Misinformed Consent: A Targeted Investigation of Application Permission Abuse in the Low-Literate Demographic

ANONYMOUS AUTHOR(S)

In this paper, we explore the idea of informed consent in digital financial applications, especially in the context of low-literate populations. We analyse a collection of 37 popular loan, gambling and trading applications uncovering four key issues:(1) Inadequacy or absence of privacy policies, (2) Unnecessary access to sensitive user data (3) Discrepancies between declared and used permissions (4) Active applications despite negative reviews and fraud allegations. Our survey of blue-collar workers reveals widespread use but lack of informed consent, low reporting, unawareness, and self-blame. Combined with insufficient oversight from the Play Store, these apps persist and exploit users. Our controlled experiments suggest that complex privacy policies and lack of contextual information in application permissions significantly impedes informed consent, highlighting the need for more accessible and comprehensible privacy disclosures.

CCS Concepts: • **Security and privacy** → *Social aspects of security and privacy*; • **Human-centered computing** → **User studies**; • **Social and professional topics** → *Privacy policies*.

Additional Key Words and Phrases: informed consent, low literacy users, financial fraud, Loan Apps, Gambling Apps, privacy policies, MobSF, LLM-based interventions, Play Store oversight, user protection

1 Introduction

Predatory financial applications are mobile apps designed to exploit unsuspecting users. Previous work in this space shows that such applications are largely unregulated [30, 35], are typically disseminated through unofficial channels [20] and often accused of serious privacy violations where they can access a user's personal and confidential data. These applications often target vulnerable individuals, such as those in financial distress, and those prone to addiction. Apps under the predatory loan category offer quick and easy loans at low collateral but end up charging exorbitant interest rates and hidden fees, often leading to a debt cycle [9]. They are also associated with aggressive and coercive debt collection practices, often resulting in harassment, intimidation, and even blackmail using private and personal data [3, 9, 10, 28].

Similarly, exploitative gambling applications prey on compulsive gambling behavior, leading to monetary and emotional harm. They typically offer easy installs and starting balances, use deceptive practices such as "free-to-play", and often end up collecting and exploiting personal information for fraudulent purposes [18]. Another popular example is trading apps [2, 7, 39] that offer easy entry into volatile markets such as cryptocurrency without proper risks disclosure.

Given this complicated landscape of unethical profiteering, it is important to research and verify financial apps before installing them. Most application have a *User Agreement*, *Privacy Policy*, or *Terms of Service* that users must accept. Typically, this includes information on data collection and third-party sharing. Most users do not read these lengthy documents where information is often buried in fine prints, giving consent without fully understanding the implications. Often these applications do not fully disclose what data they collect and use. When an application is installed for the first time, it requests access to certain features such as location, contacts, camera and microphone, etc. A user must review and approve/deny these requests. However, many users accept these permissions without reviewing or understanding what data is being collected and why.

In this paper, we explore the idea of informed consent in digital financial applications, especially in the context of low-literate populations. We analyse a collection of 37 loan, gambling and trading applications chosen due to their popularity and heavy usage in the targeted demographic. We define informed consent as the ability to comprehend and willingly agree to the terms and conditions of a service, with full knowledge of the potential risks and benefits [34, 36]. We define low-literacy as the "inability to read and understand information at a basic level" and define individuals who read, write, or speak at or below the eighth-grade level as low-literate [24]. Exploration of this problem is important for various reasons. First, there are approximately 754 million illiterate adults worldwide, two-thirds of whom are women [38]. Many more are considered functionally illiterate with limited reading and writing skills. On the other hand, smartphone penetration among the low-literate population has grown rapidly. By 2024, 3.5 billion people are expected to own a phone, most of whom are in the low-literate/semi-literate demographics. Studies show that these groups have learnt to navigate smartphones using various techniques, such as icon recognition, voice commands, asking younger relatives for help, and memorizing patterns [19]. We argue that despite being functional on mobile devices, a large set of users cannot fully comprehend applications' privacy policies and permissions, etc.

We conduct an in-depth survey of primarily low-literate blue-collar workers to assess their mobile usage habits. Users often install and use insecure/untrusted financial applications, most of them do not read and/or understand the terms and conditions and permissions, do not fully understand the risks and implications, and are unaware of their exposure. Also, popular digital financial applications often collect excessive and unnecessary permissions, and show a lack of transparency. Terms and conditions are often vague, incomplete or highly obfuscated. In the second part of the paper, we design and implement LLM-based interventions to address these issues and evaluate their impact in controlled settings. Our findings suggest that the complexity of privacy policy language and the lack of contextual information in application permissions significantly impedes informed consent, highlighting the need for more accessible and comprehensible privacy disclosures.

2 Overview of Problem Space

The low-literate demographic faces many problems when interfacing with technology [23, 24]. This holds especially true for mobile applications as the pace of evolution in this domain is fast. Below, we highlight some of these issues:

2.1 Lack of Understanding and "Informed" Consent:

Users in the low-literate population have a poor understanding of the mobile ecosystem. This lack of understanding is expected because most such users lack the resources to educate themselves about how companies profit from their behavior and indulgence. The survey that we conducted underscores several important points. For instance, 83% of users do not pay attention or understand permissions, nor do they comprehend their ability to be abused by application developers [17]. In cases where users do have some notion of how permissions can be abused, they struggle to understand privacy policies due to language barriers or cannot navigate the often vague language, and misleading details that are deliberately put by developers to hide their true intent behind collecting user data. Surely, consent given by users in these situations cannot be categorized as informed.

