

USENIX

THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

“I feel as though my privacy is being violated”: Privacy Risks and Barriers in Instant Messaging for Blind and Low-Vision Users

Sohana Akter, *University of Texas at San Antonio;* Wejdan Al Sarih, *University of Bristol;* Blessy Kalluri, *University of Texas at San Antonio;* Kopo M. Ramokapane, *University of Bristol;* Taslima Akter, *University of Texas at San Antonio*

https://www.usenix.org/conference/soups2026/presentation/akter

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

August 24–26, 2026 • Hannover, Germany

ISBN 978-1-939133-59-5

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

"I feel as though my privacy is being violated": Privacy Risks and Barriers in Instant Messaging for Blind and Low-Vision Users

Sohana Akter
University of Texas at San Antonio

Wejdan Al Sarih
University of Bristol

Blessy Kalluri
University of Texas at San Antonio

Kopo M. Ramokapane
University of Bristol

Taslima Akter
University of Texas at San Antonio

Abstract

Instant messaging applications are central to social and professional life. Yet managing privacy around their use remains a challenge, particularly for blind and low-vision (BLV) users. We conducted an exploratory qualitative study with 20 BLV participants to examine their privacy concerns and threats, barriers to exercising privacy agency, and the strategies they adopt to protect their privacy on instant messaging platforms. Our findings show that BLV users often cannot verify what content or profile information is visible to others, are frequently constrained by default settings beyond their control, and sometimes must expose private content to access basic accessibility support, such as by sharing images with AI tools for interpretation. Furthermore, participants reported ongoing difficulty discovering, understanding, and navigating the privacy features that do exist. These findings reveal critical gaps at the intersection of accessibility and privacy in instant messaging applications and we conclude by discussing design implications for more inclusive and privacy-preserving platforms.

1 Introduction

Instant messaging applications have become essential tools for communication, enabling people to maintain social relationships, collaborate professionally, and access services in real time. Popular platforms include WhatsApp, Facebook Messenger, Telegram, WeChat, and Signal, with WhatsApp alone serving over 3 billion active users each month as of 2025 [1]. Despite their widespread adoption, ensuring that these applications are both accessible and secure for all users remains a challenge. Prior research has documented numerous privacy concerns raised by users across diverse cultural contexts [36, 37, 44, 59, 70, 85]. For example, WhatsApp users in Saudi Arabia often adjusted privacy settings but still struggled with unwanted contact and limited control [70]. Vaziripour et al. showed that Telegram users in Iran valued privacy but misunderstood or underused key features, often relying on default settings [85]. WhatsApp's 2021 privacy policy sparked these tensions globally, generating widespread concern yet users found it difficult to switch due to network effects [44]. These studies highlight a recurring tension between users' desire for privacy and the practical barriers to achieving it on large-scale messaging platforms.

However, these challenges are not evenly distributed. Blind and low-vision (BLV) users must manage privacy under conditions that sighted users do not face, due to their reliance on assistive technologies and support from others. By blind or low-vision, we refer to individuals who self-identify as having a significant visual impairment that limits their ability to interact with digital interfaces without assistive technologies such as screen readers. For these users, screen readers or text-to-speech tools may read out messages or notifications aloud, inadvertently exposing sensitive content to anyone nearby [4]. BLV users also face privacy risks when relying on sighted assistance for visual interpretation [69] or configuring settings [48] and when using camera-based technologies, as captured images often contain unintended private information [45, 46, 79]. Additionally, privacy-related information and settings often remain inaccessible to BLV users [42], creating barriers to effective privacy management. Moreover, prior studies have documented persistent accessibility barriers that prevent BLV users from accessing online privacy controls and information, including inaccessible privacy policies, cookie notices, and privacy and security indicators that lack proper semantic structure [30, 41, 42, 55, 63]. These structural barriers not only constrain access to privacy information and protection but can further widen existing digital inequalities [51].

Despite this, instant messaging remains a distinct and un-

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

derexplored privacy landscape for BLV users. Unlike task-specific assistance tools or intermittently used social media platforms, instant messaging apps are used continuously for personal, professional, and intimate communications. In these real-time settings, reliance on assistive technologies, and others can amplify risks of inadvertent information disclosure [20, 67]. Yet privacy challenges BLV users face in instant messaging applications and the accessibility of the controls intended to mitigate them remain largely unexplored.

To address this gap, we conducted a qualitative study with 20 BLV participants to examine how they navigate and manage privacy in instant messaging applications. Using semi-structured interviews, we explored the accessibility barriers they encounter, the strategies they employ, and the trade-offs they make when managing their privacy on instant messaging apps. In this study, we address the following research questions:

RQ1: What privacy concerns do BLV users have when using instant messaging applications?
RQ2: What accessibility barriers do BLV users encounter in managing their privacy on instant messaging applications?
RQ3: What strategies do BLV users follow currently to manage their privacy on instant messaging applications?

Our findings show that BLV users face unique privacy vulnerabilities that extend beyond accessibility barriers. Participants reported disclosing private message content to AI systems to access messages, being unable to verify what information is visible to others, experiencing heightened risks from malicious content due to screen reader interaction patterns, and relying on default privacy settings they cannot independently configure. Despite these constraints, participants developed creative workarounds such as limiting sensitive disclosures, securing accounts and devices, using manual verification techniques, and avoiding risky interactions. However, these strategies require significant additional effort and achieve only partial protection. Overall, this work contributes to understanding the privacy vulnerabilities and accessibility barriers faced by BLV users in instant messaging, demonstrating that accessibility is a prerequisite for the effective use of privacy and security features, and offering design implications to improve their ability to manage privacy.

In summary, we make the following contributions.

1. We characterize BLV users' privacy concerns and threat perceptions in instant messaging applications.
2. We show how accessibility barriers in privacy and security controls introduce structural vulnerabilities, limiting BLV users' ability to independently verify information, configure settings, and manage data exposure.
3. We identify the strategies and trade-offs BLV users employ to mitigate privacy risks, revealing the additional effort required to achieve partial privacy protection and its security implications.

2 Related Work

2.1 Privacy of BLV Users

BLV users face unique privacy vulnerabilities stemming from their reliance on assistive technologies and inability to visually verify sensitive information. Foundational work by Ahmed et al. documented heightened privacy risks including bystanders overhearing screen reader output, vulnerability to shoulder-surfing attacks they cannot detect, and difficulty verifying URLs or visual privacy indicators [4, 5, 7]. BLV users also often depend on trusted or sighted individuals for privacy-sensitive tasks, introducing concerns about cooperative privacy management and reduced independence [48, 69].

The most extensive body of privacy research for BLV users focuses on camera-based visual assistance technologies like Be My Eyes, Aira, and Seeing AI. Multiple studies [12, 16, 58, 77–80] have examined privacy concerns when BLV users share images with human volunteers, professional assistants, or AI systems. Key findings indicate that many images captured by BLV users contain private information [45, 46, 79], yet most providers inadequately communicate data practices [32, 79]. Recent work explores privacy-preserving approaches including obfuscation tools [89, 90], privacy detection datasets [45, 46, 84], and the emerging use of generative AI for sensitive visual tasks [77]. Other work highlights bystander privacy risks, as these systems may capture images of non-consenting individuals [6, 10, 91].

Moreover, significant research attention has addressed authentication barriers for BLV users. Screen readers announce passwords and authentication codes aloud, creating eavesdropping vulnerabilities [8, 24, 25, 39]. Studies also show that BLV users face inaccessible security features, including unreadable password generators, unlabeled warnings, and integration failures [68]. Researchers have proposed alternative authentication methods including multi-touch gestures [17], haptic patterns [19, 52], and Braille-based systems [15], though adoption remains limited. CAPTCHA systems present similar accessibility barriers [50, 57].

Several studies examine BLV users' challenges accessing online privacy controls and information. Privacy policies, cookie notices, and security indicators remain largely inaccessible due to screen reader incompatibilities [30, 41, 42, 55, 63]. Similarly, inaccessible email security warnings can prevent users from recognizing phishing threats [76]. Research suggests these barriers may reduce internet engagement among BLV individuals [51], exacerbating digital inequalities. Recent work has proposed privacy question-answering assistants [41, 42] and browser tools [55] to improve access to privacy information and controls.

This body of work establishes that BLV users face distinct privacy risks, but examines them largely in task-specific tools or one-off interactions. Our study extends this work to instant messaging, a continuous, multi-party communication setting

where these risks recur in everyday use and where privacy and accessibility intersect in ways prior contexts do not capture.

2.2 Privacy in Instant Messaging Applications

Prior research has examined privacy and security practices in instant messaging across diverse user populations. Studies consistently show that while users value privacy, many misunderstand privacy features, leave default settings unchanged, and experience unwanted contact or limited control over group interactions [70, 85]. Dev et al. highlight that the majority of Indian WhatsApp users actively employ privacy controls, particularly in group communications, which are widely used in both social and professional contexts [36]. Other studies show that privacy preferences and disclosure practices vary across messaging platforms and user contexts, influencing how users manage visibility, group participation, and information sharing [37, 38, 72]. Complementing these user-centered findings, technical and comparative analyses highlight structural privacy risks and design limitations in messaging platforms. Researchers have identified privacy risks arising from metadata exposure, group membership visibility, and platform policy changes, as well as challenges users face in evaluating group security and managing privacy settings [21, 44, 60, 66, 71]. Ali and Alsaad describe the design of a secure instant messaging app that uses end-to-end encryption and access controls to safeguard user data during mobile communication [14]. While these studies have examined privacy in instant messaging for the general population, and only a few have addressed the broader privacy challenges of BLV users, the specific intersection of BLV users' privacy within instant messaging remains underexplored. We show how inaccessibility reshapes those risks within instant messaging, removing users' ability to detect or correct them.

2.3 Accessibility in Instant Messaging Applications for BLV Users

Accessibility barriers significantly affect how BLV users interact with instant messaging applications. Mainstream messaging platforms often lack proper semantic structure, accessible labels, and consistent feedback, making navigation and interaction difficult for screen reader users [33, 81, 82]. These challenges are further exacerbated by touchscreen interfaces, where blind users experience higher error rates and difficulty activating intended controls [53].

Researchers have explored design improvements and alternative messaging systems to address these barriers. Sánchez and Aguayo [74] developed a tailored messaging system incorporating accessible input and speech output, while Moraes et al. [35] demonstrated that adding semantic structure and accessibility landmarks significantly improves screen reader navigation. Other work has proposed alternative interaction methods, including auditory messaging interfaces and Braille-based input systems, to enable more effective non-visual communication [54, 56]. Accessibility challenges also extend to specific features such as emoji selection and interpretation, which remain difficult for blind users [83]. While prior work has examined instant messaging accessibility for BLV users, how inaccessibility shapes their ability to manage privacy within these applications remains largely unaddressed.

3 Methods

To understand how BLV users experience privacy in instant messaging applications, we conducted semi-structured interviews with 20 participants who all identify as blind or low vision, use screen readers, and have experience using instant messaging applications regularly.

3.1 Ethics Statement

This study received ethical approval from both of our Institutional Review Boards (IRBs). Participants were provided with an accessible digital consent form compatible with screen readers, explaining the study purpose, audio recording procedures, and their rights, including voluntary participation and the ability to withdraw at any time before data anonymization. To support informed and equitable participation, all study materials were provided in accessible formats, and participants were allowed to use their preferred assistive technologies during interviews. We used respectful language throughout and confirmed participants' preferred forms of address (e.g., pronouns). Participants were reminded in advance about the interview format and could choose whether to enable video during remote sessions. At the beginning of each interview, we reiterated study goals and confirmed consent. Interviews were audio-recorded, and transcripts were prepared by the research team to maintain confidentiality. We did not collect sensitive medical information or access participants' personal messaging content, focusing solely on their reported experiences using instant messaging applications.

