A Two-Week In-the-Wild Study of Screen Filters and Camera Sliders for Smartphone Privacy in Public Spaces

Downloaded from: https://research.chalmers.se, 2026-10-16 01:42 UTC

Citation for the original published paper (version of record):
Tjeldflaat, A., Romare, P., Onishi, Y. et al (2026). A Two-Week In-the-Wild Study of Screen Filters and Camera Sliders for Smartphone Privacy in
Public Spaces. Tei 2026 Proceedings of 20th International Conference on Tangible Embedded and Embodied Interaction. http://dx.doi.org/10.1145/3731459.3773309

N.B. When citing this work, cite the original published paper.

research.chalmers.se offers the possibility of retrieving research publications produced at Chalmers University of Technology. It covers all kind of research output: articles, dissertations, conference papers, reports etc. since 2004. research.chalmers.se is administrated and maintained by Chalmers Library

(article starts on next page)

A Two-Week In-the-Wild Study of Screen Filters and Camera Sliders for Smartphone Privacy in Public Spaces

Andreas A. Tjeldflaat*
University of Bergen
Bergen, Norway
a.tjeldflaat@gmail.com

Piero Romare*
Chalmers University of Technology
and University of Gothenburg
Gothenburg, Sweden
pieror@chalmers.se

Yuki Onishi
University of Bergen
Bergen, Norway
yuki.onishi@uib.no

Morten Fjeld
t2i Lab
Chalmers University of Technology
Gothenburg, Sweden
fjeld@chalmers.se

Bjørn Sætrevik
Faculty of Psychology
University of Bergen
Bergen, Norway
bjorn.satrevik@uib.no

Abstract

Smartphone usage in public spaces can raise privacy concerns, in terms of shoulder surfing and unintended camera capture. In real-world public space settings, we investigated the impact of tangible privacy-enhancing tools (here: screen filter and camera slider) on smartphone users' reported privacy perception, behavioral adaptations, usability and social dynamics. We conducted a mixed-method, in-the-wild study ($N = 22$) using off-the-shelf smartphone privacy tools. We investigated subjective behavioral transition by combining questionnaires with semi-structured interviews. Participants used the screen filter and the camera slider for two weeks; they reported changes in attitude and behavior after using a screen filter including screen visibility and comfort when using phones publicly. They explained decreased privacy-protective behaviors, such as actively covering their screens, suggesting a shift in perceived risk. Qualitative findings about the camera slider suggested underlying psychological mechanisms, including privacy awareness and concerns about social perception, while also offering insights regarding the tools' effectiveness.

CCS Concepts

• **Security and privacy** → **Usability in security and privacy**; **Social aspects of security and privacy**; • **Applied computing** → *Psychology*; • **Human-centered computing** → **Empirical studies in ubiquitous and mobile computing**; *Smartphones.*

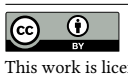
Keywords

Privacy, Smartphone, Tangible Interaction, Usability, User Experience, User Studies

ACM Reference Format:

Andreas A. Tjeldflaat, Piero Romare, Yuki Onishi, Morten Fjeld, and Bjørn Sætrevik. 2026. A Two-Week In-the-Wild Study of Screen Filters and Camera Sliders for Smartphone Privacy in Public Spaces. In *Twentieth International Conference on Tangible, Embedded, and Embodied Interaction (TEI '26), March 08–11, 2026, Chicago, IL, USA.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3731459.3773309

*Both authors contributed equally to this research.



This work is licensed under a Creative Commons Attribution 4.0 International License.
TEI '26, Chicago, IL, USA
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-1868-7/26/03
https://doi.org/10.1145/3731459.3773309

1 Introduction

In a digital world, privacy is no longer an occasional or abstract concept, but a constant, everyday challenge when interacting with smartphones in public. From smartphones to public Wi-Fi, individuals are usually around people and exposed to online tracking systems leading to privacy threats [5, 23, 48, 76]. This double exposure complicates how individuals assess and manage their privacy risks, particularly in overlapping physical and digital contexts where boundaries of information sharing is not always clear. At the same time, when people access services from their smartphone, their primary goal is usually to get quick access to the content or functionality rather than to manage their privacy. Indeed, privacy is often seen as a secondary concern [36].

There is an increasing demand to explore more intuitive and tangible forms of interaction that treat privacy not merely as a configurable setting but as a clear, actionable component of the primary user interface, motivating users to actively engage with tangible privacy mechanisms supported by direct feedback [24, 55]. Tangible and embodied solutions may support intuitive privacy management by integrating protective functions directly into everyday interactions. The adoption and utilization of online connected devices is often characterized by attitudes such as privacy concerns [26], perceived benefits and risks [42], trust [81] and perceived control [80], behavior including protection behavior and information disclosure behavior [37] and social norms driven also by cultural influences [8, 74] shaping privacy protection strategies. These strategies are shaped not only by personal beliefs but also by contextual factors, including the physical environment and perceived social acceptability. Thus, we frame our analysis using the Contextual Integrity (CI) framework, which defines privacy as the appropriate flow of information governed by specific transmission principles and attributes relevant to the context of smartphone use in public spaces. The camera slider or cover (see Figures 1 and 3, right) protects individuals from unauthorized access to their face images. Attitudes, social environment, and perceived control over protecting privacy influence the users behaviour and decision over laptop webcam covering as shown with questionnaires [50, 51].

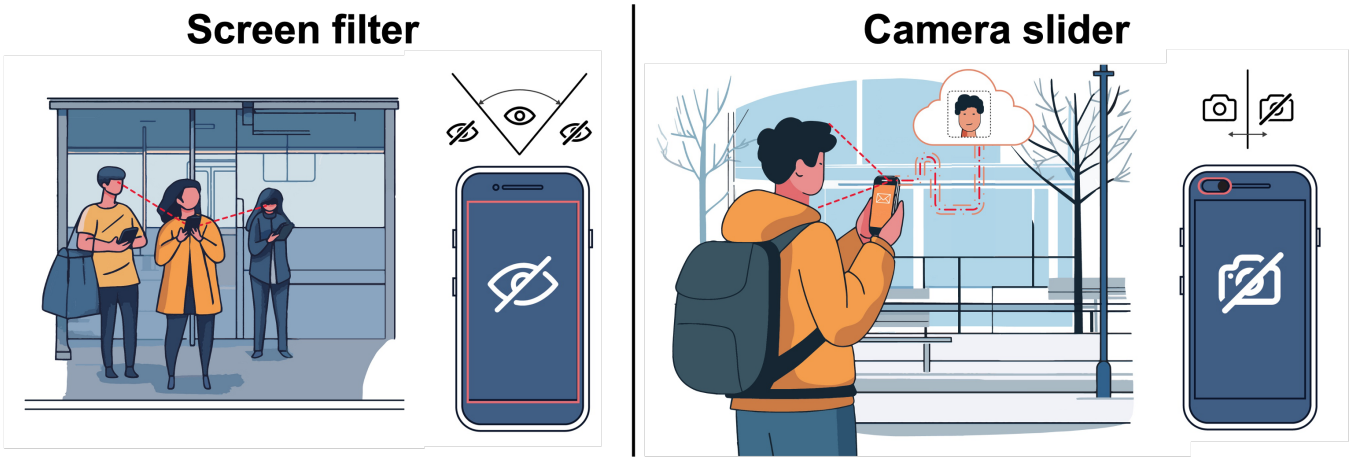


Figure 1: Everyday privacy challenges smartphone users face in public spaces, from physical intrusions like shoulder surfing (left) to invisible risks like unauthorized camera access and online data sharing (right). In addressing such challenges, we studied two tangible privacy tools; privacy screen filter (left) and camera slider (right).

