTW.2017.65

[29] Anjuli Franz and Alexander Benlian. 2022. Exploring interdependent privacy–Empirical insights into users' protection of others' privacy on online platforms. *Electronic Markets* 32, 4 (2022), 2293–2309.

[30] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. " Is My Phone Hacked?" Analyzing Clinical Computer Security Interventions With Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.

[31] Batya Friedman, Kristina Hook, Brian Gill, Lina Eidmar, Catherine Sallmander Prien, and Rachel Severson. 2008. Personlig integritet: A comparative study of perceptions of privacy in public places in Sweden and the United States. In *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*. 142–151.

[32] Aakash Gautam. 2020. Usable, acceptable, appropriable: Towards practicable privacy. *arXiv preprint arXiv:2004.07359* (2020).

[33] Google and Tata Trusts. 2017. Internet Saathi: Bridging the digital gender divide in India. https://www.ispirt.in/internet-saathi-program/. Accessed July 2025.

[34] Sophie Grimme, Susanna Marie Spoerl, Susanne Boll, and Marion Koelle. 2024. My data, my choice, my insights: women's requirements when collecting, interpreting and sharing their personal health data. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–18.

[35] Johanna Gunawan, Cristiana Santos, and Irene Kamara. 2022. Redress for dark patterns privacy harms? A case study on consent interactions. In *Proceedings of the 2022 symposium on computer science and law*. 181–194.

[36] Hana Habib, Megan Li, Ellie Young, and Lorrie Cranor. 2022. "Okay, whatever": An evaluation of cookie consent interfaces. In *Proceedings of the 2022 CHI conference on human factors in computing systems*. 1–27.

[37] Muhammad Haris, Syed Rizvi, and et al. 2014. A survey of privacy leakage detection in mobile computing. *International Journal of Computer Applications* 107, 11 (2014), 1–5.

[38] John B Horrigan. 2000. *New Internet users: What they do online, what they don't, and implications for the net's future*. Pew Internet & American Life Project Washington, DC.

[39] Soheil Human and Florian Cech. 2020. A human-centric perspective on digital consenting: The case of gafam. In *Human Centred Intelligent Systems: Proceedings of KES-HCIS 2020 Conference*. Springer, 139–159.

[40] Mathias Humbert, Benjamin Trubert, and Kévin Huguenin. 2019. A survey on interdependent privacy. *ACM Computing Surveys (CSUR)* 52, 6 (2019), 1–40.

[41] Tanzil Hussain and MM Rahman. 2012. Privacy concerns in mobile phone use in Bangladesh: A user perspective. *South Asian Journal of Information Technology* 6, 2 (2012), 134–142.

[42] Internet and Mobile Association of India (IAMAI) and Kantar. 2024. *Internet in India 2024*. Technical Report. IAMAI. Accessed: November 2025.

[43] Renza Iqbal. 2021. Gendering of smartphone ownership and autonomy among youth: narratives from rural India. *arXiv preprint arXiv:2108.09788* (2021).

[44] Steven J Jackson. 2014. Rethinking repair. In *Media Technologies: Essays on Communication, Materiality, and Society*. MIT Press, 221–240.

[45] Steven J Jackson and et al. 2017. Surveillance and the infrastructures of dispossession: Platforms, markets, and technologies of extraction in India. *Surveillance & Society* 15, 3/4 (2017), 712–719.

[46] Steven J Jackson and et al. 2018. Developing World Security and Privacy: Reframing Research and Design. In *Workshop on Security and Privacy in the Developing World at IEEE S&P*.

[47] Haojian Jin, Hong Shen, Mayank Jain, Swarun Kumar, and Jason I Hong. 2021. Lean privacy review: Collecting users' privacy concerns of data practices at a low cost. *ACM Transactions on Computer-Human Interaction (TOCHI)* 28, 5 (2021), 1–55.

[48] JaeWon Kim, Soobin Cho, Robert Wolfe, Jishnu Hari Nair, and Alexis Hiniker. 2025. Privacy as Social Norm: Systematically Reducing Dysfunctional Privacy Concerns on Social Media. *Proceedings of the ACM on Human-Computer Interaction* 9, 2 (2025), 1–39.

[49] Leah Jerop Komen. 2016. "Here you can use it": Understanding mobile phone sharing and the concerns it elicits in rural Kenya. (2016).