3.2 Study Design

We conducted the interviews remotely using video conferencing platforms. Interviews lasted between 45-60 minutes, and participants received a $30 Amazon gift card upon completion. To understand BLV users' privacy concerns, barriers to privacy, and privacy management practices in instant messaging apps, we designed a semi-structured interview protocol exploring messaging app usage patterns, privacy awareness and concerns, experiences with privacy controls, and strategies for managing privacy in accessible ways. We considered both privacy and security controls because, in instant messaging contexts, users frequently conflate these features in everyday use (e.g., [65, 66, 87]). However, our primary focus remains

privacy; security-related features such as two-step verification and end-to-end encryption were included to understand how accessibility barriers may affect BLV users' ability to protect their accounts, conversations, and shared information.

In terms of platforms to investigate, our initial plan included exploring traditional instant messaging platforms such as WhatsApp, Signal, and Telegram. However, we had to expand this list to include other platforms such as Microsoft Teams, Slack, and Discord because our pilot participants described them as instant messaging apps, as two parties using them can communicate instantly. While our primary interest was in mobile versions of these apps, we recognized that many instant messaging platforms also have desktop or web clients. We therefore did not exclude participants who discussed these versions when relevant, as excluding them would risk overlooking important aspects of BLV users' privacy practices and accessibility challenges.

Our protocol in Appendix 9.3 specifically focused on five key areas: (1) experiences with instant messaging applications, (2) perceptions of privacy threats in these platforms, (3) interactions with specific privacy controls (e.g., group chat permissions, blocking, read receipts, app locks, message editing/deletion, two-step verification, disappearing messages, and media sharing), (4) accessibility challenges with existing privacy settings, and (5) strategies currently used to protect privacy and recommendations for improvement. We began by asking about participants' general usage and experiences with instant messaging apps to build rapport and ensure that participants clearly understood that the discussion centered on familiar applications. We then asked about what they considered threats to privacy while using instant messaging apps. We introduced this topic early because we wanted to understand participants' concerns, priorities, and perceived risks before examining how they protect or manage their privacy. Our third set of questions focused on understanding which privacy controls participants were aware of and used (See Table 2). This was important because privacy research often assumes that users rely on built-in security and privacy mechanisms [34]. We examined these controls in detail to understand how they shape actual privacy outcomes and whether BLV users have equitable access to privacy protections. Next, we asked about participants' accessibility experiences when using these controls. Accessibility barriers can prevent BLV users from exercising privacy choices available to others, leading to unequal privacy outcomes. Finally, we explored participants' broader strategies for protecting their privacy. These insights help identify unmet needs, guiding design implications and opportunities for more inclusive privacy features.

3.3 Pilot Interviews

We conducted two pilot interviews with BLV users to test our protocol. After the first pilot interview, we revised several questions to remove duplicates and added additional prompts to encourage more detailed responses. The first pilot participant described using platforms such as Microsoft Teams, Slack, and Discord for instant messaging, which led us to allow discussion of these platforms in the study. Though we had originally decided not to include it, the participant from the second pilot interview also referred to Teams as an instant messaging platform. Following this, we decided to allow participants to discuss such platforms. After the second pilot, we further refined and clarified some questions and added follow-up prompts to ensure a deeper understanding of users' experiences and practices around security and privacy controls. As the changes were minimal, we did not conduct a third pilot interview. Data from the pilot interviews were not included in the final analysis.

3.4 Recruitment

We recruited 20 participants through the National Federation of the Blind (NFB) [64], leveraging the organization's established networks and communication channels to reach a diverse population of BLV instant messaging app users. Recruiting through the NFB is a common and effective strategy in accessibility research, as the organization connects individuals with a wide range of ages, levels of vision impairment, technology skills, and socioeconomic backgrounds [11, 12]. Our recruitment strategy involved posting recruitment announcements through NFB mailing lists, allowing us to reach participants beyond our own immediate networks and mitigate sampling bias [31]. Interested individuals were asked to complete a screening form. We aimed for purposive sampling [26, 31], focusing on individuals who could offer rich insights into the lived experiences of BLV users of instant messaging apps. Our inclusion criteria required participants to: (1) identify as blind or low-vision, (2) primarily use a screen reader, (3) be 18 years of age or older, (4) currently reside in the United States, (5) be an English speaker, and (6) have experience with instant messaging applications. For recruitment, we used self-identification rather than clinical acuity thresholds, consistent with accessibility research in HCI [4, 9, 62], because functional access needs vary widely across individuals and are more relevant to technology-use experiences. These criteria ensured that participants were active users of accessibility tools, able to meaningfully reflect on privacy and accessibility related challenges in instant messaging apps, and able to participate in the study without translation or interpreter support, which could introduce confidentiality issues. From our recruitment efforts, we received 102 responses (60 through the online form and 42 by email). For the respondents who contacted us through email, we only considered those who provided details that we could use to select those who matched our criteria. We selected 20 participants while balancing demographics such as age, gender, visual ability, messaging platform use, and screen reader experience to capture diverse perspectives.

3.5 Data Analysis

Two members of the research team transcribed and verified audio recordings verbatim. We analyzed the data using an inductive thematic analysis approach following Braun and Clarke [22]. Our data analysis was inductive or bottom-up approach [18,22,23]; the codes and themes emerged from the data, and we did not follow any framework.

Three researchers conducted the analysis while data collection was ongoing. Familiarization occurred during transcription, transcript verification, and repeated reading. We coded full transcripts, focusing on meaningful units of text, such as sentences or paragraphs, that capture participants' privacy concerns, accessibility barriers, or privacy-management strategies in instant messaging apps. During initial coding, two researchers independently coded two similar scripts and then met to compare interpretations and develop an initial codebook. Though they identified largely similar concepts, their labels differed; through discussion, they agreed on shared terminology and consolidated overlapping codes. Then, they continued with two additional scripts using the initial codebook, generating several new codes that were reviewed with the broader team as part of iterative codebook refinement. The third researcher then joined the coding using the updated codebook.

In the searching for and reviewing themes phases, the research team met weekly to discuss the emerging insights, review transcripts, and collaboratively develop themes. The team created analytic memos and iteratively compared the data against the emerging concepts, merging or reworking themes to ensure clarity, distinctness, and analytic coherence. Defining and naming themes was finalized once the thematic structure stabilized, thematic saturation was reached around the fifteenth script, as no new codes or themes emerged [49,75]. We continued interviewing and coding beyond this point to confirm the stability of the thematic structure and ensure analytic rigor. We then organized the final findings around three high-level areas, with analytic themes reported within each area. Since the whole research team discussed coding and themes weekly, we did not calculate inter-reliability scores between coders [27,28,40,43].

3.6 Participants

Table 1 provides detailed demographic information about our participants. Among the 20 participants, 11 (55%) identified as female, 8 (40%) as male, and 1 (5%) as non-binary. The age distribution was as follows: 6 (30%) participants were aged 30-39, 5 (25%) were aged 40-49, 5 (25%) participants were aged 50-64, and 4 (20%) participants were aged 18-29. As for their professional background, 10 (50%) participants reported being employed full-time, 1 (5%) as part-time, 1 (5%) as self-employed, 4 (20%) as unemployed and looking for work, and 4 (20%) were students. 12 (60%) reported being legally or totally blind, 8 (40%) were either low vision or seeing little light only. All of our participants (20, 100%) preferred Facebook Messenger as their instant messaging platform, 16 (80%) preferred WhatsApp, and 13 (65%) preferred Microsoft Teams. The majority of participants reported having experience using JAWS (19, 95%) and VoiceOver (18, 90%), while some had experience with NVDA, Narrator, and TalkBack.

4 Findings

We present our findings in three high-level areas that reflect our research questions and show how BLV users experience privacy in instant messaging applications: (1) their privacy concerns and perceived threats, (2) the accessibility barriers that constrain their privacy management, and (3) strategies that participants employ to protect their privacy.

4.1 Privacy Concerns and Perceived Threats

Participants expressed various privacy concerns and threats that made them hesitant to fully trust these applications. These concerns included exposure to harmful content, unintended disclosure of personal information through platform defaults and automatic behaviors, and privacy risks associated with sharing sensitive content through assistive and AI-based interpretation tools.

4.1.1 Unwanted and Malicious Content

Participants reported being exposed to unwanted or harmful content such as spam, phishing links, or unsolicited messages from unknown contacts while using instant messaging applications. For BLV users, these encounters were particularly unsettling because they could not visually inspect messages or links or assess legitimacy. Participants described having little control over preventing these intrusions or verifying their authenticity. For instance, P4 and P14 described marketing messages embedded within legitimate conversations and wondered whether these originated from human senders or automated systems. P17 explained, *"when I get these random spam messages, I feel as [though] my privacy is being violated. I get these text messages about car warranty or these political text messages. You know, I don't subscribe to anything that would send spam messages, but I still get them, and I don't understand why."*

For BLV participants, these risks were intensified by screen reader based interaction, which relies on sequential focus and repeated keystrokes. Participants feared unintentionally activating phishing links, as even routine navigation actions, such as pressing "enter" or double-tapping could trigger unsafe content without accessible warning. While mentioning Facebook Messenger P19 said, *"it [screen reader] won't read you what's in the text box, or it won't read you certain parts of the screen, you know, maybe parts of the message, like it'll*

just have a dead area, but that's actually where there's a link. And so you just have to take a chance to randomly tap on that dead area or double-tap."

While some participants noted that sequential navigation can sometimes help them avoid clicking links immediately, it does not support assessing whether a link is safe. Screen readers present phishing URLs in the same linear fashion as legitimate ones, offering no cues beyond the text itself. As P5 reflected, *"sometimes the link looks very weird, just a bunch of random letters and numbers, and the ending is not dot com, it's dot xyz, something like that. It just makes it suspicious."* For others, links from unknown contacts triggered fears of viruses or spyware, driven by uncertainty rather than confidence in their judgments. P13 reported this unease, *"sometimes the link sent to me... I'm scared to click the link because I think it's a virus or spyware link."*

4.1.2 Exposure of Personal or Sensitive Information by Default Settings

Our analysis revealed that participants were highly cautious about sharing personal identifiers such as phone numbers, locations, and profile details like who can see their profile pictures, online status, or last seen time. We found that they could not independently and quickly confirm what information was visible to others, which leaves them uncertain about the scope of their exposure. This inability to verify visibility amplified feelings of vulnerability, particularly when default settings made sensitive data public by default. For instance, P13 explained that they could not verify if the privacy settings were turned on or off as "*it is not described in accessibility.*"

Participants expressed concern about being added to groups without their consent. When informed that a setting exists to control who can add them, most admitted they were unaware of it. As a result, they were frequently added to random groups, since the default configuration allows anyone to do so. P19 wished that the application were configured so that not just anyone could add them. Alongside concerns about being added to groups, participants also worried about their phone numbers being exposed to strangers by default. In WhatsApp, phone numbers remain visible in group chats even if the recipient has not saved the contact, which leaves users with little control over this disclosure. Other participants worried about involuntary exposure because numbers are required for account creation and participation in group chats, as P12 described, *"that is an issue then, you know, I don't want to be part of that group, and on top of that, my number is visible in that group. So it's like double now."*

Profile photos and status indicators such as "last seen" were also viewed as privacy risks. Participants deliberately withheld personal photos and disabling status settings to avoid pressure or exposure. For instance, P5 said, *"I do not have a [profile] photo because I just don't want people to get my picture online. And for the ones that are able to, I do turn off the last seen settings, just because I am online, sometimes I'm doing something else, does not mean I can reply right away."*

We also found that auto-download features, enabled by default in WhatsApp and Telegram, created additional privacy vulnerabilities unique to BLV users. Files were received and stored on their devices without consent, resulting in hidden repositories of potentially sensitive content that participants could not easily monitor or manage. P11 noted, *"it [files getting auto-downloaded] bothers me. I can't tell which are duplicates and which are different... sometimes it doesn't tell you. A certain amount of time passed, and like you're trying to download it again. It just downloads it."*

Moreover, this process removed their ability to decide how to engage with incoming materials, taking away their sense of agency. Also, users worried that auto-download features violate their privacy by permanently storing their shared content in recipients' device galleries without consent, making deletion ineffective since files persist even if immediately removed from the chat interface. P6 added, *"yeah, kind of infringing on the privacy because you are just sending it for the other person to view it, like they can download it or screenshot it and save it if they want to, but for it to be done automatically, I do feel like it's just whatever you send becomes the permanent property of the recipients."*

4.1.3 AI Distrust and Privacy Concerns

Like many digital services, instant messaging platforms have adopted AI capabilities. Facebook Messenger has already added AI to improve the messages you compose and to summarize the unread messages in a conversation. As many of the screen readers and assistive technologies are also using AI nowadays, we tried to understand the thoughts of the BLV users about the usage of AI while using such applications.