The privacy screen filter or film (see Figures 1 and 3, left) can be used in everyday life for protecting privacy from shoulder surfing, and in specific contexts, such as schools, to avoid cheating [29]. By increasing the spatial frequency and decreasing the luminance contrast of visualization in a screen, it is harder for the onlooker to clearly see the details in a smartphone from a tested distance of $\approx 60 - 90$ cm, while remaining unchanged when ≈ 30 cm, showing the effectiveness of privacy protection and its usability [20, 82]. Similarly, to protect smartphone photos from onlookers, different graphical obfuscation methods were tested with the acceptability evaluated through correct identification of the obfuscated photos by the owners [75]. The Eye-shield was a software solution designed to protect images and texts in that regard, reducing recognition rates of 24% and 16% [69]. However, a recent SoK investigated the existing protection mechanisms against shoulder surfing, highlighting users' preference for non-digital alternatives [35].

In this paper, we explore the real-world impact of tangible smartphone privacy tools by focusing on two widely accessible solutions. The paper is motivated by the idea that tangible privacy tools, privacy screen filters and camera sliders, are different because of their physicality and their mechanisms influencing privacy management beyond software solutions. We argue that this physicality introduces dimensions such as control, awareness, and social interpretation, transforming how users negotiate privacy in public spaces. These tools also differ in how users engage with them: the screen filter represents passive tangible privacy, offering protection from the surrounding presence without requiring ongoing user action, in contrast to the camera slider which reflects active tangible privacy protection from online surveillance, demanding deliberate user intervention (see Figure 1). We investigate users' perceptions and everyday practices surrounding these tools, framing our discussion under the lens of CI [58].

Contributions. We preliminarily explored the impact of tangible privacy tools on engaging privacy perception through a mixed-method in-the-wild study with two types of off-the-shelf privacy tools for mobile devices using CI. The results show the following:

- The impact of privacy mobile device screen filters on enhancing the privacy perception and behavioral adaptation in public physical environments.
- The insights of social and usability challenges of the mobile device front camera slider in in public and/or social settings.
- The design interpretations on how physical usability, social perception, and contextual awareness can be balanced to support effective privacy protection.

2 Background and Related Work

This section presents a background the Contextual Integrity (CI) framework and reviews relevant existing literature. It explores the emerging field of tangible privacy tools, before specifically examining existing physical privacy protections for smartphones, such as screen filters and camera sliders, which are the focus of this paper's investigation.

2.1 Contextual Integrity

CI was elaborated by Nissenbaum [58], who defines privacy as contextual information-sharing expectation. CI identifies five parameters that are involved in structuring these norms: 1) data subject, 2) sender, 3) receiver, 4) attribute (e.g., type of information) and 5) transmission principle (e.g., conditions where the information is shared). These parameters have been widely applied to study usable privacy [52]. They are applied to understand the privacy implications from a sociotechnical perspective [9, 78]. In several contexts, studies related to information flow has been evaluated with regard to societal and contextual privacy norms to extract privacy violations when such an information flow differs from the social norms [45]. These include wearables sharing data where weight and location was perceived as less appropriate than sharing health-related attributes like heart disease risk [14]; smart voice assistance [16]; Virtual Reality (VR) classrooms that introduce new information flow within the classroom context to identify potential violations of established privacy norms [17]; virtual classrooms [22]; and video conferences where the privacy concerns include the

features related to user-tracking, such as attention, pinning and spotlighting [41]. These studies highlight the principle that, within different contexts and technologies, users' expectations of appropriate information flow depend on the sensitivity of the attribute and the context of disclosure. In this study that employed tangible privacy tools, we adopt CI as an established framework to facilitate the operationalization of privacy into concrete and observable events [7, 9].

2.2 Tangible and Embodied Privacy Tools

Research on tangible privacy is emerging and gaining scholarly attention. For example a data(pay)slip could promote user awareness about their data sharing to enhance transparency [38]. The Privacy Care Framework [56] fostered awareness and control through familiar bodily gestures, engaging haptic senses to ease privacy management. Further, [3] studied smart voice assistants and found that devices with physical privacy controls were seen as more trustworthy and usable than those with only non-tangible mechanisms. Indeed users would prefer "need for touch" and technological affinity [24]. Rodriguez et al. [62] noted that many privacy assistants lack intuitiveness and engagement, especially for less technical users, supporting tangible elements to improve usability. PriKey [25], a device-independent tangible privacy mechanism for smart homes, provides sensor-based, user-centric control over privacy invasive devices. Ahmad et al. [4] examined how bystanders would manage privacy risks in IoT applying CI and the Altman boundary regulation theory, highlighting reliance on physical environments and the need for device transparency [6].

Since webcam status LED are insufficient to deliver the recording ongoing [59], Eyecam proposes an aesthetic artifact that may increase individuals' awareness of surveillance, with multiple roles including mediator, observer, mirror, presence, and agent [72]. Webcam control and hardware toggles have been studied for smart voice assistant and smart home [3, 66] without considering the novelty effect. Regarding shoulder surfing, a few studies considered the longitudinal design to analyzed protection mechanisms [31] and authentication related threats [39]. A diary study has used as intervention design to understand who is a shoulder surfer, where and when shoulder surfing can happen [34]. Most research relies on questionnaire or interviews [31], with limited focus on behavioral impacts of tangible privacy interventions, especially in dynamic, public mobile device contexts. This paper explores the impact of tangible privacy tools through a two-week intervention in public contexts using questionnaire and interview to assess longitudinal behavioral adaptation or social environment effects.

2.3 Smartphone Tangible Privacy Tools

Existing physical privacy protections can serve as tangible privacy tools for smartphones, including microphone blockers against jamming attacks [21], RFID blockers protecting credit cards from skimming [67], two-factor authentication tokens [43, 47, 60, 61], screen filters, and camera sliders.

Screen filters help prevent shoulder surfing, a visual privacy invasion where a nearby person views a smartphone "without consent" [32]. Shoulder surfing violates the CI transmission principle as observers intercept information without consent. In public displays, the shoulder surfing is created from curiosity rather than bad intentions, since the larger is the display the more honey-pot effect is in place [18]. Considering desktop monitors and by deceiving participants, a memory test measured that they were likely to read sensitive text on larger display after finishing a small fake survey [68]. A 2016 survey found 31% of participants admitted to overlooking others' phones within a year [53], and this likely increased with smartphone diffusion. Shoulder surfing risks include identity theft, stalking, and device threats, also impacting others, such as parents and children [33]. A one-month diary study showed shoulder surfing often occurs without the victim's awareness, mostly on public transport and workplaces [34]. Indeed, by proposing public transport scenario the visual attention using eye-tracking was measured resulting that 4 out of 16 participants where able to recall the authentication pattern and that overall all the participants looked at least once at the target phone [63]. EyeSpot [40] suggested a smartphone screen hiding technique using eye-tracking that show the are of the screen content based on the user's attention. VR scenarios further revealed a behavioral attack model with idle, approach, and attack stages [1]. Depending on the viewing angle, privacy screen filters can prevent shoulder surfing from accessing sensitive information. While it can happen by accident, thus without explicit purpose rather than being bored [39], it can also led to observation attacks in the scenario where the device owner is inserting authentication credentials [28]. An easy-to-learn and use smartphone PIN system solely based on auditory or tactile stimuli has been proposed to avoid shoulder surfing [11], and for pairing the phone to external systems while preventing similar observation attacks [10]. Several schemes including spatial, temporal and visual cues have been studied to protect credentials against shoulder surfing attacks [13]. Considering the shoulder surfing perception in a questionnaire and longitudinal field study showing that 65% of participants of their questionnaire were not particularly concern about getting steal their credentials, and, if in place, others explained five measures against shoulder surfing including tilt their screen, wait the right moment, turn, covert the phone or change their unlock code. Considering the field study, only the 0.3% of the cases, the participants reported a shoulder surfer looking at their phone [39]. Findings protection strategies against shoulder surfing was the aim of [44], finding a total of seven strategies along awareness and effort dimensions. Our paper evaluates young adults' perceived privacy and behavioral adaptations toward screen filters in a two-week in-field study as partial shoulder surfing prevention.