[50] Jess Kropczynski, Reza Ghaiumy Anaraky, Mamtaj Akter, Amy J Godfrey, Heather Lipford, and Pamela J Wisniewski. 2021. Examining collaborative support for privacy and security in the broader context of tech caregiving. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–23.

[51] Ponnurangam Kumaraguru and Niharika Sachdeva. 2014. Privacy4ICTD in India: Exploring Perceptions, Attitudes and Awareness about ICT Use. *arXiv preprint arXiv:1410.3942* (2014).

[52] Leantros Kyriakoullis and Panayiotis Zaphiris. 2016. Culture and HCI: a review of recent cultural studies in HCI and social networks. *Universal Access in the Information Society* 15, 4 (2016), 629–642.

[53] Alexandra Lavranou and et al. 2023. Unraveling the complexity of mobile application permissions: Strategies to enhance users' privacy education. *Computers & Security* 128 (2023), 102700.

[54] Anna Lenhart, Sunyup Park, Michael Zimmer, and Jessica Vitak. 2023. " You Shouldn't Need to Share Your Data": Perceived Privacy Risks and Mitigation Strategies Among Privacy-Conscious Smart Home Power Users. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW2 (2023), 1–34.

[55] Mirca Madianou. 2019. Migration, transnational families, and new communication technologies. *The handbook of diasporas, media, and culture* (2019), 577–590.

[56] Karola Marky, Alina Stöver, Sarah Prange, Kira Bleck, Paul Gerber, Verena Zimmermann, Florian Müller, Florian Alt, and Max Mühlhäuser. 2024. Decide yourself or delegate-user preferences regarding the autonomy of personal privacy assistants in private IoT-equipped environments. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–20.

[57] Alice E Marwick and Danah Boyd. 2014. Networked privacy: How teenagers negotiate context in social media. *New media & society* 16, 7 (2014), 1051–1067.

[58] Aleecia M McDonald, Robert W Reeder, Patrick Gage Kelley, and Lorrie Faith Cranor. 2009. A comparative study of online privacy policies and formats. In *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 37–55.

[59] Indrani Medhi, Somani Patnaik, Emma Brunskill, SN Nagasena Gautama, William Thies, and Kentaro Toyama. 2011. Designing mobile interfaces for novice and low-literacy users. *ACM Transactions on Computer-Human Interaction (TOCHI)* 18, 1 (2011), 1–28.

[60] Vikram Mehta, Daniel Gooch, Arosha Bandara, Blaine Price, and Bashar Nuseibeh. 2021. Privacy care: A tangible interaction framework for privacy management. *ACM Transactions on Internet Technology (TOIT)* 21, 1 (2021), 1–32.

[61] Nicole Meng, Dilara Kekülüoğlu, and Kami Vaniea. 2021. Owning and sharing: Privacy perceptions of smart speaker users. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–29.

[62] Siphokazi Mgiba and Piyush Shukla. 2024. The influence of perceived invasiveness of mobile banking on adoption in emerging markets. *Journal of African Business* (2024). Early access.

[63] Mahdi H Miraz and Marie Haikel-Elsabeh. 2019. Analysis of Users' Behaviour and Adoption Trends of Social Media Payment Platforms. In *2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*. IEEE, 197–202.

[64] Savanthi Murthy, Karthik S Bhat, Sauvik Das, and Neha Kumar. 2021. Individually vulnerable, collectively safe: The security and privacy practices of households with older adults. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 1–24.

[65] Sheza Naveed, Hamza Naveed, Mobin Javed, and Maryam Mustafa. 2022. " Ask this from the person who has private stuff": Privacy Perceptions, Behaviours and Beliefs Beyond WEIRD. In *CHI Conference on Human Factors in Computing Systems*. 1–17.

[66] Telecom Regulatory Authority of India (TRAI). 2025. *The Indian Telecom Services Performance Indicators: January–March 2025*. Technical Report. TRAI. Accessed: November 2025.

[67] Tunbosun Oyewale Oladoyinbo, Oluseun Babatunde Oladoyinbo, and Adeyemo Isiaka Akinkunmi. 2024. The Importance Of Data Encryption Algorithm In Data Security. *Current Journal of International Organization of Scientific Research Journal of Mobile Computing & Application (IOSRJMCA)* 11, 2 (2024), 10–16.

[68] Jaehyun Park, Sung H Han, Hyun K Kim, Youngseok Cho, and Wonkyu Park. 2013. Developing elements of user experience for mobile phones and services: survey, interview, and observation approaches. *Human Factors and Ergonomics in Manufacturing & Service Industries* 23, 4 (2013), 279–293.