Our findings revealed that participants expressed deep skepticism about the integration of AI features into instant messaging platforms. While some acknowledged that AI could potentially improve accessibility, they were also anxious about privacy, data exploitation, and control. Many perceived AI as unnecessary or intrusive in instant messaging apps. According to them, enabling AI meant handing over personal conversations for training and surveillance. P2 explained, *"if I enable AI, I know it's going to use what I share for training data."* Others expressed fears of losing control of their sensitive conversations or their messages being scanned or stored by systems they could not monitor. P3 noted, *"I personally would prefer not to use AI. I can lose control over what happens with my device."*

Though some participants reported using AI-integrated systems as an assistant, particularly for understanding images and videos, others were hesitant to share their pictures with sensitive information. These fears were not just about distrust of AI, but about personal details being taken to improve AI systems without their consent or control. P5 said, *"as far as*

the screen readers, I feel it's OK cause they're just reading it and you're just hearing it, so I think that is fine, but when it comes to, for example, taking a picture and having the AI give you an image description, I feel like I don't want to put any sensitive information in the picture because they will probably record this picture because you already sent it to the AI. So I do feel more hesitant to send pictures with sensitive information to the AI applications."

For some participants, the problem was not only that data could be collected, but that it would be interpreted through lenses that ignored or misrepresented disability experiences. P2 mentioned, *"ninety percent of the time, AI is trained by non-disabled people, so it starts acquiring its own disability biases."* This critique highlighted that they were worried about content being appropriated for training but also being filtered through biased models that misrepresented their experiences. Despite these concerns, participants continued using AI tools, as they felt no accessible alternative existed for interpreting visual content independently, a tension long present in the blind and low-vision community [77].

4.2 Accessibility Barriers to Privacy

Participants described persistent challenges in using the privacy features of instant messaging apps. They reported encountering multiple accessibility barriers that shaped whether they used these features at all, how effectively they could configure them, and the consequences of leaving them unused.

4.2.1 Lack of Awareness of Privacy Features

Our findings revealed a significant gap in privacy and security awareness among BLV users. Participants acknowledged having limited knowledge or not knowing what privacy and security features they have in their messaging applications. P6 explained, *"I didn't know about the settings... I usually don't go to the settings unless I have a problem."*

The knowledge gaps also extended to specific protective features available in instant messaging applications. Participants were unaware of the existence of several features and controls, including group chat settings, read receipts, message view status, message timers, and self-destructing messages. The majority of the participants learned about these features for the first time during the interview. For instance, after learning about the message timer or self-destruct timer feature, P6 stated that the feature would be useful, *"I think it [message timer/self-destruct timer feature] can be helpful, when you are like sending more sensitive information, and that's only needed temporarily, I do think it can be helpful."*

Other participants highlighted that BLV users are likely to miss these features because they rely on tools that may not highlight or make these features explicit to them. For example, P11 emphasized the disadvantage of relying on screen readers for navigation, *"blind people might not know [privacy settings] are there because... you have to read everything in order for you to know that the word privacy is there, whereas visually it might stand out by a different font, color, bolding, or other indications that draw one's attention to it."*

We also found that awareness often depended on external sources, podcasts, other people, or updates rather than through the applications themselves. Participants indicated that most of the time, they did not discover these features casually, but through different sources and social networks. For instance, P18 said, *"sometimes, you know, people in groups will talk about it, and they'll give advice on how to find it... or I'll look on Google for privacy settings."*

4.2.2 Irreversible Disclosure Risk

BLV users also reported experiences where accessibility barriers limited their ability to verify content before sharing or retracting shared content, resulting in disclosure that could not be undone. When selecting photos or videos, BLV users cannot determine what a file actually contains because instant messaging applications lack built-in image descriptions and provide limited screen-reader feedback during media selection, increasing the likelihood of unintentionally disclosing sensitive or private images. While discussing media sharing, P7 explained, *"you're never really sure if you're sending what you think you're sending."* This uncertainty is further compounded by inaccessible or incomplete metadata; for example, P4 noted that in Viber, *"it doesn't tell you the date or time of the selected picture you're about to send... it only says 'photo,' 'photo,' 'video,' 'video', there's no indication that that's the one being selected."*

After content is sent, editing and deletion mechanisms do not reliably support BLV users. Participants reported that message-level editing and deletion were either inaccessible or difficult to use. P2 stated, *"it is not an accessible process. You can delete an entire chat easily and accessibly, but not individual messages."* Even when deletion options were available, participants lacked feedback confirming whether the action had succeeded. As P2 further explained, *"there's no confirmation of whether or not it's been done."*

Because these controls are time-sensitive, delays introduced by screen-reader navigation often mean that messages are read before BLV users can intervene. P7 described this challenge, saying, *"by the time I figure it out, the other person has already read it."* In addition, BLV users frequently reported uncertainty about whether deletion had any effect at all. P18 reflected on this ambiguity, *"I never know to this day if that person saw it... I did delete it... but I'm not sure if it made a difference or not."*

4.2.3 Inaccessible Features Undermine Privacy and Security

Participants described avoiding or disabling privacy and security features in instant messaging applications when those features introduced additional interaction steps or accessibility burden. For BLV users, privacy controls that required extra authentication, complex navigation, or repeated actions were often perceived as impractical for frequent messaging use. P14 said they chose not to enable app-level locks because *"it's an extra step... if I just want to respond to a message quickly, I don't feel like I wanna go through it every time."*

Two-step verification presented similar accessibility challenges. Participants reported that they were aware of such features but did not enable them because the verification process itself was difficult to complete using screen readers. P15 described verification workflows that required precise, time-sensitive input and offered limited support for screen reader users, *"verification areas won't allow you to paste... there's a text box for each individual number... and the timer is super duper short."* These interaction constraints made verification especially challenging for BLV users, particularly under time pressure. Additional barriers arose from the need to download external authenticator apps; as P5 noted, *"you have to download the authenticator app... it is a bit more inconvenient."*

Beyond authentication mechanisms, participants also described difficulty managing app-level permissions. Some reported accepting broad permissions to enable basic functionality but were unable to later verify or confidently manage that access. Limited transparency and inaccessible permission controls left participants uncertain whether apps continued to access personal data. As P11 explained, *"it seems harder to know if it shares the location while using the app or not. Those settings are harder to access."*

Across interviews, participants emphasized that privacy and security protections were only meaningful when they could be accessed and managed independently through screen readers. When accessibility failed, even technically strong security mechanisms were viewed as ineffective. P2 articulated this clearly, stating, *"if you put something encrypted in front of me that is a WCAG failure nightmare, I don't care if it's encrypted. Accessibility would still play a role... encryption is not enough if accessibility fails."*

4.2.4 Navigation and Discoverability

Our analysis shows that BLV users face persistent challenges in discovering and locating privacy features in instant messaging applications. These challenges extend beyond inconvenience and create barriers to safeguarding personal information, controlling visibility, and managing privacy sensitive features such as read receipts, blocked contacts, and group participation. Participants reported that privacy controls were often buried deep within menu structures, requiring much effort or a degree of exploration that is challenging for screen reader users. As P2 explained, *"I think that a lot of times the privacy settings are buried in the back end, and so if you are not a person who goes digging around the back end, you're not gonna find them."*

The inconsistent placement of privacy settings across different messaging platforms compounds these navigational difficulties. Since many BLV users must rely on multiple platforms for different communities or purposes, they are forced to memorize distinct and often non-intuitive navigation paths. Failure to recall these sequences results in the user having to systematically search through entire menu structures to locate the desired settings. This inconsistency slows down the ability to quickly adjust privacy settings in response to changing circumstances. For example, when a new contact is added, when a group becomes intrusive, or when a user wishes to temporarily disable read receipts. Participants also reported that the navigation path frequently changes after major updates. They explained that these updates sometimes alter the location of existing features and, in some cases reset privacy settings to default configurations without user notification. This leaves them with no knowledge that their settings have changed unless they manually review each feature. P7 explained how this presents challenges to them, *"it's pretty frustrating when, you get used to something, and they just change it for what to you might seem like no reason. For somebody without vision, like myself, once it's completely changed and something totally different, it's challenging and time-consuming and frustrating."*

Even when participants located relevant menus, unclear labeling and ambiguous interface elements further limited their ability to confidently configure privacy controls. Features such as muting groups, blocking contacts, or restricting visibility were sometimes unlabeled or poorly described, obscuring the relationship between a control and its privacy implications. P10 described encountering an unlabeled button in Telegram when attempting to block or delete a group. Similarly, P9 explained that ambiguous labeling in Discord led them to rely on experimentation, *"it's improved, but there are still a lot of like unlabeled buttons... it's oddly labeled... I just pushed stuff to try to figure out what it is."*

Participants additionally reported that the effort required to navigate and locate settings creates a significant deterrent to managing their privacy. They highlighted that this is often excessively time-consuming and sometimes discourages them from making the changes. P7 highlighted this challenge, *"trying to change any [privacy] settings is like... you first need to find the place where that specific setting might be located, which sometimes is not easy to do… so it's pretty time-consuming."*

4.3 Strategies to Protect Privacy in Instant Messaging Applications

BLV users employed a range of strategies to protect their privacy while using instant messaging apps. These strategies included behavioral precautions to minimize exposure, technical measures to secure their accounts and devices, and the use of built-in application features to control information sharing and limit unwanted interactions.

4.3.1 Behavioral Risk Minimization

Participants described relying on self-imposed behavioral strategies to reduce privacy risks, often independently of application provided privacy controls. Rather than depending solely on configurable settings, BLV users frequently minimized risk by limiting what they shared and how they interacted within messaging environments. One common strategy involved restricting the type and sensitivity of information disclosed through messaging platforms. Participants reported deliberately avoiding sharing passwords, financial details, or other confidential information via text. As P5 explained, *"I do think that it [privacy in instant messaging applications] is important to me because I don't really put much sensitive information there. I message people knowing that, OK, if somebody else, for example, even the developers or people like making the application would be able to see this, I will be fine, so I don't share, you know, passwords, and Social Security numbers and things like that."* Similarly, P11 described refraining from sending confidential material through messaging applications altogether, reflecting a conscious decision to exclude certain types of content from digital conversations rather than rely on technical privacy safeguards.