Camera sliders offer a simple, effective means to enhance perceived privacy. Manual camera sliders tend to be trusted more than hybrid or automated options, but their long-term challenges include remembering consistent privacy actions [27]. Despite the potential user load reduction of automation, reluctance to put it into practice persists [66]. We contribute by reporting social and usability challenges of manual camera sliders.

The unique challenge of public mobile device use lies in the constant negotiation between usability and privacy in dynamic shared spaces. Users often adapt their behavior, such as angling screens away from others or covering cameras manually, depending on situational context, social norms, and perceived risk. Furthermore, while some studies examine tangible tools like webcam sliders, few intervention-based studies have assessed actual behavioral adaptation over time or in real-world social environments. Our study directly addresses this by conducting a two-week intervention with

smartphone users in their everyday public contexts, moving beyond single attitudinal indication to report changes in behavior, applying CI as encouraged by Barkhuus [7].

3 Methods

We explored how tangible privacy tools for smartphone affect users' perceived privacy and behavioral adaptations in everyday public and social settings as well as the usability challenges. These tools can be broadly characterized by their way of interaction: passive tangible privacy, such as the privacy screen filter, operates without requiring continuous user intervention; while active tangible privacy, the camera slider, demands deliberate user action to engage or not the privacy protection. To explore the impact of tangible privacy tools, we set the following Research Questions (RQs):

RQ1a : How does the level of privacy perception change with the privacy screen filter in public spaces?

RQ1b : How does the user's privacy-protecting behavior adapt with a privacy screen filter in public settings?

RQ2 : What usability challenges and concerns do users report after experiencing a camera slider in public spaces?

3.1 Participants and Ethics

We recruited ($N = 22$) participants through convenience sampling by approaching individuals at the University of Bergen. We invited individuals to take part in a study about privacy in relation to technology use, with a brief purpose of study section where the specific use of tangible privacy tools was intentionally withheld until after the initial interview to protect the integrity of the pre-intervention data. A total of 24 individuals enrolled in the study, of whom 22 completed it (11 female, 11 male) and two withdrew after the pre-intervention interview. Twenty participants were in the group age of 20-25, one was between 26-30 and one over 30. With regards to ethical considerations, the study adhered to all relevant ethical guidelines for research involving human participants. We provided and obtained informed consent from all participants, with study procedures and data handling practices clearly communicated including confidentiality and anonymity. The specific procedures and practices included the requirements to participate, such as use a screen filter and camera slider on the smartphone for two weeks, the voluntary participation and right to withdraw and how the processing of personal data would be handled according to the GDPR. The study was registered in the University of Bergen internal system for data protection assessments, which formally documents data collection and handling in line with institutional, ethical, and legal standards for research involving human subjects. The study was conducted in Norwegian and translated to English.

3.2 Procedure and Study Design

The study followed a three-phase protocol: pre-intervention, intervention, and post-intervention (see Figure 2). In the 1) pre-intervention phase, participants signed an informed consent form, which included a purposefully vague description of the study's aims to minimize response bias while still complying with transparency requirements of the GDPR. Each participant then took part in a semi-structured interview to explore their starting (baseline) attitudes toward privacy and contextual experiences related to smartphone use. Following the interview, they completed a pre-intervention questionnaire and were given the two tangible privacy tools, along with a brief explanation on their application and use. The participants received the tangible privacy tools (see Figure 3) at the end of the pre-intervention phase. We briefly explained the intended use and application of each tool. Following the experimenter's instructions, the participants added the filter and camera lens slider so that the slider was on top of the filter. During the 2) intervention phase, participants used the tools in the course of their daily lives for a period of two weeks. In order to reduce performance bias and maintain ecological validity, there were no monitoring instructions during this period. In the 3) post-intervention phase, participants took part in a second semi-structured interview focused on perceived changes in comfort, behavior, social awareness, and the usability of the tools. They also completed a post-intervention questionnaire reflecting on their experiences throughout the intervention period.

This exploratory study employed a mixed-methods experimental design to explore how tangible privacy tools affect users' perceptions and behaviors in everyday public physical settings, as well as usability and social concerns. By combining qualitative interviews with quantitative measures, the study aimed to capture both what changes occurred and why those changes may have taken place during the intervention period. The experimental setup followed a pre–post retention structure, in which participants' perceptions and behavior were compared before and after a two-week intervention. During this period, the participants used two tangible privacy tools on their smartphones. Perceived privacy and behavioral adaptation with the screen filter were evaluated through participants' reported experiences in the questionnaire and interviews across various public and social settings regarding RQ1a and RQ1b, while the usability and social challenges of the camera slider were evaluated through the interviews for RQ2. Participants used their own devices throughout, and the within-subjects design allowed each participant to serve as their own control, increasing internal validity by enabling attribution of observed changes to the use of the privacy tools.

3.3 Instruments: Questionnaire, Interviews

To assess both subjective experience and behavioral changes, the data collection combined interviews and questionnaire.

Questionnaire. Participants answered a 10-Likert scale and completed a multiple choice questionnaire both before and after intervention to assess changes in privacy perception and their behavior associated with the use of the privacy screen filter. To ensure alignment with the research questions, questionnaire items were organized into thematic subscales that captured different attitudes of the user experience (e.g., general privacy experiences, perceived privacy contexts, privacy perception, behavioral adaptations). This structure enabled targeted analysis of both perceptual shifts and behavioral adaptations across the intervention period. Both questionnaires were completed independently and anonymously. Phase 1 included the interview to establish initial privacy attitude measures (Table 6 in Appendix A.1), and the pre-intervention questionnaire that can be seen together with the post-intervention questionnaire (Table 7 in Appendix A.2) was completed after the final interview. Our statistical procedures followed the recommendations in [64, 70].

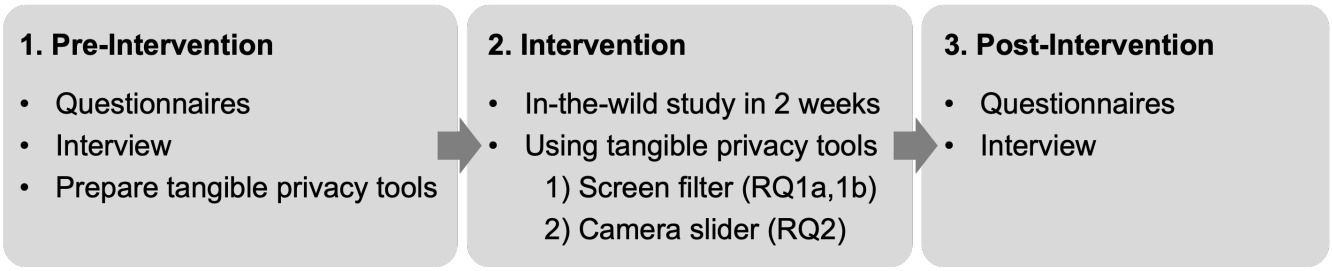


Figure 2: The three phases for our study; pre-intervention, intervention, and post-intervention.

To evaluate the entry and exit questionnaire interventions, we performed both a paired t-test and the Wilcoxon signed-rank test. Both are suitable for comparing paired or repeated measures considering a within-subject study. The paired t-test assumes that the data are normally distributed, while the Wilcoxon signed-rank test, a non-parametric alternative, was employed to account for the ordinal nature of the 10-point Likert scale and to provide robustness in the absence of normality.