[69] Matt Pinch and S. I. Ahmed. 2022. Being Seen on the App: The Politics of Visibility for Queer Men in India Using Geosocial Apps. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. ACM, 1–15.

[70] Donagani Ramakrishna and Mohammed Ali Shaik. 2024. A comprehensive analysis of cryptographic algorithms: Evaluating security, efficiency, and future challenges. *IEEE Access* (2024).

[71] Lubna Razaq, Tallal Ahmad, Samia Ibtasam, Umer Ramzan, and Shrirang Mare. 2021. " We Even Borrowed Money From Our Neighbor" Understanding Mobile-based Frauds Through Victims' Experiences. *Proceedings of the ACM on human-computer interaction* 5, CSCW1 (2021), 1–30.

[72] Amina Saeed. 2024. Perceptions of usability and trust in mobile app permissions: A study from Saudi Arabia. *Journal of Cyber Policy* (2024). In press.

[73] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. " Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 127–142.

[74] Nithya Sambasivan and Jess Holbrook. 2018. Toward responsible AI for the next billion users. *Interactions* 26, 1 (2018), 68–71.

[75] Eva-Maria Schomakers, Chantal Lidynia, and Martina Ziefle. 2022. The role of privacy in the acceptance of smart technologies: Applying the privacy calculus to technology acceptance. *International Journal of Human–Computer Interaction* 38, 13 (2022), 1276–1289.

[76] Valentin Schwind, Netsanet Zelalem Tadesse, Estefania Silva da Cunha, Yeganeh Hamidi, Soltan Sanjar Sultani, and Jessica Sehrt. 2025. A Scoping Review of Informed Consent Practices in Human-Computer Interaction Research. *ACM Transactions on Computer-Human Interaction* (2025).

[77] John S Seberger, Hyesun Choung, Jaime Snyder, and Prabu David. 2024. Better living through creepy technology? exploring tensions between a novel class of well-being apps and affective discomfort in app culture. *Proceedings of the ACM on human-computer interaction* 8, CSCW1 (2024), 1–39.

[78] John S Seberger, Irina Shklovski, Emily Swiatek, and Sameer Patil. 2022. Still creepy after all these years: The normalization of affective discomfort in app use. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–19.

[79] Sujay Basavaraj Shalawadi. 2025. Shaping User Privacy Experiences in Self-Tracking and Smart Homes: A Design Artifact Approach. (2025).

[80] Bo Shen and et al. 2021. A global study of privacy information collection on Android devices. *IEEE Transactions on Mobile Computing* 20, 9 (2021), 2693–2708.

[81] Sheetal Shrivastava and Rajeev Tripathi. 2020. Privacy issues of Android application permissions: A literature review. *International Journal of Computer Applications* 176, 30 (2020), 1–5.

[82] Mohammad Tahaei and et al. 2023. A dual perspective on mobile app permissions: User expectations and developer practices. *Digital Policy, Regulation and Governance* (2023).

[83] Yu-Ying Tu, Chia-Chi Hsu, and Frendy Creativani. 2022. Second-hand luxury goods purchase: The effects of customer value and perceived risk. *Sustainability* 14, 16 (2022), 10397.

[84] Joseph Turow, Michael Hennessy, and Nora Draper. 2015. The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. *Available at SSRN 2820060* (2015).

[85] https://legal.thomsonreuters.com/en/insights/articles/the-basics-usage-and-privacy-concerns-of-biometric-data. 20 July 2022. The basics, usage, and privacy concerns of biometric data. Accessed: 1 September, 2025.

[86] https://nextbillionusers.google/research/. 2023. Mobile devices are too expensive for billions of people — and it's keeping them offline. Accessed: 17 January, 2023.

[87] https://www.moneycontrol.com/technology/kolkata-woman-alleges-phone-repair-shop-leaked-her-personal-videos-online-article-13494830.html. 29 August 2025. Kolkata woman alleges phone repair shop leaked her personal videos online. Accessed: 1 September, 2025.

[88] https://www.pewresearch.org/internet/2019/03/07/use-of-smartphones-and-social-media-is-common-across-most-emerging-economies/. 2023. Use of smartphones and social media is common across most emerging economies. Accessed: 13 September, 2023.

[89] https://www.statista.com/statistics/792074/india-internet-penetration-rate/. 2023. Internet penetration rate in India from 2007 to 2022. Accessed: 13 September, 2023.