Participants also modified how they communicated to reduce exposure. Some reported choosing not to use profile pictures to limit personal information visibility. Others took precautions in public or shared spaces where screen readers could read messages aloud. P19 noted, *"the speech might read it out loud where everybody could hear... so I usually would have headphones on if I thought it was something I didn't want people to hear."* P12 further described proactively setting expectations with contacts, *"if you are not using a headphone, everyone can hear it. So, I sometimes tell my friends, don't send me any sensitive stuff, just call."*

Beyond limiting disclosure, participants described avoiding interactions perceived as risky. Many reported deliberately not clicking links from unknown or untrusted contacts, particularly when screen readers provided limited contextual information. P19 highlighted the difficulty of identifying embedded links, stating, *"sometimes they have some weird kind of image... it's not even saying image or photo, so you really don't know what's there unless you take a chance and double-tap on it to see if it activates. But you don't always want to visit links that you're not sure what they are."*

Participants also practiced non-engagement with suspicious or unfamiliar contacts. P11 described selectively responding, *"I might ignore or engage at surface level, like remind me who you are. And if it's vague and unsubstantiated, I don't respond. I usually don't delete, I don't block. You want to keep sending me stuff? Okay, I'll just mute it. But sometimes it's fascinating for me to see to what lengths it will continue."* Others adopted stricter policies as P19 noted, *"if it's someone I don't know, I block them right away."*

Channel switching emerged as another strategy for minimizing risk. When conversations involved highly sensitive topics, participants preferred moving to alternative communication channels. As P1 explained, *"if it needs to be a very private conversation, I'd rather have that, you know, face to face or over a landline, or you know, over a secure line...If we're sharing a PIN number or something like that."*

4.3.2 Securing Messaging Accounts and Devices

Participants implemented various technical and physical security measures to protect their messaging accounts and personal information. Strengthening authentication was one common strategy, with participants reporting actions such as changing passwords and enabling additional security features when they noticed suspicious activity. As P4 explained, *"when I noticed something unusual with my account, I just preferred to change my password and set secondary security measures."*

Permission management emerged as another protective strategy, with P11 specifically mentioning the practice of denying application permissions to limit data access and reduce potential exposure. He noted, *"I prefer not to [give access to share location with application], I see no reason. If it's like Uber or Lyft, something like that, something that are location centric, then yeah, I don't mind sharing while using the app, but otherwise I don't want the app to know where I am because there's no need for the app to know where I am."*

Physical device protection represented another important privacy safeguard. Because instant messaging apps are closely tied to personal devices, participants emphasized protecting their devices from unauthorized access. P2 noted, *"I've come across them [secret chats, hidden chats]. I do not engage them myself just because I am very, very protective of my devices."*

4.3.3 Leveraging App Features for Privacy Protection

Participants described a range of strategies they used to protect their privacy and reduce unwanted disruptions when using instant messaging apps. These strategies primarily involved leveraging built-in app features that allowed participants to manage their privacy and limit unwanted interactions.

(1) View-once feature. Participants described using and valuing features that allowed them to share information temporarily, reducing the risk of leaving sensitive content visible in chat history. For instance, P11 explained that WhatsApp's

view-once feature helped them share sensitive content more safely, *"sometimes there have been videos that I've sent as view once... I have used that feature before, and I also have sent and then deleted messages. And that's one thing I like about WhatsApp more than other platforms."*

(2) Blocking and reporting. Blocking and reporting were common actions when participants encountered harassment, spam, or unwanted contact. These features allowed them to maintain a sense of safety and prevented experiencing repeated intrusions. Participants described this as an empowering step that restored control over who could contact them. P4 mentioned, *"so I just ignore them or block them if the person seems suspicious or whatever."* P10 also highlighted, *"if I don't recognize the person...I just do like a report and block, or I can archive the chat on there."*

(3) Muting and exiting groups. Group chats were sometimes overwhelming or disruptive, particularly when participants were added without consent. Muting groups offered a way to regain control of notifications without leaving the group entirely. This strategy helped participants reduce distraction while still keeping the option to check messages on their own schedule. P11 noted, *"I will stay in there until you remove me. You added me, so I might mute it, but I might check in sometimes."*

Overall, these practices reveal how participants actively utilize accessible privacy features when available.

5 Discussion

Our findings reveal that BLV users face distinct privacy challenges when using instant messaging apps including accessibility barriers. For instance, participants consistently described being unable to independently verify what information was visible to others, struggling to configure privacy settings, and feeling forced into disclosure when no accessible alternatives existed. These experiences reveal systemic design limitations that constrain BLV users' agency and hinder their ability to protect their privacy in messaging apps.

5.1 Privacy Vulnerabilities and Challenges for BLV Users in Instant Messaging

While existing literature has primarily focused on privacy and security concerns of sighted instant messaging app users [21, 37, 60, 66, 70, 72], our findings demonstrate that BLV instant messaging app users face not only similar privacy threats but also experience heightened vulnerability due to the uncertainty inherent in non-visual interaction. Prior work has shown that users commonly encounter privacy and security threats such as spam, phishing links, and unwanted contacts [29, 70, 76]. This study shows that BLV users experience these threats not only as technical risks but as persistent sources of privacy uncertainty. Participants described difficulty determining whether incoming messages or links were legitimate [85], as they could not rely on visual cues commonly used to assess suspicious content [76, 86]. At the same time, messaging platforms did not provide equivalent non-visual risk indicators, such as clear screen reader compatible warnings or accessible link information, to support independent evaluation. As a result, privacy risk becomes not only a matter of malicious actors but also of limited ability to verify the safety of routine interactions. When users cannot confidently assess the safety of incoming content, privacy protection shifts from informed decision-making to precautionary behavior, reducing users' sense of control over their personal information. This highlights how privacy threats emerge not only from attacks, but from the absence of mechanisms that would allow users to recognize and avoid them independently.

Our findings further reveal that participants are routinely forced to disclose personal information even by leaving applications in their default settings. Users reported being added to groups without permission, having their online status and last-seen timestamps visible to others, and in the case of WhatsApp having their phone numbers exposed to unknown users in group chats [70] by default. Because these exposures occurred automatically, participants were often uncertain about what personal information was visible to others. Default auto-download settings further increased this risk by automatically saving media on their own devices and recipients' devices, sometimes without their awareness or control, extending the exposure beyond what users intended to share. Together, these findings show that privacy exposure can occur through routine platform use rather than deliberate sharing, limiting users' ability to maintain control over their personal information and increasing concerns about unintended disclosure.

Upon receiving images in messaging apps, participants often take screenshots and then send them to assistive applications or AI-based services for description. This process introduces extra steps and, more importantly, forces users to share potentially sensitive images, including bank documents or personal identification, with external services [12, 77, 86]. BLV participants repeatedly described this as feeling like a trade-off between access and privacy, reflecting a vulnerability uniquely tied to their reliance on non-visual interpretation tools. Although participants appreciated AI's ability to support communication, they expressed concerns about data collection, model training practices, and disability-related biases that could lead to misinterpretation or marginalization [9, 10, 90]. These findings highlight the need for trustworthy, privacy-preserving, and bias-aware AI supports integrated directly into messaging platforms, reducing reliance on external services and enhancing safe, independent access for BLV users [10, 29, 77]. Without addressing these risks, the growing reliance on AI could inadvertently exacerbate existing inequities for BLV users rather than mitigating them [41].

5.2 Accessibility is Prerequisite for Privacy

For BLV users, the ability to manage privacy in instant messaging applications depends fundamentally on the accessibility of privacy controls. The fundamental incompatibility between screen reader technology and instant messaging application design creates significant barriers to privacy feature access for BLV users. All participants in our study mentioned using screen readers for accessing the instant messaging applications. When privacy settings are not accessible through screen readers, privacy becomes fundamentally inaccessible to BLV users. Our findings reveal that most applications lack proper semantic structure, and prior studies demonstrate how these applications fail to follow Web Content Accessibility Guidelines (WCAG) [33, 47, 82]. This design failure effectively excludes BLV users from essential privacy controls because unlabeled buttons, missing headings, and inconsistent focus orders prevent screen readers from conveying what options exist or how to activate them. As a result, tasks such as adjusting who can see their profile, turning off 'last seen,' or enabling privacy settings become cumbersome or even impossible to complete independently [33, 83, 86].

Participants also described difficulty discovering and understanding existing privacy features. While lack of awareness of privacy settings is common among messaging users generally [2, 66], these challenges were compounded for BLV users because locating and navigating settings required sequential exploration of complex menu structures. This made it difficult to verify privacy configurations or confidently modify them. Participants also noted that application updates could introduce new accessibility barriers or alter privacy configurations, leaving them uncertain about whether their existing privacy protections remained in place. These experiences show that privacy management requires not only the presence of privacy controls but also the ability to independently access, understand, and verify them. Furthermore, participants described situations where they were unable to verify content before sharing, confirm whether messages were successfully deleted, or confidently use privacy and security features such as blocking, authentication, and permission controls. In these cases, users were unable to fully control or correct their disclosures, even when privacy mechanisms were available. This highlights a critical limitation, when privacy and security features are inaccessible, require extra steps, or lack clear feedback, BLV users are less likely to adopt them [39, 88]. Instead, participants relied on device-level protections, avoided sharing sensitive information, or abandoned platforms altogether when accessibility barriers prevented effective privacy control, reflecting broader patterns of compensatory privacy management observed in prior BLV research [85].

Our findings also reveal a deeper limitation of usable security protections in inaccessible systems. Mechanisms such as authentication and end-to-end encryption are designed to protect user privacy, but their effectiveness depends on users' ability to access and use them. When authentication interfaces are inaccessible or encryption protections cannot be independently verified, these safeguards become functionally ineffective [63]. Consequently, privacy risk emerges not from weak security mechanisms but from inaccessible interfaces that block users from these protections. This highlights that accessibility is a prerequisite for the practical effectiveness of privacy and security mechanisms [73].

5.3 Towards Inclusive Privacy Preserving Instant Messaging Applications

Designing accessible privacy controls is essential to ensure that BLV users can independently manage and protect their personal information in instant messaging apps. While prior work has examined accessibility [33, 81] and privacy [37, 70] in messaging apps separately, our research uniquely demonstrates how the inaccessibility of privacy settings creates compounded vulnerabilities for BLV users. The following design implications address both immediate accessibility barriers and deeper structural issues that prevent BLV users from exercising their fundamental right to privacy in messaging apps.

5.3.1 Improving Accessibility and Usability

Messaging applications must ensure that privacy features are not only present but fully accessible through proper semantic structure, clear labeling, and screen reader compatibility. When BLV users cannot access features for editing messages, deleting content, identifying correct recipients, or leaving groups, they lose fundamental control over their private communications, being trapped in conversations they cannot exit and unable to retract messages sent to wrong recipients [33, 81]. Swati et al. demonstrated how their WCAG-compliant Facebook Messenger prototype significantly improved efficiency and satisfaction for blind users [81]. When labels are missing or ambiguous, toggle states do not clearly indicate on/off status, BLV users cannot verify their privacy configurations, echoing findings from the study where they mentioned Telegram's interface [3] elements lacking proper labels for screen readers. Although WCAG compliance ensures basic accessibility through proper labeling, status announcements, and semantic structure, critical usability challenges can still persist. Our participants struggled to delete individual messages despite being able to delete entire chats accessibly, and found two-factor authentication setup confusing and burdensome despite recognizing its importance [39]. Moreover, participants struggled to discover privacy features because they were "buried in the back end," and they experienced navigation difficulties due to inconsistencies across different applications [13]. These findings highlight the need for applications to move beyond baseline compliance and address the practical usability barriers. To address these challenges, messaging applications must provide easier controls

for editing and deleting individual messages with clear keyboard navigation, streamlined authentication setup with accessible alternatives such as backup codes, and direct access to frequently-used privacy controls from the main interface rather than buried in nested menus [41, 63].