Interview. After the questionnaire, two interviews were employed pre and post intervention. The pre-intervention interview contained six questions and can be fully viewed in Appendix B.1. Participants answered two general questions about their privacy protection while in public, two questions about their previous experience and awareness of shoulder surfing, and two about decisions they had made to protect their privacy in public. Similarly, in the post-intervention interview of seven questions, (for the interview, see Appendix B.2), the goal was to extract insights into the participants' experiences and interactions during the two weeks of tangible privacy tool usage. The first two authors conducted the thematic analysis of the interview transcript data by following the procedure outlined in Braun and Clarke [15]. Specifically, we 1) entirely read the interview transcripts, 2) highlighted sentences or blocks of text pertaining to our research questions, 3) assigned codes to the identified excerpts, 4) grouped the codes into overarching themes and 5) reviewed the themes and their associated excerpts to ensure consistency and coherence.

3.4 Materials and Tools

Two tangible privacy tools were used in the study (see Figure 3): a privacy filter and a camera slider. A privacy filter is a thin, polarized film that can be applied to the smartphone screen to restrict visibility from side angles, enhancing visual discretion in public spaces. The filter used in the study was an off-the-shelf two-way filter. It was designed to limit visibility from lateral (left-right) angles estimated at approximately 60-90 degrees (30-45 degrees from center on each side). It also included openings for the front-facing camera lens to avoid interference with the camera. We prepared three types of filters for Apple iPhone 11, 12/13, and 14/15 devices, and gave them to participants. All participants used their own devices; while 20 participants had Apple iPhone devices, two had Android devices. Since these Android devices' screen dimensions closely matched the iPhone models, their users also could use the filters on them. Several participants already had a protective film on their device (e.g., standard films not explicitly designed for privacy purposes). In these cases, the participants were not required to remove these first. Preliminary testing by multiple participants confirmed that the combination of protective film and privacy filter did not interfere with or significatively reduce touch sensitivity or compromise its function. The camera slider (of the brand Plexgear Webcamera Protector) was approximately 18×11×9mm. This was a black plastic mechanism consisting of a frame and circular piece that could be manually slid back and forth to block or expose the lens, enabling users to physically control camera access and limit the potential for visual surveillance. It was to be placed over the front-facing camera of the phone on top of the privacy filter, mounted with self-adhesive tape.

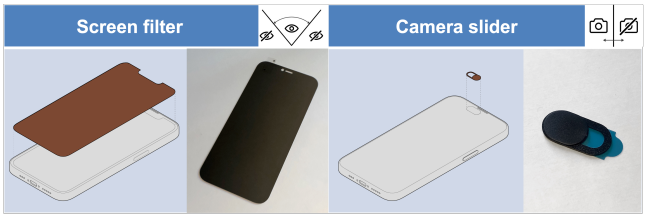


Figure 3: Tangible privacy tools provided to the participants of our study.

4 Results

In this section, we present our analysis procedures and we outline our results from the semi-structured interviews (RQ1a, RQ1b and RQ2) and the entry and exit questionnaire (RQ1a and RQ1b). In Table 1, we provide the concepts of the CI adapted to our study context.

4.1 Questionnaire Results

Given $n = 22$ participants and the use of a 10-point Likert scale, which is an ordinal scale, we ran both a paired t-test and the Wilcoxon signed-rank test to ensure the validity of our findings across different statistical assumptions [65]. We provide the p-value of the single questionnaire item comparisons to explain the statistical significance and the related effect size that provides the magnitude of the effects.

Overall, to establish internal consistency, the Cronbach's alpha (α) values for the questionnaire subscales indicated acceptable to good reliability. The privacy perception subscale demonstrated acceptable internal consistency ($\alpha \geq 0.70$) [46] in the pre-intervention,

Table 1: Contextual Integrity (CI) Parameters across the two Privacy Tools adapted to the public context.

CI Parameter	Shoulder Surfing Context	Unauthorized Camera Access Context
Data Subject	Smartphone user.	Smartphone user.
Sender	Individual actively displaying or interacting with on-screen content.	Individual operating the smartphone or app, or recording video/images.
Receiver	*Illegitimate*: bystanders or shoulder surfers. *Intended*: legitimate user or chosen peer.	*Illegitimate*: remote party, attacker, or overprivileged system process/application accessing visual data. *Intended*: legitimate user or application with explicitly granted camera access.
Attribute	Sensitive on-screen visual content (e.g., banking details, messages, or dating app interactions).	Visual data (images or video) captured by the front camera, potentially revealing personal surroundings or identity.
Transmission Principle	Expectation that on-screen content in public is visually private and not observed by others.	Expectation that camera activation and data capture occur only under explicit, intentional user consent.

Table 2: Descriptive statistics - participants' privacy attitudes in the pre-intervention phase. For all the questions the scale is: 1 = Never, 10 = Always, except for the fifth one that used 1 = Not important at all, 10 = Very important.

Question	Mean	SD	Median	Mode
How often do you actively think about who can see your screen when using your phone in a public space?	5.36	2.15	5.5	7
How often do you do something to cover your screen in order to feel more comfortable in public spaces?	4.68	1.91	4.5	3
How often have you chosen to delay or avoid using your phone due to privacy concerns in a public space?	5.27	2.16	5.5	8
Do you change how you use your smartphone depending on who is nearby?	6.91	2.33	7	7
How important is it to you that the information on your phone is only shared with people you choose yourself?	7.60	2.15	7.5	10
When you use your phone in social situations, do you tend to feel self-conscious about what's on your screen?	6.54	2.09	7	8
When you use your phone in social situations, do you tend to change how you use your phone depending on who is around you?	6.50	2.48	7	8

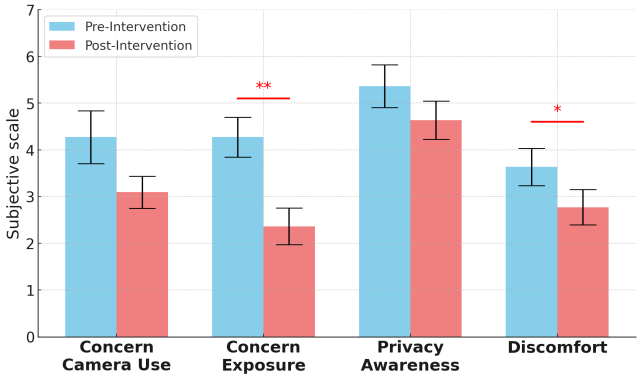
Table 3: Top three ranked categories across different smartphone use contexts (choices: library, lecture hall, common areas, street/park, café, study hall, transport, gym) and data sensitivity (choices: text/conversations, images/videos, banking/financial info, social media, study/work info, notes/calendar, shopping info.

Category	1st Rank	2nd Rank	3rd Rank
Screen Content Sensitivity	Banking / Financial Info	Texts / Conversations	Images and Videos
Highest Frequency Context	Common Areas	Public Transport	Gym
Most Comfortable Use Context	Library	Common Areas	Street / Park

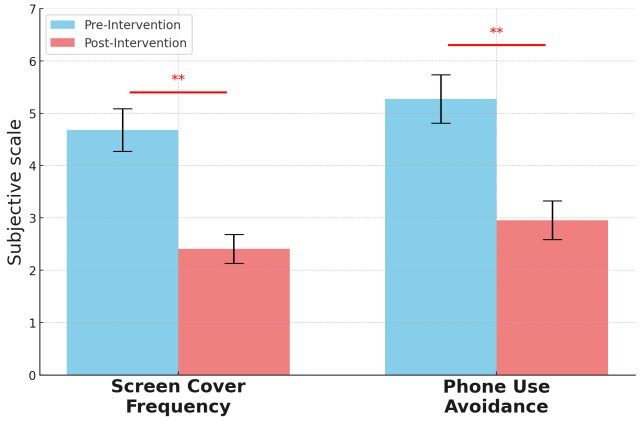
while dropping in the post-intervention. In contrast, the behavioral adaptation subscale was slightly below the threshold at pre-intervention but reached an acceptable level post-intervention. In the pre-intervention questionnaire, alpha coefficients were 0.80 for the *privacy perception* subscale and 0.66 for the *behavioral adaptation* subscale. For the post-intervention questionnaire, reliability estimates ranged from 0.64 for the *privacy perception* subscale to 0.76 for *behavioral adaptation*. Subscales that fell below the criterion suggest potential for refinement, although these values should be interpreted cautiously given the limited sample size.