[90] Pratiksha Vaidehi and Ravi Singh. 2021. Caste, gender, and digital literacy: Privacy and security among marginalized users in India. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*. 702–713.

[91] Dinuka Wijetunga. 2014. The digital divide objectified in the design: Use of the mobile telephone by underprivileged youth in Sri Lanka. *Journal of Computer-Mediated Communication* 19, 3 (2014), 712–726.

[92] Wikipedia contributors. 2025. Mobile App Permissions. https://en.wikipedia.org/wiki/Application_permissions. Accessed July 2025.

[93] Daricia Wilkinson, Paritosh Bahirat, Moses Namara, Jing Lyu, Arwa Alsubhi, Jessica Qiu, Pamela Wisniewski, and Bart P Knijnenburg. 2020. Privacy at a glance: the user-centric design of glanceable data exposure visualizations. *Proceedings on Privacy Enhancing Technologies* (2020).

[94] Cheng Xu, Xueji Liang, Yanqi Sun, and Xudong He. 2023. Fraudsters Beware: Unleashing the Power of Metaverse Technology to Uncover Financial Fraud. *International Journal of Human–Computer Interaction* (2023), 1–16.

[95] Haozhe Zhou, Mayank Goel, and Yuvraj Agarwal. 2024. Bring privacy to the table: Interactive negotiation for privacy settings of shared sensing devices. In

Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems. 1–22.

[96] Yixin Zou, Shawn Danino, Kaiwen Sun, and Florian Schaub. 2019. YouMight'Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–14.

A Interview Script

A.1 Moderator Instructions

Moderator instructions refer to guidelines or directions provided to the individual who will be moderating a discussion. These instructions are intended to ensure that the moderator understands their role, responsibilities, and the specific expectations for facilitating the discussion effectively. The content and details of moderator instructions can vary based on the nature of the participants. For the participants for whom we conducted the survey following are the moderator instructions:

(1) Work on building a strong rapport. Be personable.
(2) Offer some examples to help the participants open up from their own stories.
(3) Always ask for consent before the interview. Ask for permission.

A.2 Interview Script

Hi, thank you for providing the opportunity to talk to you. My name is X, and these are Y and Z.

Today, we are researching what it means to be a new Internet user and the perspectives of participants while using the Internet on smartphones. Everything you know and use daily. This is not an exam, everything you say is going to be helpful to us.

We encourage you to be frank and open, so we can learn how you are using phones and improve the experience overall. If you are uncomfortable, just let us know. Everything we discuss today is confidential.

Could I get your permission to record this interview? It will be stored confidentially and will be used for research purposes only. If you feel uncomfortable, just let us know. Any questions?

A.3 Questionnaire

We describe the talking points used in the interviews and the mapping with the Research Questions.

(1) General Mobile Use:
   - What do you mainly use your phone for? (For example, do you use it for calling, texting, WhatsApp, watching videos, checking bank balance, or anything else?) [RQ1, RQ2]
   - Do you share your phone with others? If yes, with whom and how often? (Who uses it: your family, friends, or someone else? How often do they use it?) [RQ1, RQ2]
(2) Awareness and Perceptions
   - What are your favorite apps or features on your phone? (Why do you use those apps: for chatting, shopping, learning, and entertainment? Have you ever thought about what information these apps might be collecting from your phone?) [RQ1, RQ3]
   - When an app asks for permission, like to access your location, camera, or contacts, do you read and understand what it means? (Do you allow it without thinking, or do you ask someone, or decide based on your own judgment?) [RQ1, RQ3]
   - How do you decide whether an app or website is safe to use? (Do you trust it if it's popular? If friends use it? If it looks professional?) [RQ1, RQ2]
(3) Practices and Behaviors
   - Have you ever deleted a message, photo, or app because you didn't want someone to see it? (Can you share what made you do that? Was it for privacy or to avoid conflict?) [RQ2]
   - If your phone stops working and you need to give it for repair, what do you do before handing it over? (Do you clear your data, remove photos, or just give it as is?) [RQ2, RQ3]
   - Have you ever asked someone (friend/repairer/child) to help you with a phone problem? How did you feel about them seeing your personal data? (How did you feel about them seeing your photos or private messages while helping?) [RQ1, RQ2]
(4) Trust and Sharing
   - Who do you trust most when sharing personal or sensitive information? (E.g., in-person vs. over the phone or via apps). When you need to share something private (like bank info or personal messages), who do you trust more: talking in person, calling, or using apps like WhatsApp or SMS? [RQ1, RQ2]
   - Have you used code words, nicknames, or indirect language to keep something private? (Can you give an example: like talking in jokes, slang, or using another language?) [RQ2]
(5) Digital Literacy and Consent
   - Have you ever helped someone install or use an app? What did you explain to them? (What things did you explain to them? Did you talk about privacy or safety?) [RQ1, RQ2]
   - Do you know how to stop an app from using your camera, microphone, or location? (Have you ever done this before or seen anyone do it?) [RQ1, RQ3]
   - When you get a warning message (e.g., "this app may harm your phone"), what do you usually do? (Do you install it anyway, uninstall it, or ask someone for help?) [RQ1, RQ3]
   - What do you think happens when you give an app access to your contacts or photos? (Do you think it stores it, shares it, or uses it for ads?) [RQ1, RQ3]
(6) Privacy and Repair
   - Have you ever hesitated to take your phone for repair because of private content? (Like photos, chats, bank info, or other personal things?) [RQ2, RQ3]
   - Has a repair person, friend, or shopkeeper ever opened your gallery or apps without asking while using or fixing your phone? How did you feel? (Did you say anything to them? Did it bother you?)[RQ2, RQ3]
   - Do you use a password or lock screen on your phone? Why or why not? (Does anyone else know your password?) [RQ2, RQ3]
(7) Trust and Social Influence
   - Do you think apps from local developers are safer than international ones? Why? (What makes you feel something