5.3.2 Adopting Privacy-Maximum Defaults

Given our findings that participants rarely modify default settings due to accessibility barriers, instant messaging applications must adopt privacy-maximizing defaults to protect BLV users proactively. Because many BLV users face challenges locating, understanding, or adjusting privacy controls, default configurations should minimize exposure to sensitive information without requiring user intervention. Specifically, applications should disable auto-download for all media types by default, require explicit and accessible consent before adding users to group chats, hide phone numbers and other identifying information in group contexts, and limit online status and profile photo visibility to "contacts only." These defaults not only reduce immediate privacy risks but also support BLV users' autonomy by ensuring that their data remains protected even when navigating complex or inaccessible settings. Participants also reported that updates often reset privacy settings or make changes without notice, leaving BLV users unaware whether their configurations remain intact. Therefore, implementing privacy-maximum defaults can substantially reduce the likelihood of accidental disclosures and improve overall safety for BLV users.

5.3.3 Supporting Informed Privacy Decision-Making

There should be proper recognition of what and how changing a setting can impact users. Often out of fear, BLV users don't change anything and later blame themselves for not knowing about the features, a phenomenon prior research identified as users getting "stuck" between accessibility and security choices [39]. Systems should offer clear, accessible explanations of privacy features and their implications when users interact with settings, reducing uncertainty and empowering informed decision-making. These explanations should be concise, written in plain language, and optimized for screen reader navigation.

5.3.4 On-Device Privacy and Accessibility Integration

On-device privacy tools are essential for BLV users, who often face a trade-off between accessibility and privacy. Messaging and collaboration apps should integrate on-device image description and malicious content detection to reduce reliance on external services that could expose sensitive data. On-device image description can provide real-time alt-text without sending content to the cloud, while audio warnings for harmful or suspicious messages enable safe, informed interaction. Developers should prioritize on-device processing, offer clearly explained, accessible privacy settings, and embed proactive alerts to empower BLV users to navigate digital environments confidently. By combining accessibility with privacy, these design strategies eliminate the need for users to compromise one for the other [12].

6 Limitations and Future Work

Our study has several limitations. First, our sample consisted only of BLV participants living in the United States. Privacy concerns and practices in instant messaging applications may vary across cultural and regional contexts [36, 37, 61, 70, 85], and future work should include more diverse populations to improve generalizability. Second, all participants in our study were screen reader users, limiting insight into the experiences of BLV users who rely on magnifiers or other assistive technologies. While some participants noted differences across mobile and desktop clients, we did not systematically compare accessibility barriers across platforms (e.g., Android vs. iOS or mobile vs. desktop), which may influence privacy control usability. Finally, our findings are based on participants' reported experiences with mainstream messaging applications. While participants discussed AI-assisted tools, we did not directly evaluate how AI-driven accessibility features may mitigate or introduce privacy risks. Future work should examine how assistive technologies and AI tools can support accessible and privacy-preserving messaging experiences.

7 Conclusion

Our study highlights that BLV users face unique privacy challenges in instant messaging applications. Participants described vulnerabilities such as exposure to malicious content, lack of awareness of key privacy features, and difficulties in configuring protections like two-factor authentication due to poor interface design. These accessibility barriers mean that BLV users often rely on default settings or outside assistance, creating inequitable burdens in safeguarding their privacy. By surfacing these concerns, we contribute an empirical account of how inaccessible design transforms privacy management into extra work for BLV users and identify opportunities for improvement. Privacy features must be designed to be not only available but also clear, discoverable, and usable by everyone. Ultimately, privacy is a right, not a privilege, and ensuring meaningful access to privacy controls is essential for creating equitable and inclusive communication platforms.

8 Acknowledgements

We would like to thank NFB, the participants who took part in our study, and the reviewers who provided useful and constructive feedback. The first author was supported by the University of Texas at San Antonio and the Computing Research

Association (CRA). Alsarih was supported by Kingdom of Saudi Arabia. Ramokapane's time was supported by EPSRC Equitable Privacy EP/W025361/1.

References

[1] Most popular messaging apps (2025). Last accessed September 2025, https://explodingtopics.com/blog/messaging-apps-stats, 2025.

[2] Ruba Abu-Salma, Kat Krol, Simon Parkin, Victoria Koh, Kevin Kwan, Jazib Mahboob, Zahra Traboulsi, and M Angela Sasse. The security blanket of the chat world: An analytic evaluation and a user study of telegram. Internet Society, 2017.

[3] Ruba Abu-Salma, M Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith. Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 137–153. IEEE, 2017.

[4] Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia. Privacy concerns and behaviors of people with visual impairments. In *Proc of the 33rd Annual ACM Conf. on Human Factors in Computing Systems*, CHI '15, page 3523–3532, New York, NY, USA, 2015. ACM.

[5] Tousif Ahmed, Roberto Hoyle, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. Understanding the physical safety, security, and privacy concerns of people with visual impairments. *IEEE Internet Computing*, 21(3):56–63, 2017.

[6] Tousif Ahmed, Apu Kapadia, Venkatesh Potluri, and Manohar Swaminathan. Up to a limit? privacy concerns of bystanders and their willingness to share additional information with visually impaired users of assistive technologies. *Proc of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 2(3):1–27, 2018.

[7] Tousif Ahmed, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. Addressing physical safety, security, and privacy for people with visual impairments. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 341–354, 2016.

[8] Md Mojibur Rahman Redoy Akanda, Ahmed Tanvir Mahdad, and Nitesh Saxena. Broken access: On the challenges of screen reader assisted two-factor and passwordless authentication. In *Proc of the ACM on Web Conf. 2025*, pages 1116–1128, 2025.

[9] Taslima Akter. Privacy considerations of the visually impaired with camera based assistive tools. In *Companion Publication of the 2020 Conf. on Computer Supported Cooperative Work and Social Computing*, pages 69–74, 2020.

[10] Taslima Akter, Tousif Ahmed, Apu Kapadia, and Manohar Swaminathan. Shared privacy concerns of the visually impaired and sighted bystanders with camera-based assistive technologies. *ACM Transactions on Accessible Computing (TACCESS)*, 15(2):1–33, 2022.

[11] Taslima Akter, Yoonha Cha, Isabela Figueira, Stacy M Branham, and Anne Marie Piper. "if i'm supposed to be the facilitator, i should be the host": Understanding the accessibility of videoconferencing for blind and low vision meeting facilitators. In *Proc of the 25th Int. ACM SIGACCESS Conf. on Computers and Accessibility*, pages 1–14, 2023.

[12] Taslima Akter, Bryan Dosono, Tousif Ahmed, Apu Kapadia, and Bryan Semaan. " i am uncomfortable sharing what i can't see": Privacy concerns of the visually impaired with camera based assistive applications. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1929–1948, 2020.

[13] Taslima Akter, Aparajita S Marathe, Darren Gergle, and Anne Marie Piper. Beyond accessibility: Understanding the ease of use and impacts of digital collaboration tools for blind and low vision workers. In *Proc of the 27th Int. ACM SIGACCESS Conf. on Computers and Accessibility*, pages 1–17, 2025.

[14] RM Ali and SN Alsaad. Instant messaging security and privacy secure instant messenger design. In *IOP Conf. Series: Materials Science and Engineering*, volume 881, page 012117. IOP Publishing, 2020.

[15] Mrim Alnfiai and Srinivas Sampalli. Braillepassword: accessible web authentication technique on touchscreen devices. *Journal of Ambient Intelligence and Humanized Computing*, 10(6):2375–2391, 2019.

[16] Mauro Avila, Katrin Wolf, Anke Brock, and Niels Henze. Remote assistance for blind users in daily life: A survey about be my eyes. In *Proc of the 9th ACM Int. Conf. on PErvasive Technologies Related to Assistive Environments*, pages 1–2, 2016.

[17] Shiri Azenkot, Kyle Rector, Richard Ladner, and Jacob Wobbrock. Passchords: secure multi-touch authentication for blind people. In *Proc of the 14th Int. ACM SIGACCESS Conf. on Computers and accessibility*, pages 159–166, 2012.

[18] Theophilus Azungah. Qualitative research: deductive and inductive approaches to data analysis. *Qualitative research journal*, 18(4):383–400, 2018.

[19] Palavi V Bhole, Ziming Li, Shivang Bokolia, Tae Oh, Garreth W Tigwell, and Roshan L Peiris. Haptic2fa: haptics-based accessible two-factor authentication for blind and low vision people. *Proc of the ACM on Human-Computer Interaction*, 8(MHCI):1–20, 2024.

[20] Erlend Bønes, Per Hasvold, Eva Henriksen, and Thomas Strandenaes. Risk analysis of information security in a mobile instant messaging and presence system for healthcare. *Int. journal of medical informatics*, 76(9):677–687, 2007.

[21] Johnny Botha, WC Vant, and Louise Leenen. A comparison of chat applications in terms of security and privacy. In *Proc. 18th Eur. Conf. Cyber Warfare Secur*, page 55, 2019.

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

[23] Virginia Braun and Victoria Clarke. Successful qualitative research: A practical guide for beginners. 2013.

[24] Daniella Briotto Faustino and Audrey Girouard. Bend passwords on bendypass: a user authentication method for people with vision impairment. In *Proc of the 20th Int. ACM SIGACCESS Conf. on Computers and Accessibility*, pages 435–437, 2018.

[25] Daniella Briotto Faustino and Audrey Girouard. Understanding authentication method use on mobile devices by people with vision impairment. In *Proc of the 20th Int. ACM SIGACCESS Conf. on Computers and Accessibility*, pages 217–228, 2018.

[26] Steve Campbell, Melanie Greenwood, Sarah Prior, Toniele Shearer, Kerrie Walkem, Sarah Young, Danielle Bywaters, and Kim Walker. Purposive sampling: complex or simple? research case examples. *Journal of research in Nursing*, 25(8):652–661, 2020.

[27] M. A. Cascio, Eunlye Lee, Nicole Vaudrin, and Darcy A. Freedman. A team-based approach to open coding: Considerations for creating intercoder consensus. *Field Methods*, 31:116 – 130, 2019.

[28] Kason Ka Ching Cheung and Kevin W. H. Tai. The use of intercoder reliability in qualitative interview data analysis in science education. *Research in Science & Technological Education*, 41:1155 – 1175, 2021.

[29] Yu-Ling Chou, Yi-Hsiu Lin, Tzu-Yi Lin, Hsin Ying You, and Yung-Ju Chang. Why did you/i read but not reply? im users' unresponded-to read-receipt practices and explanations of them. In *Proc of the 2022 CHI Conf. on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. ACM.

[30] James M Clarke, Maryam Mehrnezhad, and Ehsan Toreini. Invisible, unreadable, and inaudible cookie notices: an evaluation of cookie notices for users with visual impairments. *ACM transactions on accessible computing*, 17(1):1–39, 2024.

[31] David Collier and James Mahoney. Insights and pitfalls: Selection bias in qualitative research. *World politics*, 49(1):56–91, 1996.

[32] Kirk Crawford, Yi Xuan Khoo, Asha Kumar, Helena Mentis, and Foad Hamidi. Decoding the privacy policies of assistive technologies. In *Proc of the 21st Int. Web for All Conf.*, pages 87–95, 2024.