Initial Privacy Attitudes. At the start of our investigation, participants demonstrated awareness and concern regarding privacy when using smartphones in public (see Table 2). On average, they sometimes actively thought about who could see their screen (Mean = 5.36, Median = 5.5) and often chose to delay or avoid phone use due to privacy concerns (Mean = 5.27, Median = 5.5). Participants also adapted their phone use reliably depending on social proximity (Mean = 6.91, Median = 7). Furthermore, the importance placed on selective information sharing was high (Mean = 7.60, Median = 7.5). However, physical protective actions, such as covering the screen, were less frequent (Mean = 4.68, Median = 4.5). Among our participants, only one had previously used a privacy screen filter before, and approximately half reported generally covering their phone cameras (e.g., not necessarily using dedicated camera sliders). Table 3 further contextualizes these attitudes by identifying smartphone use patterns, where the so-called attribute in the CI framework considered were ranked. Banking and financial information were higher ranked in the screen content sensitivity, underscoring users' heightened concern for the visibility of personal and financial data in public physical settings, followed by texts and conversations, then by images and videos. Common areas and public transport were the most frequent contexts for phone use, while participants felt most comfortable using their phones in solitary or semi-social spaces like libraries and common areas.

RQ1a *Privacy Perception.* Following the two-week intervention, participants demonstrated moderate but meaningful improvements in their concerns, awareness and discomfort (see Figure 4a). The frequency of discomfort during smartphone use in public decreased significantly ($p = 0.034, d = 0.41$), suggesting increased confidence and comfort. Notably, concern about unwanted screen exposure dropped ($p < 0.001, d = 1.1$), indicating heightened perceived control over privacy risks in public physical settings. While concern



(a) Privacy Perception.



(b) Behavioral Adaptation.

Figure 4: Privacy Perception - Behavioral Adaptation *: $p < 0.05$, **: $p < 0.01$. Original questionnaires were 10-Likert scale and we cut above 7 point of graph for readability.

about unauthorized camera use showed a decreasing trend, it did not reach statistical significance, and awareness of screen visibility remained largely unchanged ($p > 0.05$), reflecting sustained vigilance despite reduced anxiety. Although sensitivity to specific content types, such as texts, banking information, social media, images, and study/work-related content, remained stable with no statistically significant changes (see Table 4), participants, nonetheless, reported reduced avoidance of several app categories in public physical settings (Figure 5). The proportion of participants who avoided video calls dropped substantially from 82% pre-intervention to 41% post-intervention. Avoidance of social media apps declined slightly, from 18% to 14%. More pronounced reductions were observed for shopping apps from 27% to 9% and dating apps from 55% to 27%, suggesting a shift in comfort even in the absence of measurable changes in perceived content sensitivity. Overall, these findings reveal that the intervention effectively reduced generalized privacy concerns and discomfort while maintaining caution toward privacy risks, indicating a positive recalibration of perceived privacy management in public smartphone use also reflecting in CI attributes including types of information and the public context where the norms governing their transmission.

RQ1b *Behavioral Adaptation.* The intervention prompted indicated behavioral adaptations toward enhanced privacy protection in public smartphone use (see Figure 4b and Table 4 below). The frequency of physically covering the screen decreased significantly post-intervention ($p < 0.001, d = 1.1$), suggesting that participants felt less need for explicit physical protective behaviors, potentially due to increased confidence in more subtle or effective strategies. At the same time, reported avoidance of smartphone use due to privacy concerns declined markedly ($p < 0.001, d = 1.13$), indicating a broader behavioral shift toward engaging more openly with their devices in public without compromising privacy. Context-specific comfort increased significantly in more privacy-sensitive environments, with participants reporting greater ease using their phones in lecture halls ($p = 0.005, d = 0.74$), public transport ($p = 0.01, d = 0.67$), and gyms ($p = 0.042, d = 0.49$). No significant changes were observed in other common contexts (e.g., common areas, streets, cafés), suggesting the intervention's perceptual impact was strongest in settings where users initially felt more vulnerable. These exploratory findings indicate that participants became more comfortable accessing a wider range of smartphone functionalities in public spaces. The screen filter successfully re-established the transmission principle against shoulder surfing. This is evident in the data showing participants felt significantly less need for explicit behavioral guarding (e.g., physical covering of the screen) and were willing to access sensitive attributes (banking, dating apps) in vulnerable contexts like public transport. This shift confirms the tool successfully enforced the intended contextual norm for information flow. Together, the results for RQ1b demonstrate that the intervention not only influenced participants' attitudes but also led to meaningful shifts in reported app usage patterns, highlighting a transition from privacy concern to adaptive smartphone use when using the tangible privacy tools.

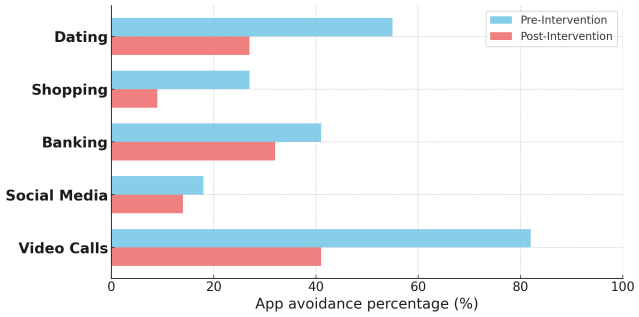


Figure 5: Percentage differences per app avoidance usage reported in pre (blue) and post (red) interventions.

4.2 Thematic Analysis of User Interview

As noted in Kumar et al. [45], qualitative reports using applied CI analysis can enhance the socio-political aspects into the more common quantitative methods. We followed their recommendations while reporting the interview results in this section, in particular identifying CI parameters, contextualizing data - in our case category of applications - and expectations, interpreting meaning, experience and social context. Participants engaged readily with the

Table 4: Privacy perception and behavioural adaptation comparison between pre and post interventions. Results from paired-sample t-tests (t) and Wilcoxon signed-rank tests (w) are shown. Statistically significant results are highlighted in bold ($*p < 0.05$, $**p < 0.01$).

	Item	p-value	Effect Size
Privacy Perception - Sensitivity	Texts/Calls	t = 1.000, w = 0.786	0.000
	Banking Info	t = 0.847, w = 0.887	-0.042
	Pictures/Videos	t = 0.919, w = 0.894	0.022
	Social Media	t = 0.584, w = 0.701	-0.119
	Study/Work Info	t = 0.136, w = 0.062	-0.331
	Notes/Calendar	t = 0.949, w = 0.810	0.014
	Shopping Info	t = 0.657, w = 0.520	-0.096
Behavioural Adaptation - Context	Library	t = 0.776, w = 0.908	-0.062
	Lecture Hall	**t = 0.002**, w = 0.005****	**0.741**
	Common Areas	t = 0.247, w = 0.251	0.254
	Street/Park	t = 0.248, w = 0.125	0.253
	Café	t = 0.329, w = 0.246	0.213
	Study Hall	t = 0.192, w = 0.191	0.288
	Transport	**t = 0.005**, w = 0.010***	**0.669**
	Gym	**t = 0.036*, w = 0.042***	**0.492**

interview format. Through thematic analysis of post-intervention semi-structured interviews we gained insights into participants' experiences, from which emerged nine codes which could be grouped into three themes: (i) perceived privacy, (ii) behavioral adaptation, and (iii) adoption and usage barriers. Thematic saturation was observed across the themes to mitigate reporting bias with a strong Cohen's kappa level of agreement [54] between the coders of 0.83.