2.2 Collective Ignorance:

Members of a group who are largely uninformed about the risks and implications of certain actions often develop a false sense of security as everyone simply assumes others are more knowledgeable and are making the right decisions. This phenomenon is described as *Collective or Pluralistic Ignorance* [26] and is often the underlying cause of several bandwagon trends observed among a particular stratum of society. Low-literate mobile users are no exception. Users tend to trust apps without question when they see others using them, granting permissions easily. As a result, once an app gains enough users, developers can potentially engage in unethical practices, like mass data collection, with little resistance. Hence, low-literate continue to fall into the pitfalls of this vicious ecosystem.

2.3 Addictive Nature of Applications:

Another issue worth highlighting is that some applications that are popular in the blue-collar community tend to be addictive. For instance, gambling applications, which lure users in with false promises of quick rewards and "easy money," rely on the *Hook Model* [15] to keep enticing users to return to the application. These tricks rely on dishing out intermittent rewards at downstream milestones, which prolongs the gameplay.

2.4 Poor Grasp of Interest Structure:

Like gambling, microfinance apps are also widespread in the low-literate population, especially daily-wage workers, and small loan programs (often called microloans). However, some respondents from our survey, reported that they did not have access to the interest structure of the loan or could not easily find the terms and conditions of the loan. Even though this does not directly pertain to application permissions, it does fall under the larger umbrella of information hiding. Trapping vulnerable users, who are struggling to make ends meet, into the vicious cycle of interest-based installments without disclosing interest rates and penalties borders extortion.

2.5 Difficulty Navigating Modern Interfaces:

Usage patterns among low-literate users show limited use and application of mobile phones [12]. Instead, users in this demographic prefer to manually document information where needed [21]. Furthermore, focus more on voice and graphic-based interfaces as much as possible [21, 29], avoiding complex interfaces [5]. In fact, first-time users are unable to use textual interfaces altogether [24, 25]. These struggles partially explain why users from this demographic remain unaware of advanced features, limiting their engagement and experience [22, 27]. Again, this issue highlights the indifference of application developers towards the needs and concerns of the low-literate population.

2.6 Susceptibility to Scams And Dubious Practices:

Due to several factors, low-literate users are more vulnerable on their phones and online. Interfaces are complex and a lack of tailored design exacerbates their difficulty accessing essential information [14, 31]. Furthermore, they are likelier to misunderstand the context of applications, accidentally triggering in-app purchases, even making them more susceptible to phishing [24, 31]. There is also a lack of familiarity with well-known sources and a preference for multimedia, which results in the inability to discern misinformation, emotional reactions to misleading content, poor decision-making, and easier susceptibility to scams [4, 11, 37].

Socioeconomic challenges and low-literacy are tightly coupled and lead to starting phone engagement at a much later stage, a reliance on peers, and perceived low self-efficacy [33] These users in the lowest income bracket are more

than twice as likely to suffer due to online scams, are more likely to report reputation damage and have their accounts compromised. Despite this, individuals from economically disadvantaged backgrounds are often more comfortable sharing personal data, likely due to a limited understanding of the potential risks or a trade-off for free services [3, 8, 28].

2.7 Poor Cybersecurity Hygiene:

Low-literate users often struggle to understand security/privacy settings; often remaining unaware of these features. Most users tend to stick with the provided default settings. However, as demonstrated in our survey, when informed about these options, users can adjust their privacy settings. Some are even willing to pay small fees in exchange for fewer permission requirements, indicating a desire for more streamlined control over their data [3, 33].

3 Methodology

Here, we conduct a baseline user-survey among mostly illiterate blue-collar workers to establish that users are typically unaware of terms and conditions or potential exposure they have signed up for upon installing an application. We also explore reasons behind this phenomenon and its privacy and security implications from a user's perspective. Additionally, we also explore the discrepancies between users' perceived and actual risk.

We use Mobile Security Framework (MobSF) [1] to measure the privacy and security impact of these applications. Having established a baseline, we design and evaluate several LLM-based interventions that addresses this problem.

3.1 Survey Design

We obtained IRB approval for our survey methodology from our local institutional review board. We sampled our survey participants from blue-collar workers working in and around the industrial area in our city. The surveys were largely conducted in Urdu, the participant's native language. The interviews were one-on-one and had a series of structured and unstructured questions. We were transparent about our research's purpose, aims, and motivations. We also explained in detail why we were collecting the data, who could access it, and how it could be accessed. Our subjects were candid about the challenges they faced with technology and readily admitted when they had difficulty understanding our questions or requests. We concluded each survey by educating the participants about the potential threats and obtaining explicit approval for using their responses. Our sample had more male than female participants [6], and while both groups were low-literate, the median education level for men was primary school, whereas, for women, it was none, reflecting cultural norms prioritizing boys' education due to perceived higher economic returns [16, 32]. Table 1 shows the education level distribution split by area and gender.