[33] Cláudia Ferreira Da Silva, Simone Bacellar Leal Ferreira, and João Felipe Moreira Ramos. Whatsapp accessibility from the perspective of visually impaired people. In *Proc of the 15th Brazilian Symposium on Human Factors in Computing Systems*, pages 1–10, 2016.

[34] Partha Das Chowdhury, Andrés Domínguez Hernández, Kopo Marvin Ramokapane, and Awais Rashid. From utility to capability: A new paradigm to conceptualize and develop inclusive pets. In *Proc of the 2022 New Security Paradigms Workshop*, pages 60–74, 2022.

[35] João Antônio Desidério de Moraes, Geovana Ramos Sousa Silva, and Edna Dias Canedo. Towards enabling inclusive conversations: Bridging accessibility gaps for the visually impaired in a chatbot web chat. In *Proc of the XXIII Brazilian Symposium on Human Factors in Computing Systems*, pages 1–11, 2024.

[36] Jayati Dev, Sanchari Das, and Linda Jean Camp. Privacy practices, preferences, and compunctions: Whatsapp users in india. In *HAISA*, pages 135–146, 2018.

[37] Jayati Dev, Sanchari Das, Yasmeen Rashidi, and L Jean Camp. Personalized whatsapp privacy: Demographic and cultural influences on indian and saudi users. *Available at SSRN 3391021*, 2019.

[38] Jayati Dev, Pablo Moriano, and L Jean Camp. Lessons learnt from comparing {WhatsApp} privacy concerns across saudi and indian populations. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 81–97, 2020.

[39] Bryan Dosono, Jordan Hayes, and Yang Wang. {"I'm}{Stuck!"}: A contextual inquiry of people with visual impairments in authentication. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 151–168, 2015.

[40] Victoria Elliott. Thinking about the coding process in qualitative data analysis. *The Qualitative Report*, 23(11):2850–2861, November 2018.

[41] Yuanyuan Feng, Abhilasha Ravichander, Yaxing Yao, Shikun Zhang, and Rex Chen. Understanding how to inform blind and {Low-Vision} users about data privacy through privacy question answering assistants. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 2065–2082, 2024.

[42] Yuanyuan Feng, Abhilasha Ravichander, Yaxing Yao, Shikun Zhang, and Norman Sadeh. Exploring and improving the accessibility of data privacy-related information for people who are blind or low-vision. *arXiv preprint arXiv:2208.09959*, 2022.

[43] D. Garrison, M. Cleveland-Innes, Marguerite Koole, and James Kappelman. Revisiting methodological issues in transcript analysis: Negotiated coding and reliability. *Internet High. Educ.*, 9:1–8, 2006.

[44] Carla F. Griggio, Midas Nouwens, and Clemens Nylandsted Klokmose. Caught in the network: The impact of whatsapp's 2021 privacy policy update on users' messaging app ecosystems. In *Proc of the 2022 CHI Conf. on Human Factors in Computing Systems*, CHI '22, New York, NY, USA, 2022. ACM.

[45] Danna Gurari, Qing Li, Chi Lin, Yinan Zhao, Anhong Guo, Abigale Stangl, and Jeffrey P Bigham. Vizwiz-priv: A dataset for recognizing the presence and purpose of private visual information in images taken by blind people. In *Proc of the IEEE/CVF Conf. on Computer Vision and Pattern Recognition*, pages 939–948, 2019.

[46] Danna Gurari, Qing Li, Abigale J Stangl, Anhong Guo, Chi Lin, Kristen Grauman, Jiebo Luo, and Jeffrey P Bigham. Vizwiz grand challenge: Answering visual questions from blind people. In *Proc of the IEEE Conf. on Computer Vision and Pattern Recognition*, pages 3608–3617, 2018.

[47] Sara Hamideh Kerdar, Liane Bächler, and Britta Marleen Kirchhoff. The accessibility of digital technologies for people with visual impairment and blindness: a scoping review. *Discover Computing*, 27(1):24, 2024.

[48] Jordan Hayes, Smirity Kaushik, Charlotte Emily Price, and Yang Wang. Cooperative privacy and security: Learning from people with visual impairments and their allies. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, pages 1–20, 2019.

[49] Monique Hennink and Bonnie N Kaiser. Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social science & medicine*, 292:114523, 2022.

[50] Jonathan Holman, Jonathan Lazar, Jinjuan Heidi Feng, and John D'Arcy. Developing usable captchas for blind users. In *Proc of the 9th Int. ACM SIGACCESS Conf. on Computers and accessibility*, pages 245–246, 2007.

[51] Fethi A Inan, Akbar S Namin, Rona L Pogrund, and Keith S Jones. Internet use and cybersecurity concerns of individuals with visual impairments. *Journal of Educational Technology & Society*, 19(1):28–40, 2016.

[52] Manisha V Kamarushi, Stacey L Watson, Garreth W Tigwell, and Roshan L Peiris. Onebuttonpin: a single button authentication method for blind or low vision users to improve accessibility and prevent eavesdropping. *Proc of the ACM on Human-Computer Interaction*, (MHCI):1–22, 2022.

[53] Shaun K Kane, Jeffrey P Bigham, and Jacob O Wobbrock. Slide rule: making mobile touch screens accessible to blind people using multi-touch interaction techniques. In *Proc of the 10th Int. ACM SIGACCESS Conf. on Computers and accessibility*, pages 73–80, 2008.

[54] Pegah Karimi, Emanuele Plebani, and Davide Bolchini. Textflow: Screenless access to non-visual smart messaging. In *Proc of the 26th Int. Conf. on Intelligent User Interfaces*, pages 186–196, 2021.

[55] Smirity Kaushik, Natã M Barbosa, Yaman Yu, Tanusree Sharma, Zachary Kilhoffer, JooYoung Seo, Sauvik Das, and Yang Wang. {GuardLens}: Supporting safer online browsing for people with visual impairments. In *19th Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 361–380, 2023.

[56] Daniel Kocieliński and Jolanta Brzostek-Pawłowska. Improving the accessibility of touchscreen-based mobile devices: Integrating android-based devices and braille notetakers. In *2013 Federated Conf. on Computer Science and Info Systems*, pages 655–658. IEEE, 2013.

[57] Jonathan Lazar, Jinjuan Feng, Tim Brooks, Genna Melamed, Brian Wentz, Jon Holman, Abiodun Olalere, and Nnanna Ekedebe. The soundsright captcha: an improved approach to audio human interaction proofs for blind users. In *Proc of the SIGCHI Conf. on Human Factors in Computing Systems*, CHI '12, page 2267–2276, New York, NY, USA, 2012. ACM.

[58] Sooyeon Lee, Madison Reddie, Chun-Hua Tsai, Jordan Beck, Mary Beth Rosson, and John M. Carroll. The emerging professional practice of remote sighted assistance for people with visual impairments. In *Proc of the 2020 CHI Conf. on Human Factors in Computing Systems*, CHI '20, page 1–12, NY, USA, 2020. ACM.

[59] Paul Benjamin Lowry, Jinwei Cao, and Andrea Everard. Privacy concerns vs desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures. *Journal of Management Information Systems*, 27(4):163–200, 2011.

[60] Robin Mueller, Sebastian Schrittwieser, Peter Fruehwirt, Peter Kieseberg, and Edgar Weippl. Security and privacy of smartphone messaging applications. *Int. Journal of Pervasive Computing and Communications*, 11(2):132–150, 2015.

[61] Collins W Munyendo, Kentrell Owens, Faith Strong, Shaoqi Wang, Adam J Aviv, Tadayoshi Kohno, and Franziska Roesner. "you have to ignore the dangers": User perceptions of the security and privacy benefits of whatsapp mods. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 4515–4533. IEEE, 2025.

[62] Vishnu Nair, Hanxiu 'Hazel' Zhu, and Brian A. Smith. Imageassist: Tools for enhancing touchscreen-based image exploration systems for blind and low vision users. In *Proc of the 2023 CHI Conf. on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. ACM.

[63] Daniela Napoli, Khadija Baig, Sana Maqsood, and Sonia Chiasson. " i'm literally just hoping this will {Work:'}'obstacles blocking the online security and privacy of users with visual disabilities. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 263–280, 2021.

[64] National Federation of the Blind. https://nfb.org/.

[65] Sean Oesch, Ruba Abu-Salma, Oumar Diallo, Juliane Krämer, James Simmons, Justin Wu, and Scott Ruoti. Understanding user perceptions of security and privacy for group chat: a survey of users in the us and uk. In *Proc of the 36th Annual Computer Security Applications Conf.*, pages 234–248, 2020.

[66] Sean Oesch, Ruba Abu-Salma, Oumar Diallo, Juliane Krämer, James Simmons, Justin Wu, and Scott Ruoti. User perceptions of security and privacy for group chat. *Digital Threats: Research and Practice (DTRAP)*, 3(2):1–29, 2022.

[67] Sameer Patil and Alfred Kobsa. Instant messaging and privacy. In *Proc of HCI*, volume 4, pages 85–88. Leeds, UK, 2004.

[68] Alexander Ponticello, Filipo Sharevski, Simon Anell, and Katharina Krombholz. How blind and low-vision users manage their passwords. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security*, pages 3192–3205, 2025.

[69] Michael Asante Quainoo, Michael Yao Wodui Serwornoo, and Christiana Hammond. Facebook experiences of visually impaired students: A deconstruction of the challenges and benefits. *British Journal of Visual Impairment*, 41(2):400–413, 2023.

[70] Yasmeen Rashidi, Kami Vaniea, and Jean L Camp. Understanding saudis' privacy concerns when using whatsapp. In *Usable Security and Privacy 2016*, 2016.

[71] Nidhi Rastogi and James Hendler. Whatsapp security and role of metadata in preserving privacy. *arXiv Prepr. arXiv1701*, 6817:269–275, 2017.

[72] Jake Reichel, Fleming Peck, Mikako Inaba, Bisrat Moges, Brahmnoor Singh Chawla, and Marshini Chetty. 'i have too much respect for my elders': Understanding south african mobile users' perceptions of privacy and current behaviors on facebook and {WhatsApp}. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1949–1966, 2020.

[73] Karen Renaud and Lizzie Coles-Kemp. Accessible and inclusive cyber security: a nuanced and complex challenge. *SN Computer Science*, 3(5):346, 2022.

[74] Jaime Sánchez and Fernando Aguayo. Mobile messenger for the blind. In *Universal Access in Ambient Intelligence Environments: 9th ERCIM Workshop on User Interfaces for All, Königswinter, Germany, September 27-28, 2006. Revised Papers*, pages 369–385. Springer, 2007.

[75] Benjamin Saunders, Julius Sim, Tom Kingstone, Shula Baker, Jackie Waterfield, Bernadette Bartlam, Heather Burroughs, and Clare Jinks. Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & quantity*, 52(4):1893–1907, 2018.

[76] Filipo Sharevski and Aziz Zeidieh. Assessing suspicious emails with banner warnings among blind and {Low-Vision} users in realistic settings. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 2083–2100, 2024.

[77] Tanusree Sharma, Yu-Yun Tseng, Lotus Zhang, Ayae Ide, Kelly Avery Mack, Leah Findlater, Danna Gurari, and Yang Wang. "before, i asked my mom, now i ask chatgpt": Visual privacy management with generative ai for blind and low-vision people. In *Proc of the 27th Int. ACM SIGACCESS Conf. on Computers and Accessibility*, pages 1–14, 2025.

[78] Abigale Stangl, Emma Sadjo, Pardis Emami-Naeini, Yang Wang, Danna Gurari, and Leah Findlater. "dump it, destroy it, send it to data heaven": Blind people's

expectations for visual privacy in visual assistance technologies. In *Proc of the 20th Int. Web for All Conf.*, pages 134–147, 2023.

