Beyond Screen and Speech: Tangible Privacy and Security Interfaces for Blind and Low-Vision Instant Messaging

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

Smartphone-based instant messaging is central to everyday communication, but its privacy and security protections often depend on visual screens and spoken screen-reader output. In a qualitative study with 20 blind and low-vision screen-reader users, we found that participants sometimes avoided security features because they added inaccessible steps, felt uncertain about what data messaging apps could access, and risked exposing private messages or authentication codes when screen readers spoke content aloud. In this study we use these findings to motivate smartphone-compatible tangible privacy and security interfaces (TaPSI), such as phone attachments, wearables, or haptic buttons that communicate through vibration or physical feedback. We argue that these interfaces could help blind and low-vision users confirm security actions, understand permission states, and receive private information without broadcasting it aloud.

1 Introduction

Instant messaging applications are now routine spaces for private, social, and professional communication, but their privacy and security mechanisms remain largely tied to smartphone screens, visual interfaces, and speech-based accessibility. Prior work has shown that blind and low-vision (BLV) users face barriers in authentication [4, 9], online privacy controls [10, 11, 15], and assistive technologies, including inaccessible interfaces, eavesdropping risks, and dependence on workarounds or assistance [2, 3, 6, 12].

USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

Our study of BLV users' privacy experiences in instant messaging similarly found that protections can become ineffective when they require precise, time-sensitive, or screen-dependent interaction. In this submission, we focus on three findings from that study: the interaction burden of security features, uncertainty around app permissions, and exposure through screen-reader speech. Together, these findings show that BLV users' messaging privacy depends not only on whether protections exist, but whether they can be operated, perceived, and kept private through non-visual means.

Tangible privacy and security interfaces (TaPSI) offer a useful lens for rethinking these challenges. The TaPSI Research Framework defines TaPSI as physical tangibles that can be manipulated or perceived by touch to help users manage, protect, or understand privacy and security [8]. Its systematization identifies authentication, privacy choice mechanisms, access control, and privacy indicators and warnings as the main application areas, while also calling for more work on inclusive privacy and security since most TaPSI have not been designed or validated for accessibility [8]. Prior work on accessible haptic authentication [7, 13] and on tangible privacy management [1, 14, 16] shows how physical controls can make security actions and privacy choices more perceptible and verifiable.

This study uses our findings to motivate BLV instant messaging privacy as an important direction for TaPSI research. We show how tangible and haptic interaction could inform future smartphone-compatible designs that reduce inaccessible interaction burden, make app permission states more perceptible, and provide private feedback channels that do not broadcast sensitive content through speech.

2 Methods

We conducted an IRB-approved qualitative interview study with 20 BLV screen-reader users who regularly used instant messaging apps. This study draws on the same interview data as our companion study [5]. Interviews were remote, lasted 45–60 minutes, and covered messaging practices, privacy

and security concerns, and accessibility barriers. Participants were recruited through National Federation of the Blind mailing lists using purposive sampling; eligibility required self-identification as blind or low vision, primary screen-reader use, age 18+, US residence, and English fluency. We analyzed transcripts using inductive thematic analysis, with three researchers iteratively developing codes and themes. Here we focus on findings most relevant to tangible privacy and security interfaces.

3 Findings

3.1 Interaction burden discourages security feature use

Participants avoided or disabled security features when those features introduced additional interaction steps or accessibility burden. Two-step verification was the clearest case. Participants faced difficulties using it with a screen reader. As P15 described, *"verification areas won't allow you to paste... there's a text box for each individual number... and the timer is super duper short."* Additional barriers arise when they need to download external authenticator apps. This reflects a deeper principle, that accessibility gates security itself. P2 articulated this clearly, stating, *"if you put something encrypted in front of me that is a WCAG [Web Content Accessibility Guidelines] failure nightmare, I don't care if it's encrypted. Accessibility would still play a role... encryption is not enough if accessibility fails."*

3.2 App permission controls add uncertainty to privacy management

Participants found it difficult to understand and manage app permissions in smartphone-based messaging apps. Some accepted broad permissions to use basic features, such as sharing media or location, but were later unsure what data the app could still access or how to review or change those permissions. For screen-reader users, permission settings were not always easy to locate or interpret. As P11 noted, *"it seems harder to know if it shares the location while using the app or not. Those settings are harder to access."* This uncertainty reduced participants' confidence in controlling what information messaging apps could access.

3.3 Exposure through speech

BLV users often access messages through synthesized speech, which can make private messages and authentication codes audible in nearby physical spaces. Participants were aware of this risk and developed their own ways to manage it. For example, P19 relied on headphones to reduce exposure, *"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."* Yet this is a workaround rather than a built-in privacy protection. It requires users to actively manage the physical conditions of message access and can create a trade-off between keeping content private and remaining aware of their surroundings.

4 Discussion

Our findings point to a consistent pattern: the privacy and security problems BLV users face in messaging correspond closely to capabilities that tangible interfaces can provide.