Table 1. Distribution of Education Levels by Area and Gender

Category	Primary (0-3)	Middle School (4-7)	Middle and High School (7-10)
Males in Urban Areas	3.13% (1/32)	25.00% (8/32)	46.88% (15/32)
Males in Rural Areas	0% (0/32)	18.75% (6/32)	28.13% (9/32)
Females in Urban Areas	9.38% (3/32)	3.13% (1/32)	3.13% (1/32)
Females in Rural Areas	9.38% (3/32)	0% (0/32)	0% (0/32)

3.2 Survey Findings

Popular Apps: We collected a detailed inventory of all apps installed on the participants' phones. The most common apps were WhatsApp (78.12%), Facebook (65.62%), TikTok (56.25%), YouTube (40.62%), JazzCash (21.88%), Ludo (18.75%), Easypaisa (15.62%), Instagram (15.62%), Snapchat (12.50%), and Play Store (9.38%). There was a variation in the finance apps used, as many used Jazzcash, Easypaisa, Paisayaar, Binance, and Nayapay. Interestingly, all our participants had the default English-based textual interface. Several participants downloaded apps from unofficial play-stores. Some Participants had 3rd parties install software for them while the majority downloaded these apps using voice commands. A typical response related to the above was: *"the girl from across the street helps me with everything ... and whenever I see a good app on TikTok, I go to her, and she sets it up for me."*

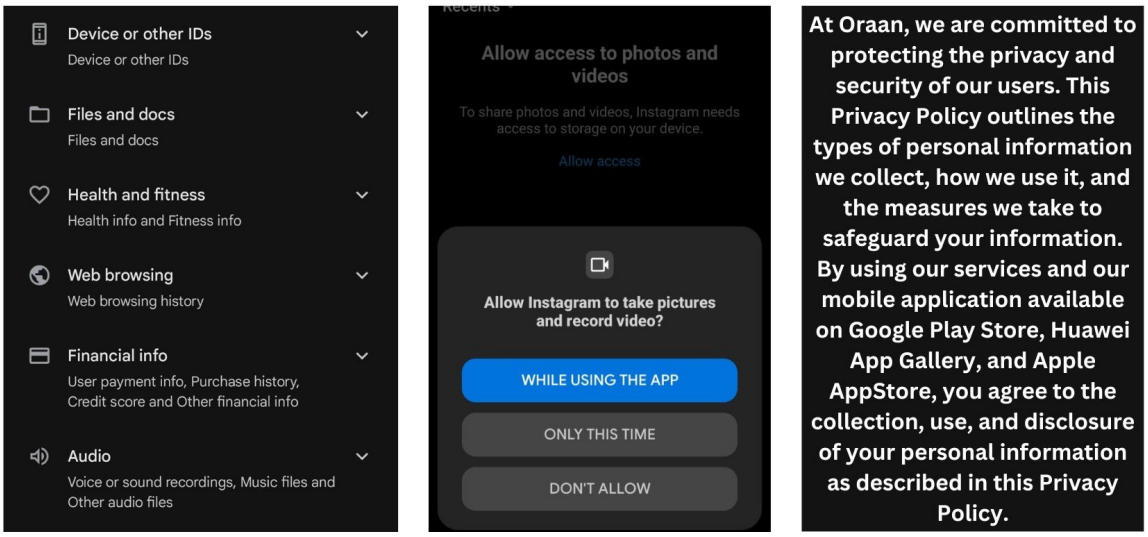

Fig. 1. We tested our participant's awareness of permissions using the ability to understand Play Store permissions (left), runtime permissions (center), and privacy policies (right).

Permissions: When prompted, the majority of the participants (all except two) reported that apps had never requested consent to access their data. In instances where apps like Facebook had access to their photos, participants struggled to comprehend how this access occurred without their direct action, such as sending or posting photos. The participants treated phone storage much like physical storage. If a photo hadn't been posted/sent online by the participant, they could not conceive how a 3rd party like an application developer could access it. To understand if the participant had any awareness whatsoever of permissions, we presented various documents, including privacy policies from different apps, and asked participants to explain what each document did. Many of them could not comprehend the purpose of these privacy policies.

Next, the interviewer opened an app on her/his phone and intentionally triggered a runtime permission request (see Figure 1 middle image). When prompted with a blue button to either accept or reject the permission to access photos and galley, nearly all users clicked on it without understanding what it meant or entailed. When asked *"What did you think the button did"* responses varied from thinking it was to delete something from the phone, to thinking it was

just one of the features of a phone. To evaluate users' understanding of app permissions and data safety, we showed them the "Data Safety" section on the Play Store page of a popular financial application. Users could recognize icons representing different types of data usage, but struggled to connect them to the app permissions they had granted. This disconnect between recognizing symbols and understanding their implications was a recurring theme in our study.

Security Awareness: All our participants identified contacts and/or photos as sensitive data. Three participants also identified banking information as sensitive data. Most considered "keeping the phone in my hand" as an adequate data security measure. *"I don't let strangers access my phone, and no one knows my password, so I don't understand how anyone could access my photos"*. When prompted with who was responsible for the data on their devices, the majority said that it was the user, while others felt that either the government or the application developer was responsible.

Key Insights:

- All respondents owned smartphones, but 97% struggled with permissions, terms, and privacy policies. 70% relied heavily on visual and oral cues due to language barriers.
- A majority of participants installed apps and took loans (22%) based on recommendations from friends or family with little or no understanding of security, privacy, or financial obligations.
- Users trusted loan apps based on brand recognition or familiarity (65%), and a majority of them (94%) were uncomfortable with financial jargon and ignored legal disclosures. Most skipped or did not understand privacy policies (96%), and a vast majority assumed mainstream platforms like Play Store were safe by default and accepted all permissions.
- Respondents took quick loans without understanding terms (interest rates, repayment conditions) due to urgency. None of them focused on interest rates as they were not expecting them to be this high.
- Around 45% of the people did not know about data protection rules, and a vast majority (85%) had no awareness of permissions. The participants were similarly confused about the responsibility of keeping data safe.
- **Gendered differences**: A significantly higher percentage of men (60%) identify photos as sensitive data compared to women(45%), on the other hand, a greater percentage of women (27% compared to 4%) wouldn't want a third party to access their contacts.
- **Gendered differences**: Women were slightly more aware than men of specific data protection regulations. Two women were aware of such regulations, citing emergency services (1122), while none of the men were aware.