[79] Abigale Stangl, Kristina Shiroma, Nathan Davis, Bo Xie, Kenneth R Fleischmann, Leah Findlater, and Danna Gurari. Privacy concerns for visual assistance technologies. *ACM Transactions on Accessible Computing (TACCESS)*, 15(2):1–43, 2022.

[80] Abigale Stangl, Kristina Shiroma, Bo Xie, Kenneth R Fleischmann, and Danna Gurari. Visual content considered private by people who are blind. In *Proc of the 22nd Int. ACM SIGACCESS Conf. on Computers and Accessibility*, pages 1–12, 2020.

[81] Mamoona Atif Swati, Mustafa Madni, Uzair Iqbal Janjua, and Iftikhar Ahmed Khan. Enhanced accessibility of facebook messenger for blind users. *KIET Journal of Computing and Information Sciences*, 5(2), 2022.

[82] Mamoona Atif Swati, Tahir Mustafa Madni, Uzair Iqbal Janjua, and Iftikhar Ahmad. Accessibility of social media application for blinds. In *2021 4th Int. Conf. on computing & information sciences (ICCIS)*, pages 1–6. IEEE, 2021.

[83] Garreth W. Tigwell, Benjamin M. Gorman, and Rachel Menzies. Emoji accessibility for visually impaired people. In *Proc of the 2020 CHI Conf. on Human Factors in Computing Systems*, CHI '20, page 1–14, New York, NY, USA, 2020. ACM.

[84] Yu-Yun Tseng, Tanusree Sharma, Lotus Zhang, Abigale Stangl, Leah Findlater, Yang Wang, and Danna Gurari. Biv-priv-seg: Locating private content in images taken by people with visual impairments. In *2025 IEEE/CVF Winter Conf. on Applications of Computer Vision (WACV)*, pages 430–440. IEEE, 2025.

[85] Elham Vaziripour, Justin Wu, Reza Farahbakhsh, Kent Seamons, Mark O'Neill, and Daniel Zappala. A survey of the privacy preferences and practices of iranian users of telegram. In *Workshop on Usable Security (USEC)*, volume 1, 2018.

[86] Violeta Voykinska, Shiri Azenkot, Shaomei Wu, and Gilly Leshed. How blind people interact with visual content on social networking services. In *Proc of the 19th ACM Conf. on computer-supported cooperative work & social computing*, pages 1584–1595, 2016.

[87] Edgar Weippl and Sebastian Schrittwieser. Introduction to security and privacy. *Hannes Werthner· Carlo Ghezzi· Jeff Kramer· Julian Nida-Rümelin· Bashar Nuseibeh· Erich Prem·*, page 397, 2024.

[88] Alma Whitten, J Doug Tygar, et al. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In *USENIX security symposium*, volume 348, pages 169–184, 1999.

[89] Jingyi Xie, Rui Yu, He Zhang, Sooyeon Lee, Syed Masum Billah, and John M. Carroll. Bubblecam: Engaging privacy in remote sighted assistance. In *Proc of the 2024 CHI Conf. on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. ACM.

[90] Lotus Zhang, Abigale Stangl, Tanusree Sharma, Yu-Yun Tseng, Inan Xu, Danna Gurari, Yang Wang, and Leah Findlater. Designing accessible obfuscation support for blind individuals' visual privacy management. In *Proc of the 2024 CHI Conf. on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. ACM.

[91] Yuhang Zhao, Yaxing Yao, Jiaru Fu, and Nihan Zhou. {"If} sighted people know, i should be able to {know:"} privacy perceptions of bystanders with visual impairments around camera-based technology. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 4661–4678, 2023.

9 Appendix

9.1 Full Codebook Link

Complete visible accessible codebook can be found at https://github.com/sohana003/soups2026-instant-messaging-blv-privacy-codebook.

9.2 Positionality

While none of us identify as BLV, our identities, experiences, and relationships with BLV communities shape how we designed this study, interpreted participants' accounts, and discussed our findings. As sighted researchers studying BLV individuals, we operate from positions of relative privilege that influence what we notice, how we frame barriers, and the narratives we choose to discuss. Our research team brings varied experience working with BLV communities and expertise in security and privacy, spanning human–computer interaction, usable security, and accessibility. Two early-stage authors focus on BLV users and approach this work with a commitment to learning from participants and with an awareness that their positionality as newcomers may shape how they interpret BLV users' experiences. One of them volunteers in local tech clinics that support community members (including BLV individuals) with security and privacy needs. One author is an expert in usable security with over nine years of experience designing and evaluating inclusive security and privacy controls. They also lead community-based tech clinics that support BLV users. This hands-on clinic engagement informs the team's practical insight into BLV technology use, and they recognize that their position as helpers can introduce power dynamics that may shape researcher–participant interactions. The final author has

worked at the intersection of accessibility and privacy for more than nine years and is actively engaged with their local BLV community. Their long-term relationships and subject-matter expertise inform how the team frames accessibility challenges, though they also recognize that their experience can lead to assumptions about shared norms that may not apply to all BLV users.

9.3 Interview Protocol

Experience with instant messaging applications

1. Which instant messaging apps do you use most often?
   - How often do you use them? (e.g., everyday, once a week)
   - What device do you primarily use? (Smartphone, Tablet, Computer)
   - What operating system do you primarily use? (iOS, Android, Windows, macOS, Other)
   - How long have you been using these applications?
   - Who do you mostly communicate with? (friends, family, colleagues)
2. What has your experience been like in terms of accessibility when using instant messaging apps?
   - If issues are mentioned: What challenges do you face?
3. Of the apps you mentioned, which do you prefer the most?
   - Why do you prefer this application?
   - Which features do you mostly use in this app?

   Exploring Perceptions of Privacy
4. How do you feel about privacy when using instant messaging apps?
   - If concerns are mentioned: Describe situations where you felt concerned.
   - How did you deal with those concerns?

   Understanding User Engagement with Privacy Features
5. Have you ever updated your privacy settings (e.g., online status, profile picture)?
   - Which settings do you change?
   - How often do you update them?
   - How easy or difficult was it?
6. Are you aware that apps let you control who sees your last seen, online status, or profile photo?
   - Have you ever checked or changed these settings?
   - Did you face challenges trying to locate these settings?
   - If unaware: Would you use this feature in the future? Why?
7. Are you part of any group chats?
   - Have you ever been added without your consent?
   - How do you deal with such situations?
   - Who do you prefer adding you to groups?
   - Are you familiar with group add-permission settings?
   - If yes: Have you tried changing the default "Everyone" setting?
   - How was your experience finding the setting?
   - Would you find this feature useful?
   - How do you feel about strangers seeing your phone number?
8. Have you ever been a group admin or moderator?
   - Have you used settings to manage group interaction (sending messages, editing info, adding/removing members)?
   - How was the experience managing these settings?
   - If they use WhatsApp: Have you used advanced chat privacy settings?
9. How do you normally deal with unwanted chats or people you do not want to chat with?
   - Have you ever blocked someone?
   - How was the experience using the blocking feature?
10. Have you ever used the feature that shows who has read your message?
    - How was your experience?
    - How do you feel when you're unsure whether your message was seen?
    - Do you feel pressure to respond after seeing a message?
11. Are you aware of a feature that lets you read messages without the sender knowing?
    - If yes: Have you changed or used it?
    - If no: Does the idea seem useful?
12. Most apps have an app lock feature. Have you used it?
    - How was the setup experience?
    - Are you aware of chat-specific lock/hide settings?
    - Have you used them? How was the experience?
    - If not: Would such control be helpful?
13. Have you ever edited or deleted a message after sending it?
    - How was your experience?
14. Have you ever enabled two-step verification?
    - How helpful was it?
    - What was your experience setting and using it?
    - If not: Do you feel secure without it?
15. Have you used message timer/self-destruct features?
    - If yes: Describe your experience.
    - If no: Does it seem useful for privacy? Why?
16. Have you used features like Secret Chats, Hidden Chats, or Archived Chats?
    - How was your experience?
    - How helpful were they for privacy?
    - If no: Would such features be useful? Why?
17. Can you walk me through how you select and send photos or media files?
    - Do you use tools/apps to identify images before sending them?
    - How do you feel about using such tools?
    - What are your auto-download settings?
    - How do you feel about auto-downloaded media?
    - Would mistaken auto-downloaded media pose a privacy issue?

    Privacy Concerns of Instant Messaging Apps
18. Do you use a screen reader?
    - If yes: Which one?
19. Do you use other assistive technologies?
    - Which ones?
    - How is your experience using them for private/sensitive messages?
20. Many screen readers now use AI. Were you aware?
    - How do you feel about this?
21. Have you ever asked a human assistant to read a message?
    - How do you feel about sharing private messages?
22. Have you heard of "End-to-end Encryption"?
    - If yes: What is your understanding?
    - If no: (Provide explanation)
    - How important is end-to-end encryption?
    - Does encryption influence your trust or usage of an app?

    Evaluating User Satisfaction with Privacy Settings
23. Are there privacy settings you avoid due to difficulty or poor accessibility?
    - What accessibility challenges do you face?
24. Do you feel that being blind or low vision affects how you learn about or use privacy features?
    - How do you usually learn about such features?
25. Do you think current privacy settings support the needs of blind or low-vision people?
    - If no: What features should be added?

    Do these apps support clear communication for both blind/low-vision and sighted users?
    - If no: What challenges or differences have you noticed?

    What advice would you give developers to make privacy settings more user-friendly for blind or low-vision users?
    Is there anything else you'd like to share about the accessibility of privacy features?

