Dynamic Privacy and the Contextual Calibration of Control for Smartphones in Public Spaces

PIERO ROMARE, Chalmers University of Technology, Sweden

Smartphone users face a dual challenge: immediate physical threats like shoulder surfing and abstract risks like unauthorized camera access. While tangible tools offer protection, their adoption is mediated by usability barriers and social stigma. Drawing on an in-the-wild study ($N = 22$), this paper discusses the transition toward dynamic, context-aware privacy controls, such as built-in polarized filters and automated camera sliders. Our findings suggest that users prioritize privacy protection for proximate physical threats but view remote digital protections through a lens of social paranoia. We interpret that privacy perceptions are shaped by the psychological distance of the threat. By partially delegating control to agents and sensors that map a user's context and behavior to screen filter and camera slider settings, privacy mechanisms can be designed to reduce cognitive load while preserving social norms.

Additional Key Words and Phrases: Privacy, Smartphone, Tangible Interaction, Usability, User Experience, User Studies

1 Smartphone Privacy Control in Public Areas

Smartphone users in public spaces face a constant negotiation between utility and privacy. Privacy is frequently relegated to a secondary task [3] because primary goals, such as quick information access to service functionality, take precedence. In a recent two-week in-the-wild study ($N = 22$) [7], we investigated the impact of two tangible privacy-enhancing tools: passive privacy screen filters and active camera sliders (see Figure 1). The study suggests that the privacy screen filter successfully re-established Contextual Integrity (CI) by enforcing an appropriate transmission policy against shoulder surfing. It limits visibility to lateral angles without requiring a device owner's action, helping to prevent onlookers from visually identifying smartphone screen content without consent [2] or knowledge. Participants reported a significant decrease in concern about unwanted screen exposure ($p < 0.001$) and a reduction in physical guarding behaviors, such as angling the body or manually covering the screen ($p < 0.001$). In contrast, the camera slider represented active tangible privacy, demanding deliberate user intervention to activate/deactivate it. While intended to protect against unauthorized camera access, an invisible risk often governed by overprivileged applications [8], the slider faced significant adoption barriers. We found its effectiveness was constrained by usability issues, such as interference with FaceID and camera centric apps, leading to high abandonment rates.

2 Psychological and Interpersonal Distance

The physical space that individuals maintain in public is often proportional to the sensitivity of the data at risk. While users of fixed public terminals (like ATMs) maintain larger interpersonal distances due to high-sensitivity attributes (PINs) [4], smartphones move with their owners through diverse, overlapping physical and digital contexts.

Our study findings [7] can be interpreted through the lens of psychological distance in how users perceive these threats. Participants responded more positively to screen filters, suggesting that shoulder surfing may be viewed as a

Author's Contact Information: Piero Romare, pieror@chalmers.se, Chalmers University of Technology, Gothenburg, Sweden.

Manuscript submitted to ACM

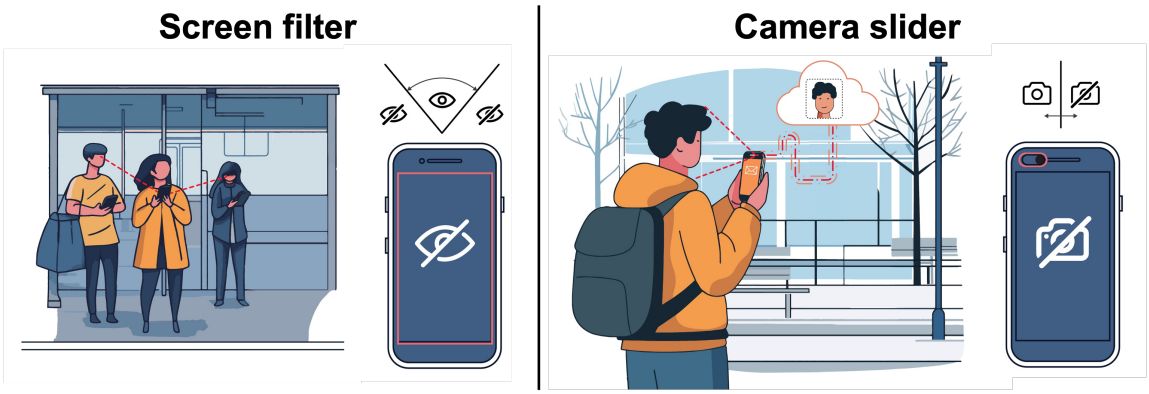

Fig. 1. The two situated privacy protection tangible tools for smartphones: privacy polarized screen filter (left) and camera slider (right) from [7]

concrete threat occurring in their immediate space. Conversely, unauthorized remote camera access tends to be viewed as an abstract or remote threat, leading to less engagement with the camera slider. This difference may be further influenced by their distinct adversary models: while the screen filter targets immediate visual onlookers in the physical environment, the camera slider addresses remote, digital adversaries. Furthermore, the social signaling of tangible tools proved to be a critical barrier. Six participants voiced concerns about being perceived as paranoid or anxious by bystanders. This underscores the need for privacy solutions that address both technical security and social dynamics.