4 Security analysis of the Applications

We statically analyzed the most common applications using the Mobile Security Framework (MobSF) [1]. MobSF classifies app permissions based on their potential for misuse and assesses their relevance in the context of user privacy, security, and sensitive data access. **Normal permissions** pose minimal security risks and are typically granted without user intervention and have minimal impact on personal data. **Dangerous permissions**, by contrast, involve access to sensitive user data or critical device functions (e.g., location, contacts, gallery, etc.), these require explicit consent due to their potential impact on privacy and security.

Contextual Risk Assessment: MobSF also does *context-based risk assessment* to understand the risk of different combinations of permissions. For instance, permissions like `READ_CONTACTS` or `ACCESS_FINE_LOCATION` are flagged as

high-risk, particularly when combined with network permissions such as `INTERNET`, imply that the app may track and transmit a user's location data without consent. This allows us to highlight dangerous *combinations of permissions* the can be potentially malicious. MobSF assigns a *risk score* to each app that reflects the potential for privacy violations, device manipulation, or unauthorized data access.

Key Findings: By using MobSF, we were able to analyze 37 applications, identifying several permissions (and combinations) that were flagged as particularly problematic. Figure 2 shows the number of dangerous permissions across the 37 applications that we investigated. The key insights behind these findings can be summarized as:

- **Over-Privileged Applications:** Of the 37 apps analyzed, more than 70% requested permissions beyond what would be necessary for their primary functionality. For instance, one microloan app, requested permissions to access the user's call logs and SMS history. This level of access is unnecessary for processing loans and raises concerns about whether the app is harvesting data for purposes unrelated to its core function. This kind of over-privileging was particularly prevalent among gambling and loan apps, where the collection of personal data could be used to profile users for targeted advertising or other forms of exploitation.

- **Access to Sensitive User Data:** Many application had access to sensitive user data, such as personal identifiers, location data, and media files. For example, one gambling app requested access to the device's GPS location,

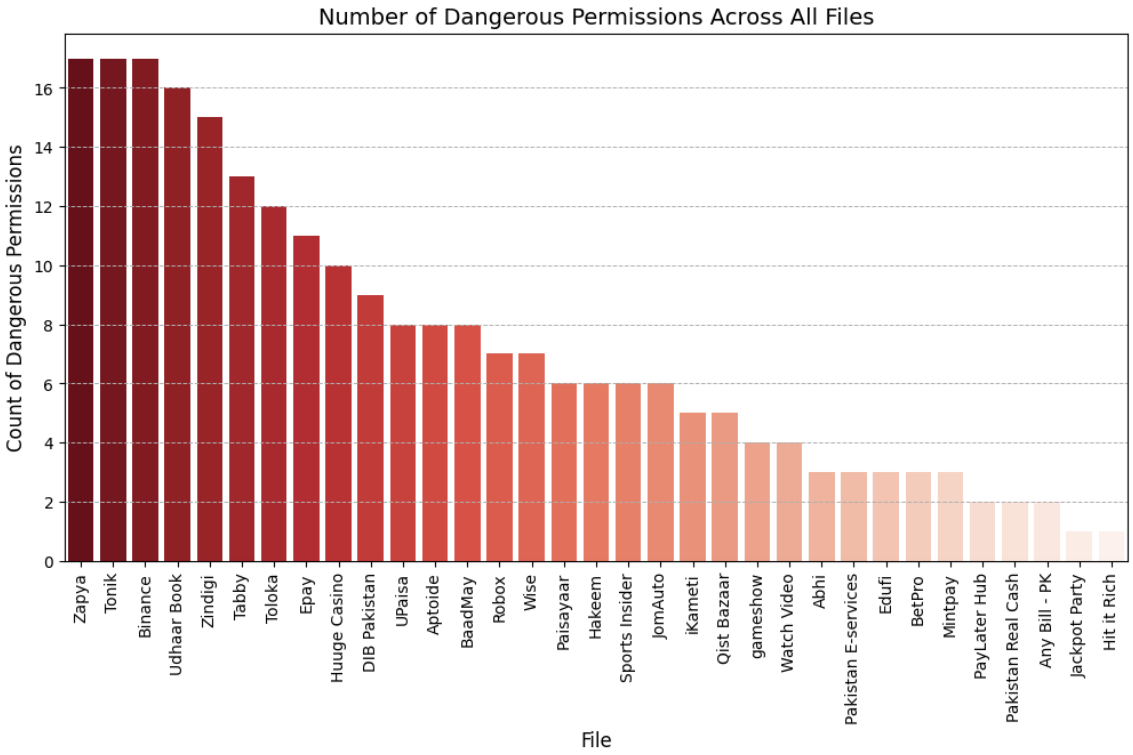

Fig. 2. Number of MobSF classified dangerous permissions across 37 shortlisted applications.

ostensibly to "improve user experience." However, this kind of access can be used to track users or expose their location data to third parties without their knowledge or consent. Moreover, several of the apps did not provide clear or accessible privacy policies, making it difficult for users to understand what data was being collected and why.