9.4 Codebook

Theme	Code	Description	Example quote
Unwanted and Malicious Content	Receipt of spam and unsolicited content	BLV users encounter spam, phishing links, and unwanted messages. Limited ability to visually verify content increases anxiety and reduces trust.	"When I get these random spam messages, I feel as my privacy is being violated." (P17)
	Risk of unintentional activation	Sequential focus, "dead areas," and unclear navigation lead to accidental activation of harmful links.	"You just have to take a chance to randomly tap on that dead area or double tap … which I don't like." (P19)
	Inability to assess link legitimacy	Participants cannot independently judge whether links from unknown senders are safe, relying on textual cues that are easy to misread or absent altogether.	"I'm scared to click the link because I think it's a virus or spyware link." (P13)
Exposure of Personal or Sensitive Information by Default Settings	Inability to verify visible information	Participants cannot independently and quickly confirm what personal information is visible to others, which amplifies their general feeling of vulnerability.	"There are privacy settings, which may support all our privacy needs, but most of them may not be accessible." (P2) "You don't know if the privacy setting is turned on or off … it is not described in accessibility." (P13)
	Default group inclusion permissions	Concerns about being added to groups without consent due to permissive default settings, compounded by participants' unawareness that controls to restrict this exist.	"I'd like if it [application] said, you know, hey, you've been asked to join this group, do you accept yes or no?" (P1)
	Phone number visibility in group contexts	Default exposure of phone numbers in WhatsApp group chats, including to non-contacts, leaves participants with limited control over a disclosure they did not consent to.	"I don't want to be part of that group, and on top of that, my number is visible in that group." (P12)
	Profile and status indicator visibility	Concerns about default visibility of profile photos, last-seen timestamps, and online status, which participants address through deliberate withholding or disabling.	"I do not have a [profile] photo because I just don't want people to get my picture online." (P5)
	Auto-download as silent exposure	Default auto-download settings in platforms such as WhatsApp and Telegram store media on devices without user consent, creating hidden repositories that participants cannot easily monitor or manage and sometimes do not know about. Auto-download on recipients' devices also undermines later deletion.	"For it to be done automatically, I do feel like it's just whatever you send becomes the permanent property of the recipients." (P6)
AI Distrust and Privacy Concerns	Distrust of AI data practices	Participants frame AI integration as entailing data collection, training, or surveillance over which they have limited control.	"If I enable AI, I know it's going to use what I share for training data." (P2)
	Reluctance to share sensitive content with AI	Participants selectively use AI tools and hesitate to share sensitive images with AI-based description services.	"They will probably record this picture because you already sent it to the AI. So I do feel more hesitant to send pictures with sensitive information." (P5)
	Disability bias in AI systems	Concerns that AI is trained primarily by sighted and non-disabled developers and consequently misrepresents BLV experiences or applies biased interpretation.	"Ninety percent of the time, AI is trained by non-disabled people, so it starts acquiring its own disability biases." (P2)
Lack of Awareness of Privacy Features	Limited knowledge of available features	Participants did not know about specific privacy and security controls, such as group permissions, read receipts, view-status, message timers, and self-destructing messages, until prompted.	"I didn't know about the settings … I usually don't go to the settings unless I have a problem." (P6)
	Visual salience does not transfer to non-visual access	Visual salience cues that draw sighted users' attention to privacy controls, such as font weight, color, bolding, and layout emphasis, have no equivalents in non-visual interaction, forcing linear discovery.	"Visually it might stand out by different font, different color, different bolding, or other indications that draw one's attention to it." (P11)
	Reliance on external sources for feature awareness	Participants learn about privacy features through external channels, such as peers, social networks, podcasts, and web searches, rather than through the messaging application itself.	"Sometimes, you know, people in groups will talk about it, and they'll give advice on how to find it." (P18)
Irreversible Disclosure Risk	Inability to verify content before sharing	Media pickers lack image descriptions, accessible metadata, and reliable selection feedback, making it unclear which image or file is about to be sent.	"You're never really sure if you're sending what you think you're sending." (P7)
	Inaccessible editing and deletion	Per-message edit and delete operations are difficult to perform reliably via screen reader, even when the equivalent chat-level operation is accessible.	"You can delete an entire chat easily and accessibly, but not individual messages." (P2)
	Time-sensitivity defeated by interaction speed	Screen-reader navigation delays mean that messages are typically read by recipients before BLV users can complete the deletion action.	"By the time I figure it out, the other person has already read it." (P7)
Inaccessible Features Undermine Privacy and Security	Accessibility burden discourages feature adoption	Features that introduce additional steps, authentication, or navigation effort are perceived as impractical for routine messaging use.	"Verification areas won't allow you to paste … there's a text box for each individual number … and the timer is super duper short." (P15)
	Opaque permission management	Participants accept broad app-level permissions to enable basic functionality but cannot later verify or confidently manage that access.	"It seems harder to know if it shares the location while using the app or not. Those settings are harder to access." (P11)
	Inaccessibility undermines technical security	Even strong technical security mechanisms, such as encryption, are functionally ineffective when their interfaces are inaccessible. Accessibility is articulated as a prerequisite for security.	"If you put something encrypted in front of me that is a WCAG failure nightmare, I don't care if it's encrypted … encryption is not enough if accessibility fails." (P2)
Navigation and Discoverability	Privacy controls buried in menus	Privacy settings sit deep within nested menu structures, requiring extensive exploration that is particularly costly for screen reader users.	"A lot of times the privacy settings are buried in the back end, and so if you are not a person who goes digging around the back end, you're not gonna find them." (P2)
	Cross-platform inconsistency	Different messaging applications place privacy controls in different locations and use different navigation paths, forcing BLV users to memorize multiple inconsistent structures.	"I hit escape and oh if I hit escape here on the computer it's gonna take my whole chat box away … I think that's the only challenge, is just keeping up because so many are widely accepted across the country and in industry, just keeping it all straight is the biggest challenge." (P1)
	Disruption from updates	Application updates relocate features and may reset privacy settings without notice, leaving participants uncertain whether their configurations remain intact.	"Once it's completely changed and something totally different, it's challenging and time consuming and frustrating." (P7)
	Unlabeled and ambiguous controls	Buttons and controls lack accessible labels, or labels are vague enough that the function cannot be inferred without trial.	"There are still a lot of like unlabeled buttons … it's oddly labeled … I just pushed stuff to try to figure out what it is." (P9, Discord)
	Effort as deterrent to privacy management	The time and effort required to find and configure privacy controls discourages participants from actively managing their privacy.	"Trying to change any [privacy] settings is like … you first need to find the place where that specific setting might be located, which sometimes is not easy to do … so it's pretty time-consuming." (P7)
Behavioral Risk Minimization	Limiting sensitive disclosure	Avoiding the sharing of high-sensitivity information, such as passwords, financial details, and identification numbers, through messaging applications.	"I don't share, you know, passwords, and Social Security numbers." (P5)
	Adapting to ambient screen reader output	Modifying communication and device practices to account for the risk that screen reader output will be overheard by people nearby.	"The speech might read it out loud where everybody could hear … so I usually would have headphones on if I thought it was something I didn't want people to hear." (P19)
	Avoiding risky interaction	Refusing or limiting engagement with unknown senders, suspicious links, and ambiguous interface elements.	"You don't always want to visit links that you're not sure what they are." (P19)
	Channel switching for sensitive content	Moving conversations involving highly sensitive content, such as PINs and account numbers, to alternative channels considered more secure.	"If it needs to be a very private conversation, I'd rather have that, you know, face to face or over a landline, or you know, over a secure line." (P1)
Securing Messaging Accounts and Devices	Strengthening authentication	Changing passwords and enabling additional security measures, often reactively in response to suspicious activity.	"When I noticed something unusual with my account, I just preferred to change my password and set secondary security measures." (P4)
	Selective permission management	Granting app-level permissions only when contextually justified by the app's function.	"I prefer not to [give access to share location with application] … otherwise I don't want the app to know where I am because there's no need for the app to know where I am." (P11)
	Physical device protection	Protecting the personal device itself, recognizing that messaging privacy is inseparable from device security.	"I do not engage them myself just because I am very, very protective of my devices." (P2)
Leveraging App Features for Privacy Protection	Ephemeral content controls	Using features that allow temporary sharing or post-hoc removal of content to reduce the long-term footprint of sensitive disclosures.	"Sometimes there have been videos that I've sent as view once... I have used that feature before, and I also have sent and then deleted messages." (P11)
	Blocking and reporting	Using block and report functions to manage unwanted contact and reclaim a sense of control over the conversation surface.	"If I don't recognize the person … I just do like a report and block, or I can archive the chat on there." (P10)
	Group control without exit	Using mute and similar features to reduce disruption from groups without fully leaving them, particularly when groups were joined without consent.	"I will stay in there until you remove me. You added me, so I might mute it, but I might check in sometimes." (P11)

Table 1: Demographic information of participants

Participant	Age range	Gender	Self-reported visual ability	Employment status	Instant Messaging Applications used	Screen readers used
P1	40–49	Male	Totally blind	Employed full-time	Facebook Messenger; Microsoft Teams; Google Chat; text messaging over iPhone	JAWS; VoiceOver
P2	30–39	Female	Totally blind	Self-employed	Facebook Messenger; Microsoft Teams; Slack; iMessage	JAWS; NVDA; VoiceOver
P3	30–39	Female	Totally blind	Employed full-time	WhatsApp; Facebook Messenger	JAWS; VoiceOver
P4	30–39	Female	Legally blind	Student	WhatsApp; Facebook Messenger; Telegram; Viber; Microsoft Teams	JAWS; VoiceOver
P5	18–29	Non-binary	Legally blind	Student	WhatsApp; Facebook Messenger; Microsoft Teams; Google Chat; Slack; Discord	JAWS; TalkBack
P6	18–29	Female	Blind	Student	WhatsApp; Facebook Messenger; Microsoft Teams; Google Chat; Slack; Discord	JAWS; TalkBack
P7	40–49	Male	No vision - right eye; Low vision -left eye	Unemployed	WhatsApp; Facebook Messenger; Telegram; Signal; Microsoft Teams; Zoom Chat; Instagram DM	JAWS; VoiceOver; Narrator
P8	18–29	Female	Blind with minimal light perception	Unemployed	WhatsApp; Facebook Messenger; Telegram; Discord	JAWS; VoiceOver
P9	30–39	Female	Nonexistent	Student	WhatsApp; Facebook Messenger; Telegram; Microsoft Teams; Google Chat; Discord	JAWS; VoiceOver; Voice Assistant
P10	50–64	Male	Low vision	Employed full-time	Facebook Messenger; Microsoft Teams	JAWS; NVDA; VoiceOver; TalkBack; Narrator; ZoomText/Fusion
P11	30–39	Male	No light perception / zero-sight	Employed full-time	WhatsApp; Facebook Messenger; Telegram; Microsoft Teams; Google Chat; Slack; Zoom; Skype	JAWS; VoiceOver
P12	40–49	Male	Partially see shadows, light or dark	Unemployed	WhatsApp; Facebook Messenger; Telegram; Viber; Microsoft Teams; Discord	JAWS; NVDA; VoiceOver; TalkBack; Prudent screen reader; JIESHIO
P13	40–49	Male	Totally blind	Employed full-time	WhatsApp; Facebook Messenger; Google Chat	JAWS; NVDA; VoiceOver
P14	18–29	Female	Blind, very little usable vision	Employed full-time	WhatsApp; Facebook Messenger; Viber; Microsoft Teams; Slack; Discord	JAWS; NVDA; VoiceOver
P15	30–39	Female	Little bit of vision; not able to see the texts; low vision	Employed full-time	WhatsApp; Facebook Messenger; iMessage	VoiceOver
P16	50–64	Female	Totally blind	Employed full-time	WhatsApp; Facebook Messenger; iMessage	JAWS; NVDA; VoiceOver; Narrator; Voice Assistant; orca
P17	40–49	Male	Totally blind	Employed full-time	Facebook Messenger; Microsoft Teams	JAWS; VoiceOver; Narrator
P18	50–64	Female	Can detect some light	Employed part-time	WhatsApp; Facebook Messenger; Telegram; Signal; Slack	JAWS; NVDA; VoiceOver; TalkBack; Narrator
P19	50–64	Female	Blind, light perception only	Unemployed	WhatsApp; Facebook Messenger; Slack	JAWS; VoiceOver
P20	50–64	Male	Totally blind	Employed full-time	WhatsApp; Facebook Messenger; Microsoft Teams; Google Chat; Slack; Discord	JAWS; NVDA; VoiceOver; Narrator

Table 2: Privacy and security controls explored across instant messaging applications.

Privacy/Security Control	**Applications in Which This Control Was Explored**
Last seen and online	WhatsApp, Messenger, Telegram, Snapchat, Viber
Read receipts	WhatsApp, Messenger, Telegram, Signal, Viber
Blocked users	WhatsApp, Messenger, Telegram, Snapchat, Viber
Two-step verification	WhatsApp, Telegram, Snapchat, Viber
Message timer / self-destruct timer	WhatsApp, Telegram, Signal, Viber
Who can see my profile photo	WhatsApp, Telegram, Viber
Who can add me to the group	WhatsApp, Telegram, Viber
Who can contact you	Telegram, Signal, Snapchat
App lock	WhatsApp, Telegram, Messenger
Secret chat / hidden chats / archived chats	Telegram, Viber, WhatsApp
Who can see my info/bio	WhatsApp, Telegram
Who can see your phone number	Telegram, Signal
Who can see my DOB	Telegram, Viber
Chat lock	WhatsApp
End-to-end encryption	WhatsApp, Signal
Media sharing / auto-download	WhatsApp, Telegram, Viber