Table 5: Themes and codes from the thematic analysis.

Themes	Codes
Perceived Privacy	Consciousness and Privacy Comfort
	Selective App Engagement
	Distrust in Privacy Tool Effectiveness
Behavioral Adaptation	Reduced Behavioral Guarding
	Expanded Public Device Usage
	Social Interaction Friction
Adoption and Usage Barriers	Technical Usability Barriers
	Social Signalling Concerns
	Emergent Privacy Awareness

4.2.1 ***RQ1a - Perceived Privacy***.

Consciousness and Privacy Comfort. Seventeen participants out of twenty-two reported feeling more aware of their screen's visibility to others in public physical settings. The use of privacy tools appeared to increase their consciousness around what others could potentially see, making them feel more in control of their digital privacy. For example, participant P05 said *"It just felt a bit more private, that was nice."* Similarly, participant P11 reflected, *"I've thought a lot about it when I've been in public, that people don't see the same from other angles. That has felt a bit comforting to me."*. With the added sense of protection, they described feeling less worried about who might be looking at their screens. Participant P04 said, *"You think less about it... just use it"*. Participant P15 shared, *"But then I noticed I was like...'Wait, I have that screen on,' so I did things because of that, instead of not using it"*. Three participants (P06, P10 and P15) used the filters implicitly, indeed P06 *"I was conscious of the camera lens, but wasn't conscious of the filter, [...] it's a good thing that they're just doing their job without me thinking about them."*. P14 added, *"I started to be a bit more conscious. I think about it once in a while. 'Oh yes, I have this screen filter.' I think I've just kind of forgotten when I've got it, so it hasn't really changed the way I've used my phone."*.

Selective App Engagement. The tools influenced participants' willingness to engage with certain apps in public. Fourteen of them described choosing to open or avoid specific applications based on how protected they felt—especially apps that could reveal personal or sensitive content. In particular, participant P03 directly included attribute and transmission principle, two aspects of the CI framework, in selecting app and context, they shared *"Then I could use [dating app] at the gym"*. Likewise, participant P24 highlighted the attribute (e.g., social media app) by explaining, *"When I'm on [social media], you kind of don't want people to see it. [...] I didn't feel so exposed"*.. Two participants (P15 and P22) don't feel constrained in using sensitive information related to banking, personal interactions or social media while in public transport, P15: *"In the bus I was like, 'Wait, I have on that screen filter', so I did things instead of not using it. So then the bank, pictures, messages and things like that"*. This shift means that users realigned their utilization of sensitive data with the attribute parameter of CI.

Distrust in Privacy Tool Effectiveness. Participants (n=3) expressed doubts about the actual effectiveness of the tools in blocking screen visibility. This skepticism often originated from the fact that they could still see the screen clearly themselves, which made it difficult to fully trust that others could not do the same from certain angles. Participant P03 and P17 discussed about social media within the family context, with P03 stating that *"I was around my family and I've gotten a [video/image from a social media app] from a friend and I didn't really trust the screen either"*. Participant P21 elaborated, *"I haven't felt that others can't see my screen. It's just that when I look*

at it from the front, I can see it myself. So, like, I don't think my brain really feels it's private".

4.2.2 ***RQ1b - Behavioral Adaptation***.

Reduced Behavioral Guarding. Nine participants reported that they stopped engaging in typical privacy-protective behaviors, such as turning down screen brightness or angling their body to shield the display. The perceived protection provided by the tools seemed to replace these earlier habits, reflecting a transfer of responsibility from the user to the tool. Participant P20 remarked, *"I don't turn down the brightness and stuff like I normally do automatically"*. Participant P16 added, *"I think I'm a bit more open in my body language. That's the only thing I've noticed"*. Participant P15 noted, *"you quickly get used to the idea that if you want to show things, you have to hand the phone over, so they can hold it themselves or try to angle it straight towards people. I feel like that became automatic very quickly [...] it was more of an adaptation thing."*

Expanded Public Device Usage. Ten participants noted a greater willingness to use their smartphones in public places, particularly in public transport. Participant P07 include useful information regarding the CI receiver: *"I write a message to my mother without feeling that someone else will get it"*. Participants P08, P10, P16, P17, P18, P20 in the public transport felt safer and more aware, with P08 stating *"I was checking something sensitive while sitting on the tram, then I felt a little bit safer."*.

Social Interaction Friction. While the tools enhanced individual privacy, they also introduced challenges in social contexts. Participants (n=5) reported that it became harder to share content with others, such as showing photos or videos to friends. Participant P24 noted, "*Another time I was reminded by others commenting on the screen [...] like...'Okay, I can't see... Why is your screen black?'*". Participant P17 added, *"Sometimes when you want to show things to people, you have to find the right angle"*. Participant P07 pointed the problem of showing videos to friends *"I try to show the same video to three different people, I have to show it several times so that everyone can see it."*.

4.2.3 ***RQ2 - Adoption and Usage Barriers***.

Usability Barriers. Usability issues were widespread and frequently mentioned. Participants (n=11) reported frustration with reduced touch sensitivity, facial recognition unlocking malfunctions, and a general decrease in product responsiveness. Participants P08, P12, P13, P14, P20, P21 reported problems with the FaceID and P12 stated, *"Yeah, it was a bit more annoying, with Face ID not working"*, with P13 that extended the problem related to the camera, *"And then it's not so easy to FaceTime, I use it several times a week"*. Furthermore, Participants P15 and P17 found problems in taking pictures, *"it's affected the quality of my front camera"*. Unfortunately, we also detected from the interviews that several participants had problems in maintaining the camera slider attached to their smartphone. Such usability barriers disrupted the normal, expected function of the smartphone.

Social Signalling Concerns. Six participants voiced concerns about how their use of privacy tools might be interpreted by others. The camera slider, in particular, was seen as a possible signal of paranoia, secrecy, or social withdrawal. Participant P08 reflected, *"If others saw the camera protector, they might think I was a kind of anxious person"*. Participant P22 explained, *"Now I have a bit more privacy on my screen, but at the same time, I want to be perceived as an open person, and then it feels wrong"*. Participant P03 discussed with others and stated *"Over the camera, I've talked to several people who think that I'm a bit paranoid, but we also agreed that it's smart"*. Participant P14 discussed about the comments received, such as *"Curiosity or maybe a bit judgmental. Like 'Do you have it? Why? Are you so super paranoid?"*. The camera slider can address the digital intrusion norm, but introduced a social norm disruption. This illustrates that while the physical tool can potentially secured the CI principle against illegitimate senders, it conflicted with implicit social norms surrounding openness and trust in public.