5 Ensuring Informed Consent

Our analysis highlights the challenges faced by low-literacy users when interacting with financial/gambling apps. Many such applications not only request excessive permissions but also fail to adequately inform users of the consequences of granting such access. The apps operate with minimal oversight and this creates a high-risk environment where users are vulnerable to data exploitation and privacy breaches. Our results demonstrate the need to ensure that: a) application permissions are tied to their core functionality, and b) the need to have clear, contextualized and accessible privacy policies that enable informed decision-making.

To address these gaps, we designed two interventions to improve user comprehension of privacy security policies and application terms and conditions and evaluated their results in controlled settings.

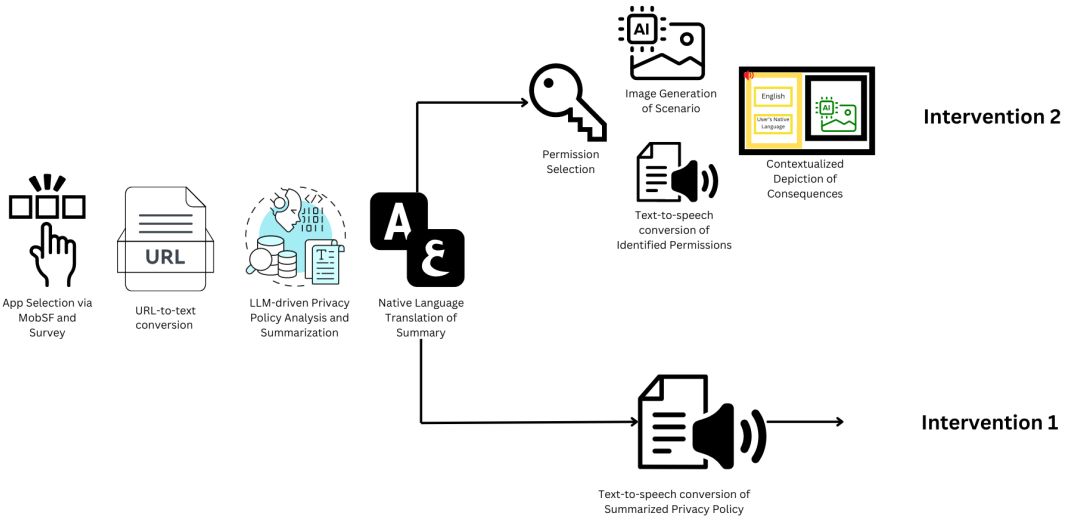

Fig. 3. Step wise pipeline for our Machine Learning-based Privacy Policy Interventions

5.1 Using LLMs to summarize polices

The first approach involved using Large Language Models (LLMs) to summarize privacy policies into simple and concise text. Additionally, we converted the text to audio snippets in local languages bridging language barrier. The key idea is better comprehension could lead to improved decision-making among our study participants. We designed domain-specific prompts to summarize the policies and manually validated their accuracy. Our approach required

Table 2. Intervention 2 results as separated by gender

Gender	Previous Impression of Apps	Confidence/Caution After Privacy Policy
Male	88% Confident, 21% Distrustful	94% Cautious, 6% Neutral
Female	73% Confident, 17% Neutral, 10% Indifferent	92% Cautious, 5% Confident

a four-step process: a) downloaded all apps' privacy policies. b) pre-processed the text and used `gemini-1.5-flash` Large Language Model to create domain specific summaries. c) Translated the summary into user's native language (Urdu/Punjabi). Lastly, d) converted the translated into speech using the Google Text-To-Speech (`gTTS`) library.

- Particular care was taken to create context-specific prompts to guide the model's behavior, and create contextually correct, comprehensible results. The prompt choice was crucial since privacy policies often contain dense legal language, and identifying key components ensures that subsequent summaries capture the most important information.
- Summaries generated by LLMs may not fully capture the nuanced legal language and implications of privacy policies. To ensure accuracy and completeness, these summaries was reviewed by legal professionals. We also incorporated a disclaimer into the policies to address both user-centered and legal considerations. A disclaimer is essential in legal-contexts where privacy policies are binding.
- Technical terms may not translate effectively into other languages (e.g., Urdu), leading to potential misunderstandings. Additional data cleaning and expert review are needed to ensure the intended legal meaning is preserved. To this end, a lawyer was consulted who reviewed the summaries and voice notes to ensure they were accurately representing the policy.

5.2 LLM generated summaries with visual cues

For our second intervention, we augmented our summaries with contextual visual cues to help our participants understand the policies. Research shows visual cues are among the most effective tools for engaging low-literate populations [13]. The team carefully crafted AI generated images depicting potential dangers of various app permissions and policies. The goal was to create *vivid* and *relatable* scenarios where the user would be able to contextualize the privacy policies and permissions and the implications of granting them.

In order to test our hypothesis, we picked a subset of high-risk permissions and created vivid images. (Please see Appendix 6) to show the potential consequence of allowing these permissions to an application. Our objective was to craft strong, attention-grabbing messages that urged users to pause and consider their choices carefully. The aim was to ensure the message could be readily understood and resonates with all users, especially those with lower literacy levels. Most importantly, a balance between caution and empowerment was carefully maintained, ensuring that users felt in control of their privacy without being overwhelmed by potential risks.