3 Delegated Control and Dynamic Calibration

Our study demonstrated that common strategies against shoulder surfing, such as manually turning down screen brightness or angling the body, are often abandoned when tangible protection is perceived as "doing its job" [7]. This suggests an user readiness for delegated control. Considering recent innovations like dynamic screen filtering [5], systems will soon be able to adjust visibility based on specific applications or notification sensitivity. This allows for a personalization of protection where the system automatically obscures the screen for selected apps (i.e., banking or dating apps) while remaining transparent when showing a video to a friend (i.e., from social media). Furthermore, using accelerometer data alongside with a behavioral triggering system, it could be possible detect high risk environments such as public transport or crowded areas by monitoring the density of nearby bluetooth devices around. This approach serves as privacy preserving alternative to GPS location tracking. Moreover, by fusing accelerometer data and data usage patterns, systems could feasibly predict when a user intends to show a video to a friend, allowing for the automatic deactivation of the privacy screen filter.

Regarding camera privacy, we propose a shift away from purely manual sliders, which our study showed to be ineffective due to usability constraints. While smart home camera automated covering or hybrid solutions are less trusted by individuals [1], they offer a significant advantage in preventing memorability issues [6]. In the smartphone context, we suggest that the default state should be physically covered to implement privacy by default. By delegating control to a context-aware AI agent, the system can synchronize security with concrete user behaviors. For example, a behavioral triggering system could verify the actual need for the camera based on the active application, its related sensitivity, and the device owner's behavior before initiating an uncovering action. The device owner should also be able

to manually turn the camera slider on and off when the automation does not meet their needs, and they should always be informed and able to supervise camera activation to ensure data capture occurs only under explicit, intentional conditions.

4 Conclusion and Future Works

Our previous findings [7] suggest a divergence in the adoption and perception of tangible privacy tools in Figure 1 based on the psychological distance of the threat they mitigate. While passive screen filters effectively re-establish CI via suitable context-dependable restrictions of visible screen content, thereby addressing proximate physical threats like shoulder surfing, camera sliders struggle with usability barriers and social stigma. Moving forward, we suggest a transition toward dynamic, context-aware privacy mechanisms that synchronize security with the user's active digital and physical state.

Future research could prioritize the integration of AI agents and sensors to automate transitions between open and private states, thereby reducing the cognitive load of manual privacy management. This dynamic filtering should be governed by user-defined policies, allowing individuals to configure how the intelligent agent handles specific apps or environments. A primary design challenge remains in ensuring that these policies are intuitive and easy to set up, preventing the configuration process from becoming a secondary task in itself. Beyond technical implementation, another challenge remains in addressing meaningful transparency and usable control. Systems must provide clear feedback, such as UI indicators or subtle haptic cues, to confirm protection is active, particularly when users cannot visually verify effectiveness from their own viewing angle. By automating the transmission principle of CI based on app-sensitivity and behavioral triggers, design can preserve social norms while maintaining robust privacy in public spaces.

References

[1] Do, Y., Park, J.W., Wu, Y., Basu, A., Zhang, D., Abowd, G.D., Das, S.: Smart webcam cover: Exploring the design of an intelligent webcam cover to improve usability and trust. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies **5**(4), 1–21 (2021)

[2] Farzand, H., Bhardwaj, K., Marky, K., Khamis, M.: The interplay between personal relationships & shoulder surfing mitigation. In: Proceedings of Mensch und Computer 2021, pp. 338–343 (2021)

[3] Fischer-Hübner, S., Karegar, F.: Challenges of usable privacy. In: The Curious Case of Usable Privacy: Challenges, Solutions, and Prospects, pp. 103–131. Springer (2024)

[4] Li, S., Li, Y.M.: How far is far enough? a measure of information privacy in terms of interpersonal distance. Environment and Behavior **39**(3), 317–331 (2007)

[5] Samsung Newsroom: Coming soon: A new layer of privacy. https://news.samsung.com/us/coming-soon-new-layer-privacy-five-years-in-making/ (Jan 2026), press release about Samsung's new privacy layer for mobile devices, accessed 2026-02-05

[6] Shalawadi, S., Getschmann, C., van Berkel, N., Echtler, F.: Manual, hybrid, and automatic privacy covers for smart home cameras. In: Proceedings of the 2024 ACM Designing Interactive Systems Conference. pp. 3453–3470 (2024)

[7] Tjeldflaat, A.A., Romare, P., Onishi, Y., Fjeld, M., Sætrevik, B.: A two-week in-the-wild study of screen filters and camera sliders for smartphone privacy in public spaces. In: Proceedings of the Twentieth International Conference on Tangible, Embedded, and Embodied Interaction. pp. 1–17 (2026)

[8] Wu, S., Liu, J.: Overprivileged permission detection for android applications. In: ICC 2019-2019 IEEE International Conference on Communications (ICC). pp. 1–6. IEEE (2019)