Emergent Privacy Awareness. Five participants explained that their awareness to protect their privacy became more present in their everyday life by being exposed to our study. Participant P08 reported, *"I maybe got a bit self-conscious about that camera protector"*. Participant P17 stated, *"The fact that you yourself somehow don't think it's possible that someone is looking through your camera, [...] so I become a bit more self-conscious"* and later came back to the topic and indicating a partial re-establishment of the security norm against this abstract threat mentioning that *"I haven't been too worried about people looking through my camera. But it was kind of nice to know that even if someone did it, they couldn't see anything."*. Participant P22 highlighted a difference in terms of effects of the two tools used during the two weeks, in particular *"In terms of privacy, I'm much more afraid of the data collected inside the phone, if you can call it that, than the people who look from the side. [...] Because it's nice to be absolutely sure that it's not possible to look at you through the camera."*

5 Discussion

This paper, focusing on tangible smartphone privacy tools, highlights that the privacy screen filter demonstrated a positive impact on perceived privacy and facilitated behavioral adaptation, whereas the camera slider encountered more social criticism and usability difficulties. In this two-week in-the-wild study with N=22 participants employed questionnaires and interviews, we found:

1. The privacy screen filter enhanced perceived privacy and encouraged behavioral adaptation in public settings (RQ1a–RQ1b): participants reported lower concern about unwanted screen exposure, decreased physical guarding behaviors, and greater comfort using sensitive apps (e.g., banking, dating) in shared environments. These findings show how the screen filter re-established appropriate information norms under the CI framework.

2. The camera slider's effectiveness was constrained by usability issues and social perception (RQ2): interference with functions such as FaceID and camera use, together with worries about appearing anxious or paranoid, hindered adoption and social acceptability, limiting its perceived privacy benefits.

3. Perceived proximity of privacy threats may shape interaction with tangible privacy tools: while still exploratory, in our study, participants reacted more strongly to concrete, immediate risks (e.g., shoulder surfing) than to abstract ones (e.g., remote

camera access). This emphasizes the designing of tools that address both technical, psychological and social dimensions of privacy.

5.1 Privacy Screen Filter

In this study, we applied the CI framework. A privacy screen filter therefore helps preserve CI by enforcing the appropriate transmission principle, limiting the flow of information so that it reaches only the intended recipient and preventing passive data acquisition by illegitimate recipients (e.g., shoulder surfers).

Enhancing Privacy Perception. The privacy screen filter significantly improved perceived screen privacy (RQ1a), evidenced by a notable decrease in concern about unwanted screen exposure ($p < 0.001, d = 1.1$) and reduced discomfort during public smartphone use ($p = 0.034, d = 0.41$). Participants frequently reported feeling more aware of their screen's visibility to others in public physical settings, which made them feel more in control of their privacy. Furthermore, the screen filter's effectiveness was sometimes so seamless that participants like P06 noted it was *"a good thing that they're just doing their job without me thinking about them"*. No statistical significance was found regarding the sensitivity to explicit content information on the smartphone screen. However, participants reported that the filter enabled them to comfortably access a wider range of previously avoided app categories, such as video calls (avoidance decreased substantially from 82% pre-intervention to 41% post-intervention), shopping apps (27% to 9%), and dating apps (55% to 27%). This perception of app usage expansion signifies a realignment of user utilization with the attribute (type of information) parameter of CI. Participants felt comfortable using applications containing sensitive information, like banking or dating apps, in public transport, confirming the findings in [34], because the screen filter helped establish an appropriate information flow while preventing unauthorized viewing because of shoulder surfing. As Participant P08 stated, *"I was checking something sensitive while sitting on the tram, then I felt a bit safer"*, which supports how the tool facilitated adherence to their personal contextual norms for information sharing.

Adapting Behavior in Public Use. Our study also noted behavioral adaptations (RQ1b) toward enhanced privacy protection in public smartphone use. The frequency of physically covering the screen decreased significantly post-intervention ($p < 0.001, d = 1.1$), suggesting that participants felt less need for explicit privacy-protective behaviors, possibly due to increased confidence in the filter's subtle effectiveness. Participant P20 remarked, *"It's kind of like I don't turn down the brightness and stuff like I normally do automatically"*. Meanwhile, reported avoidance of smartphone use due to privacy concerns declined ($p < 0.001, d = 1.13$), indicating a behavioral shift toward expanded public device usage. This behavioral adaptation directly relates to the transmission principle of CI, as users felt more assured that their information was being shared only under their desired conditions and not intercepted by shoulder surfers. The increased comfort was particularly significant in environments previously investigated with similar results in [34], such as lecture halls ($p = 0.005, d = 0.74$), public transport ($p = 0.01, d = 0.67$), and gyms ($p = 0.042, d = 0.49$), highlighting how the filter helped align information flow with specific contextual norms where screen visibility is often expected to be limited.

Usability and Tool Effectiveness. While predominantly positive, the screen filter presented some usability challenges. Participants occasionally (n=2) needed to adjust their viewing positions, especially when not looking at the phone head-on, with participant P08 noting, *"If I'm sitting on the sofa in a few different types of positions and I'm looking at my phone, I notice that I either have to straighten up or hold it"*. Furthermore, social interaction friction was observed when participants (n=5) attempted to share screen content with others. This suggests that while the filter improved individual privacy by controlling the transmission principle for personal viewing, it could inadvertently impede the ease of shared viewing, a different facet of information flow within social contexts. Qualitatively, three participants also expressed a distrust in privacy tool effectiveness, as they could still see their own screen clearly from the front, making it difficult to fully believe others could not do the same from different angle. Given that participants' comfort increased significantly in specific contexts, future screen filters could be designed to integrate with smartphone sensors or app usage data. This could allow for context-aware activation, automatically engaging the filter when the user enters a privacy-sensitive environment or opens a sensitive application (e.g., banking app), aligning with the transmission principle and attribute parameters of CI. Moreover, filters that can dynamically adjust their privacy level based on the proximity of people in front of the screen via a temporary stopping of the "privacy" filter mode, could be a further development opportunity to explore.

5.2 Camera Slider

While the screen filter protects against illegitimate visual receivers (e.g., shoulder surfers) in the physical space, the camera slider protects against illegitimate visual senders (e.g., app, attacker, system process) that was not contextually allowed to receive it in the digital space. The camera slider, while intended to prevent unauthorized camera access, faced more social criticism and usability challenges (RQ2). As communicated in the interview results (n=11), its adoption was limited due to issues with the slide, for example four participants reported that its use sometimes interfered with standard phone functions like facial recognition unlocking, or using camera-centric applications, such as some social media, indeed Participant P17 exposed, *it's affected the quality of my front camera.* A solution about FaceID, obfuscating with a physical blur layer the camera, was proposed for FaceID smartphone authentication method achieving 95% of accuracy for authentication and 100% for deauthentication [19]. Furthermore, participants (n=4) expressed concerns about how the visible presence of a camera slider might be perceived by others, leading to worries about appearing anxious or paranoid, Participant P08 explained, *If others saw the camera protector, they might think I was a kind of anxious person.* This social signaling aspect can create inconvenience, potentially stopping the perceived privacy benefits if users feel socially disadvantaged by using the tool. The social learning theory applied to the webcam covering demonstrated that people with low self-control prefer to use the webcam covering when they are aware of the potential risks, or after having experienced privacy violation themselves [57].

This indicates that while tangible tools can enhance privacy perception, their design should also account for social dynamics, as found for laptop webcam [50], and practical user experience to achieve broader adoption and behavioral change. Future designs should aim to mitigate these practical inconveniences and social friction points to maximize the effectiveness of such privacy solutions. Integrating automation with clear user feedback may support privacy awareness even when users forget to act, helping maintain trust and reducing social friction.