5.3 Discussions and Results

We compared the results of both of our interventions using a controlled study. Our observations revealed that participants who were previously unaware (73% confident women turned into 92% cautious, as shown in Table 3) of the privacy practices associated with the apps were surprised upon receiving the simplified information. Many participants subsequently reconsidered their decision to download the app. These findings also suggest that the complexity of privacy policy language significantly impedes informed consent, highlighting the need for more accessible and comprehensible

privacy disclosures. The use of visual cues and native languages also greatly improved participant comprehension. While People with less educational background were however confused by the technical and complicated jargon, visual cues were much better at explaining the consequences of permissions and policies to people.

Our study clearly shows that popular digital financial applications frequently indulge in dubious practices, ignoring the needs of low-literate users. Issues pertaining to excessive and unnecessary permissions, terms and conditions being vague, incomplete, or deliberately obscure are widespread. Our findings indicate that the complexity of privacy policy language and the absence of contextual information in app permissions hinder informed consent, underscoring the need for clearer and more accessible privacy disclosures.

References

[1] Ajin Abraham. 2023. Mobile Security Framework (MobSF). https://github.com/MobSF/Mobile-Security-Framework-MobSF. Accessed: 2024-09-12.

[2] Bhupendra Acharya, Muhammad Saad, Antonio Emanuele Cinà, Lea Schönherr, Hoang Dai Nguyen, Adam Oest, Phani Vadrevu, and Thorsten Holz. 2024. Conning the crypto conman: End-to-end analysis of cryptocurrency-based technical support scams. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 17–35.

[3] Vaibhav Aggarwal, Neha Aggarwal, Barkha Dhingra, Shallu Batra, and Mahender Yadav. 2024. Predatory loan mobile apps in India: A new form of cyber psychological manipulation. In *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*. IEEE, 1918–1922.

[4] Ayesha Ali and Ihsan Ayyub Qazi. 2022. Digital literacy and vulnerability to misinformation: Evidence from Facebook users in Pakistan. *Journal of Quantitative Description: Digital Media* 2 (2022).

[5] Rajibul Anam and Abdelouahab Abid. 2020. Usability study of smart phone messaging for elderly and low-literate users. *International Journal of Advanced Computer Science and Applications* 11, 3 (2020).

[6] Nausheen H Anwar, Sarwat Viqar, and Daanish Mustafa. 2018. Intersections of gender, mobility, and violence in urban Pakistan. In *Social Theories of Urban Violence in the Global South*. Routledge, 15–31.

[7] Massimo Bartoletti, Stefano Lande, Andrea Loddo, Livio Pompianu, and Sergio Serusi. 2021. Cryptocurrency scams: analysis and perspectives. *Ieee Access* 9 (2021), 148353–148373.

[8] Moritz Büchi, Noemi Festic, Natascha Just, and Michael Latzer. 2021. Digital inequalities in online privacy protection: effects of age, education and gender. In *Handbook of digital inequality*. Edward Elgar Publishing, 296–310.

[9] James H Carr and Lopa Kolluri. 2001. Predatory lending: An overview. *Fannie Mae Foundation* (2001), 1–17.

[10] Zhuo Chen, Lei Wu, Yubo Hu, Jing Cheng, Yufeng Hu, Yajin Zhou, Zhushou Tang, Yexuan Chen, Jinku Li, and Kui Ren. 2023. Lifting The Grey Curtain: Analyzing the Ecosystem of Android Scam Apps. *IEEE Transactions on Dependable and Secure Computing* (2023).

[11] Mohamed-Amine Choukou, Diana C Sanchez-Ramirez, Margriet Pol, Mohy Uddin, Caroline Monnin, and Shabbir Syed-Abdul. 2022. COVID-19 infodemic and digital health literacy in vulnerable populations: a scoping review. *Digital health* 8 (2022), 20552076221076927.

[12] Pankaj Doke and Anirudha Joshi. 2015. Mobile phone usage by low literate users. In *Proceedings of the 7th Indian Conference on Human-Computer Interaction*. 10–18.

[13] Ros Dowse, Thato Ramela, Kirsty-Lee Barford, and Sara Browne. 2010. Developing visual images for communicating information aboutantiretroviral side effects to a low-literate population. *African Journal of AIDS Research* 9, 3 (2010), 213–224.

[14] EA Draffan, Chaohai Ding, Mike Wald, and Russell Newman. 2020. Multilingual Symbolic Support for Low Levels of Literacy on the Web. In *Companion Publication of the 12th ACM Conference on Web Science*. 60–63.

[15] N Eyal and R Hoover. 2019. Hooked: How to Build Habit-Forming Products. 2016. *First published* (2019).

[16] CIT Farooq, HN Ahmad, and MN Shinwari. 2023. Addressing Gender Disparities in Education: Empowering Girls through Education in Pakistan. *Global Social Sciences Review, VIII* (2023), 390–396.

[17] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. 2012. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the eighth symposium on usable privacy and security*. 1–14.

[18] MD Griffiths. 2010. Crime and gambling: a brief overview of gambling fraud on the Internet. *Internet journal of criminology* (2010).

[19] GSMA. 2024. The Mobile Economy 2024. https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2024/02/260224-The-Mobile-Economy-2024.pdf Accessed: 2024-09-13.

[20] Ronald Paul Hill and John C Kozup. 2007. Consumer experiences with predatory lending practices. *Journal of consumer affairs* 41, 1 (2007), 29–46.