is trustworthy: language, popularity, or something else?) [RQ2]
- Who do you turn to when you don't understand a phone or app setting? (Do you ask family, children, shopkeepers, or friends?) [RQ1, RQ2]
- Do people around you (family, friends, shopkeepers) influence the way you think about online safety? (Have they given you any advice or taught you anything about staying safe online?) [RQ1, RQ2]

(8) Scenario-based questions:
- Broken Phone: Imagine your phone suddenly stops working, and you need to take it to a local repair shop. It has your photos, bank app, and personal messages. What do you do before handing it over? Do you delete things? Do you worry about the repair person accessing your content? [RQ3]
- Sharing a Phone with Family: Let's say your sibling or spouse often borrows your phone. You get a message from someone private. What do you do? Do you hide apps? Use patterns? Delete messages? [RQ2]
- Installing a New App: A new app promises rewards or entertainment, but asks for access to your contacts and location. Would you install it? What do you consider before saying yes? Do you know what these permissions mean? [RQ1]
- Helping an Elderly Relative: Your older relative has a smartphone, but doesn't understand permissions. They ask you to install a health or finance app for them. What do you do? Do you explain the permissions? Do you think it's important for them to understand? [RQ1, RQ2]
- Using a Borrowed Phone: Imagine you're using a friend's or relative's phone to check something online. You see a private photo or message pop up. What would you do? Do you tell them? Ignore it? Does this ever happen? [RQ1, RQ2]
- Selling or Giving Away a Phone: You plan to give your old phone to someone else. What steps do you take before handing it over? Do you delete apps? Format it? Worry about any leftover data? [RQ2, RQ3]
- Cloud Backup Surprise: You delete photos from your phone, but later find out they are still on Google Photos or iCloud. How would you react? [RQ1, RQ3]
- Using Free Public WiFi: You find free WiFi at a cafe and need to check your bank account. Would you connect? Why or why not? What steps would you take? [RQ2, RQ3]
- Receiving a lottery: Imagine you ever receive a call from a number you don't recognize, stating that you have won 1 lakh in a lucky draw. Would you give your details? [RQ3]
- Sharing account details: Your friend is out of town and runs into an emergency that requires a money transfer since their bank account does not have enough money. Will you transfer the money? Why or why not? [RQ1, RQ2]

A.4 Artifact Availability

The anonymized dataset and interview guide used in this study are available at: https://github.com/Priyankapopuri08/PoPETs-Understanding-Privacy-Practices.git