Two of our findings share a root cause: security depends on the screen-and-speech channel, which is at once hard to operate and impossible to keep private. Codes that must be typed under a short timer are abandoned, and content spoken aloud is exposed to anyone nearby. Tangible and haptic interaction addresses both by moving interaction and feedback onto touch, perceptible to the user yet inaudible and unwatchable to others. OneButtonPIN replaces a typed PIN with a counted haptic sequence that resists eavesdropping and shoulder-surfing [13], and Haptic2FA delivers a one-time code as a felt pattern, removing the timed entry and the separate authenticator app [7]. This rests on a broader principle: tangible designs can make information perceptible to the user while shielding it from observers [1, 8]. The burden and the exposure are therefore not inherent to messaging security but to its screen-and-speech delivery, which a tangible channel can remove. Such mechanisms, however, have been built for the login moment rather than the continuous flow of messaging, and largely for authentication rather than the receipt of everyday content, pointing toward tangible privacy indicators and warnings [8] as an underexplored direction in this context.

A third problem is different in kind: BLV users cannot perceive or confirm what data an app may access, since permission state is buried and unverifiable. Access control is a core TaPSI domain [8], and tangible mechanisms have been shown to make sensor state both controllable and certain. Per-sensor controls instill high certainty of privacy in smart homes [16]. PrivacyCare externalizes privacy management into physical interaction [14]. This work targets physical sensors rather than software permissions, so the form factor does not transfer to a phone; the principle does. A tangible, eyes-free way to perceive and verify permission state remains, to our knowledge, unexplored for messaging.

5 Conclusion

For BLV users, the privacy and security failures of instant messaging share one root: protection that cannot be operated, perceived, or kept private without sight or speech. Tangible interfaces are well matched to exactly these needs, yet have

rarely been brought to everyday communication. We therefore offer BLV messaging privacy as a concrete, high-value direction for tangible privacy and security research.

Video

A short video accompanying this submission is available at: https://www.youtube.com/watch?v=7fvR0UYlzTE?hl=en&cc_load_policy=1

References

[1] Imtiaz Ahmad, Rosta Farzan, Apu Kapadia, and Adam J. Lee. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW2), October 2020. doi: 10.1145/3415187.

[2] Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia. Privacy concerns and behaviors of people with visual impairments. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, page 3523–3532, New York, NY, USA, 2015. Association for Computing Machinery. doi: 10.1145/2702123.2702334.

[3] 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, Denver, CO, June 2016. USENIX Association. URL https://www.usenix.org/conference/soups2016/technical-sessions/presentation/ahmed.

[4] 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 *Proceedings of the ACM on Web Conference 2025*, WWW '25, page 1116–1128, New York, NY, USA, 2025. Association for Computing Machinery. doi: 10.1145/3696410.3714579.

[5] Sohana Akter, Wejdan Al Sarih, Blessy Kalluri, Kopo Marvin Ramokapane, and Taslima Akter. "i feel as though my privacy is being violated": Privacy risks and barriers in instant messaging for blind and low-vision users. In *Proceedings of the Twenty-First Symposium on Usable Privacy and Security (SOUPS 2026)*. USENIX Association, 2026. To appear.

[6] 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. USENIX Association, August 2020. URL https://www.usenix.org/conference/usenixsecurity20/presentation/akter.

[7] 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. ACM Hum.-Comput. Interact.*, 8(MHCI), September 2024. doi: 10.1145/3676509.

[8] Sarah Delgado Rodriguez, Maximiliane Windl, Florian Alt, and Karola Marky. The tapsi research framework - a systematization of knowledge on tangible privacy and security interfaces. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25, New York, NY, USA, 2025. Association for Computing Machinery. doi: 10.1145/3706598.3713968.

[9] 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, Ottawa, July 2015. USENIX Association. URL https://www.usenix.org/conference/soups2015/proceedings/presentation/dosono.

[10] 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, 2022. URL https://arxiv.org/abs/2208.09959.

[11] 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, Philadelphia, PA, August 2024. USENIX Association. URL https://www.usenix.org/conference/usenixsecurity24/presentation/feng-yuanyuan.

[12] 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, Santa Clara, CA, August 2019. USENIX Association. URL https://www.usenix.org/conference/soups2019/presentation/hayes.

[13] Manisha Varma Kamarushi, Stacey L. Watson, Garreth W. Tigwell, and Roshan L. Peiris. Onebutton-pin: A single button authentication method for blind or low vision users to improve accessibility and prevent

eavesdropping. *Proc. ACM Hum.-Comput. Interact.*, 6 (MHCI), September 2022. doi: 10.1145/3546747.

[14] Vikram Mehta, Daniel Gooch, Arosha Bandara, Blaine Price, and Bashar Nuseibeh. Privacy care: A tangible interaction framework for privacy management. *ACM Trans. Internet Technol.*, 21(1), February 2021. ISSN 1533-5399. doi: 10.1145/3430506.

[15] 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. USENIX Association, August 2021. URL https://www.usenix.org/conference/soups2021/presentation/napoli.

[16] Maximiliane Windl, Albrecht Schmidt, and Sebastian S. Feger. Investigating tangible privacy-preserving mechanisms for future smart homes. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery. doi: 10.1145/3544548.3581167.