[21] Anirudha Joshi, Nikhil Welankar, Naveen BL, Kirti Kanitkar, and Riyaj Sheikh. 2008. Rangoli: a visual phonebook for low-literate users. In *Proceedings of the 10th international conference on Human computer interaction with mobile devices and services*. 217–223.

[22] Disha Kumar, Vagish Hemmige, Michael A Kallen, Thomas P Giordano, and Monisha Arya. 2019. Mobile phones may not bridge the digital divide: a look at mobile phone literacy in an underserved patient population. *Cureus* 11, 2 (2019).

[23] Indrani Medhi, S Raghu Menon, Edward Cutrell, and Kentaro Toyama. 2010. Beyond strict illiteracy: abstracted learning among low-literate users. In *Proceedings of the 4th ACM/IEEE International Conference on Information and Communication Technologies and Development*. 1–9.

[24] 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.

[25] Indrani Medhi Thies. 2017. SIGCHI Social Impact Award Talk–Designing for Low-Literate Users. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. 8–9.

[26] Alcindo Mendes, Ernesto Lopez-Valeiras, and Rogerio Joao Lunkes. 2017. Pluralistic ignorance: Conceptual framework, antecedents and consequences. *Intangible Capital* 13, 4 (2017), 781–804.

[27] Khadijah D Mohammed, Victoria Uren, Sian Joel-Edgar, and Priscilla Omonedo. 2023. Usability and User Experience of Mobile Applications: A Case of Functional Illiterates in Nigeria. In *Proceedings of the 4th African Human Computer Interaction Conference*. 98–105.

[28] Collins W Munyendo, Yasemin Acar, and Adam J Aviv. 2022. "desperate times call for desperate measures": User concerns with mobile loan apps in kenya. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2304–2319.

[29] Mame Awa Ndiaye and Moustafa Zouinar. 2014. The usage of mobile phones by low-literate users in Senegal: An ethnographic study. In *Proceedings of 4th International Conference on M4D Mobile Communication for Development*. 272–280.

[30] Christopher K Odinet. 2020. Predatory Fintech and the Politics of Banking. *Iowa L. Rev.* 106 (2020), 1739.

[31] Tapan S Parikh, Paul Javid, Sasikumar K, Kaushik Ghosh, and Kentaro Toyama. 2006. Mobile phones and paper documents: Evaluating a new approach for capturing microfinance data in rural India. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*. 551–560.

[32] Humaira Kamal Pasha. 2024. Gender differences in education: are girls neglected in Pakistani society? *Journal of the Knowledge Economy* 15, 1 (2024), 3466–3511.

[33] Margarida Rodrigues and Federico Biagi. 2017. Digital technologies and learning outcomes of students from low socio-economic background: An Analysis of PISA 2015. *JRC Science for Policy Report* (2017).

[34] Mariana Rodriguez-Patarroyo, Angelica Torres-Quintero, Andres I Vecino-Ortiz, Kristina Hallez, Aixa Natalia Franco-Rodriguez, Eduardo A Rueda Barrera, Stephanie Puerto, Dustin G Gibson, Alain Labrique, George W Pariyo, et al. 2021. Informed consent for mobile phone health surveys in Colombia: a qualitative study. *Journal of Empirical Research on Human Research Ethics* 16, 1-2 (2021), 24–34.

[35] Mora Saritha. 2023. DEMYSTIFYING THE MISERY BEHIND LOAN APPS IN INDIA. *Indian Journal of Finance and Banking* 13, 1 (2023), 104–109.

[36] P Shah, I Thornton, D Turrin, et al. 2024. *Informed Consent*. StatPearls Publishing, Treasure Island (FL). https://www.ncbi.nlm.nih.gov/books/NBK430827/ [Updated 2023 Jun 5].

[37] Cordelia Rose Stewart and Sheau-Fen Yap. 2020. Low literacy, policy and consumer vulnerability: Are we really doing enough? *International Journal of Consumer Studies* 44, 4 (2020), 343–352.

[38] UNESCO. [n. d.]. The Need for Literacy. https://www.unesco.org/en/literacy/need-know#:~:text=Despite%20this%20worldwide%20at%20least,to%20aquire%20basic%20literacy%20skills.

[39] Pengcheng Xia, Haoyu Wang, Bowen Zhang, Ru Ji, Bingyu Gao, Lei Wu, Xiapu Luo, and Guoai Xu. 2020. Characterizing cryptocurrency exchange scams. *Computers & Security* 98 (2020), 101993.

6 Appendices

Fig. 4. Location permission intervention with transcript and translation.

Do you grant this app permission to access your mobile camera?

Be cautious if you allow this. An unsecured app could secretly record your most private moments without your consent. For instance, some apps have been caught recording users' private videos through their cameras and then blackmailing them for money. Imagine if your most personal videos ended up in the hands of someone who could use them to embarrass you or make your life a nightmare—such breaches can completely destroy your life. Always be careful about which apps you allow to access your camera

اگر آپ اجازت دیتے ہیں، تو محتاط رہیں۔ یہ ایپ خفیہ طور پر آپ کی سب سے نجی لمحات کو ریکارڈ کر سکتی ہے، بغیر آپ کی رضا مندی کے۔ تصور کریں کہ آپ کی ذاتی ویڈیوز کسی کے ہاتھ میں جا سکتی ہیں جو انہیں بدنام کرنے، بلیک میل کرنے، یا حتیٰ کہ آپ کی زندگی کو مکمل طور پر جہنم بنانے کے لیے استعمال کر سکتا ہے۔ ایک دن آپ کو معلوم ہو سکتا ہے کہ آپ کی نجی ویڈیوز انٹرنیٹ پر وائرل ہو چکی ہیں، یا آپ کی تصاویر کا استعمال آپ کی ملازمت یا ذاتی تعلقات کو تباہ کرنے کے لیے کیا جا رہا ہے—ایسی خلاف ورزیاں آپ کی زندگی کو مکمل طور پر تباہ کر سکتی ہیں۔ اس لیے ہمیشہ محتاط رہیں کہ آپ کس ایپ کو اپنے کیمرے کی رسائی دیتے ہیں۔

Fig. 5. Contact permission intervention with transcript and translation.