B Participant Table

Table 1: List of all participants

Participant	Gender	Age	Occupation	Education
P1	F	36	House Helper	3rd standard
P2	F	19	Student	B.Tech (pursuing)
P3	F	58	Home-maker	12th standard
P4	F	47	Home-maker	MBA
P5	M	43	Watchman	5th standard
P6	M	45	Rikshaw Driver	10th standard
P7	F	19	Student	B.Com (pursuing)
P8	F	38	Tailor	8th standard
P9	F	44	Tailor	5th standard
P10	M	26	Delivery boy	12th standard
P11	F	54	Homemaker	8th standard
P12	F	31	Construction worker	6th standard
P13	F	38	Construction worker	8th standard
P14	M	24	Delivery boy	10th standard
P15	M	39	Construction worker	4th standard
P16	F	30	Construction worker	4th standard
P17	F	27	Tailor	6th standard
P18	F	34	Tailor	8th standard
P19	F	35	Homemaker	5th standard
P20	M	22	Student + part time work	B.Com
P21	F	42	Construction worker	5th standard
P22	F	22	Student	B.Tech
P23	F	50	Homemaker	5th standard
P24	M	28	Delivery boy (e-commerce)	10th standard
P25	M	31	Construction worker	6th standard
P26	F	31	Tailor	10th standard
P27	M	35	Shopkeeper	12th standard
P28	F	35	Tailor	6th standard
P29	M	38	Farmer	2nd standard
P30	F	39	Tailor	7th standard
P31	M	22	Student	B.Tech
P32	F	40	Shopkeeper	2nd standard
P33	M	22	Student	B.Tech
P34	F	40	Tailor	3rd standard
P35	M	28	Construction worker	4th standard
P36	F	36	Home maker	No education
P37	F	26	Tailor	10th standard
P38	M	42	Bus conductor	8th standard
P39	M	22	Student	B.Com
P40	M	31	Rikshaw Driver	8th standard
P41	M	22	Student + part time work	B.Tech
P42	F	56	House helper	No education
P43	M	34	Tailor	6th standard
P44	M	36	Tailor	No education
P45	M	44	Shop helper	2nd standard
P46	M	29	Delivery boy	4th standard
P47	M	39	Watchman	No education
P48	F	38	Homemaker	MBA
P49	M	58	Construction work	No education
P50	M	41	Construction work	6th standard

C Code Book

Table 2: Lists all the codes obtained by qualitative analysis of interview data. The count of the code or theme was derived by aggregating participant responses.

Code/Theme	Count
Perceived Lack of Control	**66**
Forced Consent – Permissions appeared suddenly and had to be accepted to continue.	16
No Real Choice – Users allowed access even when mistrustful, as apps would not work otherwise.	20
Compelled by Services – Essential apps (e.g., finance) forced ID submission to function.	12
Blind Trust in Defaults – Users assumed default settings were correct and never changed them.	10
Mistrust, but Compliance – Despite discomfort, users shared data when apps insisted.	8
Eschewal of terms and policies	**53**
Skipping Permissions – Complex permission requests were skipped without reading.	14
Ignoring Settings – Users never checked app settings due to lack of understanding.	9
Withdrawal from Use – Some stopped using apps entirely when they felt confused.	11
Trial and Error – Users experimented by installing/uninstalling until something worked.	12
Avoiding English Interfaces – Apps in English were avoided until explained by someone else.	7
Delegating Digital Decisions	**59**
Intergenerational Help – Younger family members set up phones and apps for elders.	14
Trust in Relatives' Choices – Users assumed apps chosen by relatives were safe.	11
Dependence on Children – Children were relied upon to install or manage apps.	9
Gendered Delegation – Husbands/men handled phone settings for women.	7
Shopkeeper/Repair Reliance – Shopkeepers or repairmen made phone decisions.	8
Silent Acceptance – Users did not question what helpers did on their phones.	10
Everyday Privacy Workarounds	**73**
Content Substitution – Instead of personal photos, users shared poems or greetings.	13
Multiple Accounts – Users created duplicate accounts for different audiences.	10
Locking/Hiding Apps – Apps were locked or hidden from others in the household.	15
Immediate Deletion – Sensitive content was deleted right after viewing.	12
Code Words & Slang – Nicknames or slang were used to hide meaning.	9
Offline Alternatives – Private conversations were moved offline.	8
Device Sharing Rules – Users set verbal rules for family when sharing devices.	6
Fear of Exposure and Harm	**71**
Repair Shop Risks – Concern that repairmen may access private content.	12
Family/Household Exposure – Fear that relatives may see private chats/photos.	14
Community Stories of Misuse – Stories of others' photos being misused influenced caution.	11
Harassment by Strangers – Fear of unwanted calls or harassment from leaked numbers.	10
Fear of Financial Fraud – Avoided online banking due to fraud risk.	9
Reputation Damage – Fear of relatives judging private messages.	8
Gendered Harassment – Women avoided sharing photos to prevent misuse.	7