Do you grant this app permission to send and receive messages?

If you allow this, be extremely cautious. The app may access and store your conversations, which could be used to exploit your personal information or sensitive discussions. Imagine your private messages being leaked or shared without your consent, potentially leading to blackmail, threats, or ruining your personal or professional life. Such breaches can severely damage your privacy. Always be careful about which apps you allow to access your messages

کیا آپ اس ایپ کو پیغامات بھیجنے اور وصول کرنے کی اجازت دیتے ہیں؟ اگر آپ اسے اجازت دیتے ہیں، تو انتہائی محتاط رہیں۔ ایپ آپ کی بات چیت تک رسائی حاصل کر سکتی ہے اور انہیں محفوظ کر سکتی ہے، جو کہ آپ کی ذاتی معلومات یا حساس بات چیت کا استحصال کرنے کے لیے استعمال کی جا سکتی ہیں۔ تصور کریں کہ آپ کے نجی پیغامات آپ کی اجازت کے بغیر لیک ہو جائیں یا شیئر کر دیے جائیں، جس سے آپ کی ذاتی یا پیشہ ورانہ زندگی کو نقصان پہنچ سکتا ہے یا آپ کو بلیک میل اور دھمکیوں کا سامنا کرنا پڑ سکتا ہے۔ ایسی خلاف ورزیاں آپ کی پرائیویسی کو شدید نقصان پہنچا سکتی ہیں۔ ہمیشہ احتیاط کریں کہ کن ایپس کو آپ اپنے پیغامات تک رسائی کی اجازت دیتے ہیں۔

Fig. 6. Message permission intervention with transcript and translation

Table 3. Summary of Data Protection and Responsibility

Question	Most Common Response	Percentage
Important Data	Photos, Gallery	40%
	Contacts	15%
	WhatsApp Messages, Voice Notes	10%
	Family Members' Photos/Numbers	20%
	Other (Google ID, Jazzcash, SIM data)	15%
Informed on how data is protected	No	85%
	Yes	15%
Awareness of data protection rules and regulations	No	90%
	Yes	10%
Apps asking for permissions	No, or not aware	80%
	Yes	20%
Responsible for protecting data	User	30%
	App Developer	40%
	Government	30%

Table 4. Relationship Between Responsibility and Permissions Awareness

Responsible for Data	Aware of Permissions	Not Aware of Permissions
App Developer	3 (15%)	9 (45%)
User	2 (10%)	4 (20%)
Government	1 (5%)	5 (25%)
Total	6 (30%)	18 (90%)

Table 5. Relationship Between Responsibility and Awareness of Data Protection Rules

Responsible for Data	Aware of Data Protection Rules	Not Aware of Data Protection Rules
App Developer	2 (10%)	10 (50%)
User	1 (5%)	5 (25%)
Government	1 (5%)	5 (25%)
Total	4 (20%)	20 (80%)

Table 6. Relationship Between Permissions Awareness and Data Protection Awareness

Aware of Permissions	Aware of Data Protection Rules	Not Aware of Data Protection Rules
Yes	2 (10%)	4 (20%)
No	2 (10%)	16 (70%)
Total	4 (20%)	20 (80%)

Table 7. Relationship Between Important Data and Permissions Awareness

Important Data	Aware of Permissions	Not Aware of Permissions
Photos/Gallery	3 (15%)	7 (35%)
Contacts/Phone Number	1 (5%)	4 (20%)
WhatsApp/Voice Notes	2 (10%)	3 (15%)
Total	6 (30%)	14 (70%)

Table 8. Relationship Between Important Data and Responsibility for Data Protection

Important Data	App Developer Responsible	User Responsible	Government Responsible
Photos/Gallery	6 (30%)	2 (10%)	2 (10%)
Contacts/Phone Number	2 (10%)	2 (10%)	1 (5%)
WhatsApp/Voice Notes	3 (15%)	1 (5%)	1 (5%)
Total	11 (55%)	5 (25%)	4 (20%)

Table 9. Relationship Between Awareness of Data Protection Rules and Responsibility for Data

Aware of Data Protection Rules	App Developer Responsible	User Responsible	Government Responsible
Yes	1 (5%)	1 (5%)	2 (10%)
No	9 (45%)	4 (20%)	3 (15%)
Total	10 (50%)	5 (25%)	5 (25%)

Table 10. Intervention 1 results as separated by gender

Gender	Previous Impression of Apps	Confidence/Caution After Privacy Policy
Male	88% Confident, 21% Distrustful	86% Cautious, 7% Confident, 7% Indifferent
Female	73% Confident, 17% Neutral, 10% Cautious	42% Cautious, 45% Indifferent,13% confident