5.3 Contextual Integrity

Regarding the CI framework, the passive privacy screen filter successfully re-established CI by enforcing the appropriate transmission principle against shoulder surfing. Before the intervention, the norm required the data subject to actively intervene (e.g., angling the screen, covering it) to enforce the non-interception rule (see Table 2). Limiting the flow of sensitive attributes (e.g., banking or dating app data), as highlighted also during the interview from P15 and P22: "didn't feel so exposed", from illegitimate receivers significantly improve the reduction of physical covering and change the transmission principle. Indeed, Participant P07: "I write a message to my mother without feeling that someone else will get it". The filter reinforces the integrity of the communication channel by guaranteeing the information reaches only the chosen receiver. This reintroduce the expected privacy norm that led to significant behavioral adaptation, since participants dropping physical guarding behaviors and expanding their use of sensitive applications, as reported in the qualitative findings with around the half of participants (n=11), including in public transport and lecture halls, as in [34], and gym where P03: "could use [dating app] at the gym". In contrast, the camera slider illustrates a conflict in norm preservation: while it enforces a technical CI principle against illegitimate remote senders in the digital space, its physical visibility disrupted critical social norms in the public context. It introduced social friction when users needed to share content with authorized receivers (e.g., friends), forcing users to adjust the angle or hand over the phone. Participants' worries about being negatively judged by others (n=6) and the presence of technical usability conflicts (n=11) confirm that attempting to enforce one CI norm can lead to the disruption of other practical usability property or social norms.

5.4 Psychological Distance and Design Implications

The different findings between the two tools offer implications for the design and deployment of tangible privacy tools. First, our study confirms that usability is relevant for the adoption and effectiveness of privacy solutions [49]. The camera slider's technical glitches and social friction points can create problems for the participants, while the screen filter facilitated demonstrable changes in behavior and perception. This suggests that merely providing a privacy mechanism is insufficient; its design should proactively mitigate practical inconveniences and account for social dynamics to enable behavioral changes.

Psychological Distance and Tangible Privacy Perception. While differences in usability offer a initial explanation for the divergent reception of the two tools, there may also be a complementary psychological dimension at play. Specifically, users may perceive and respond more readily to privacy threats that feel immediate and tangible, such as the risk of shoulder surfing mitigated by the screen filter, compared to more abstract or remote threats, like unauthorized camera access. This distinction aligns with the Construal Level Theory (CLT), which states that individuals mentally establish events that are psychologically distant, whether in time, space, social context, or likelihood, at a higher, more abstract level, than what is taking place for the individual in the current here-and-now [73]. Applied to this study, previous experiences may play a role, together with the immediate visual threat of shoulder surfing being psychologically "closer" and more concrete, leading to a more positive recognition of the screen filter. In contrast, the abstract, potential threat of remote camera access might be psychologically "further", leading to less engagement with the camera slider, especially when compounded by usability issues [2, 77]. Regarding laptop webcam, individuals' level of concern does not significantly impact their decision to cover it [50]. Moreover, this interpretation aligns with the control paradox regarding the camera as part of smart assistants studied on tangible privacy feedbacks, where participants felt less risks since the decreased ambiguity about the device status [3].

Design Implications for Tangible Privacy Tools. Despite these issues, some participants reported an emergent privacy awareness regarding their camera, acknowledging a new sense of security in knowing that remote access would be blocked, as Participant P17: *"I haven't been too worried about people looking through my camera. But it was kind of nice to know that even if someone did it, they couldn't see anything."*. More studies are needed considering that the literature demonstrated how individuals prefer a manual action to activate the protection on their smart home cameras as they feel to be in control even if the cognitive load is high [66]. On the other hand, the automatic protection of laptop cameras showed more reliability and helped to avoid human error [27]. The tool itself demands an additional active step for the user, which requires memory while accessing the smartphone functionalities. In our results, we found contextual predispositions when our participants were bothered by the camera slider, in particular while accessing the FaceID for authenticating themselves and while accessing social media where taking photos or videos is an essential functionality. Our preliminary results would motivate the tangible and embodied community to investigate further effective and simple tangible privacy solutions considering contextual properties, privacy perceptions and social acceptance. Future works could include the designing and testing hybrid, context-aware tangible privacy solutions, such as a privacy screen filter that polarized the screen while accessing to banking app or a camera slider that uncover the camera when individuals take the phone from the pocket since it often follows the authentication procedure with facial recognition. Indeed the hybrid camera covering has been confirmed to be effective [27]. Furthermore, future works could also explore how social contexts and the presence of bystanders influence the continued use, perceived safety, and social acceptability of tangible privacy tools. In this context, the bystander can be seen as unauthorized receiver or a potential sender under the CI lens. For instance, observational or play-acted scenarios could be designed where a shoulder surfer

challenge the participant's visible use of a camera cover or screen filter. Such settings would help to understand how users negotiate privacy norms when potential observers or threat actors are present. Previous works studies the camera use in public settings including live streaming, from the streamer side who usually have the direct control of the recordings [79] and the bystanders one who often are unaware of others people recordings [30]. Bystanders are interested in being part of the streaming process, including visual consent for the recording [71] and the possibility to block transmission [12]. Measuring the comfort of the bystanders while the streamer's device is equipped with a camera slider or tangible or digital obfuscation techniques could provide further insights regarding their privacy in public settings.

6 Limitations

Conducting an in-the-wild study involves trade-offs, as participants interact with the tools in their natural environments without direct researcher supervision. Because of some attachment problems of the camera slider in the participants' phones reported during the post-intervention interviews, we decided to not include the questions regarding the camera slider behavioral adaptation in the main body of this report, while keeping the perceived privacy information as in Figure 4a. The unreported questions are available in Appendix A.3 with descriptive statistics. The sample size of our investigation was relatively small ($N = 22$), especially regarding the questionnaire results in Figure 4 and Table 4, which necessitates caution in interpreting and generalizing the findings. Further, our participants were mostly students belonging to a certain age group, which may have also limited the possible range of responses.

7 Conclusion

This study explored the real-world impact of tangible smartphone privacy tools, specifically privacy screen filters and camera sliders, on users' perceptions and behavioral adaptations in public spaces. Employing a two-week, mixed-method, in-the-wild design with 22 participants, the research provided insights into the efficacy and challenges associated with these privacy solutions. Our findings highlight distinct outcomes for each tool; the privacy screen filter demonstrated a positive impact on users' perceived privacy and facilitated the behavioral adaptation, while the camera slider elicited more social criticism and usability difficulties.

Acknowledgments

We thank the participants for their active engagement during the two weeks of data collection. We thank the anonymized reviewers for their useful comments. This work was partially supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation.

References

[1] Yasmeen Abdrabou, Radiah Rivu, Tarek Ammar, Jonathan Liebers, Alia Saad, Carina Liebers, Uwe Gruenefeld, Pascal Knierim, Mohamed Khamis, Ville Mäkelä, et al. 2022. Understanding Shoulder Surfer Behavior Using Virtual Reality. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. IEEE, 576–577.

[2] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 40–46.

[3] Imtiaz Ahmad, Taslima Akter, Zachary Buher, Rosta Farzan, Apu Kapadia, and Adam J Lee. 2022. Tangible privacy for smart voice assistants: Bystanders' perceptions of physical device controls. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–31.

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

[5] Suzan Ali, Tousif Osman, Mohammad Mannan, and Amr Youssef. 2019. On privacy risks of public wifi captive portals. In *International Workshop on Data Privacy Management*. Springer, 80–98.

[6] I. Altman. 1975. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole Publishing Company. https://books.google.it/books?id=GLBPAAAAMAAJ

[7] Louise Barkhuus. 2012. The mismeasurement of privacy: using contextual integrity to reconsider privacy in HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 367–376.

[8] Ardion Beldad and Margareta Citra Kusumadewi. 2015. Here's my location, for your information: The impact of trust, benefits, and social influence on location sharing application use among Indonesian university students. *Computers in human behavior* 49 (2015), 102–110.

[9] Sebastian Benthall, Seda Gürses, Helen Nissenbaum, et al. 2017. Contextual integrity through the lens of computer science. *Foundations and Trends® in Privacy and Security* 2, 1 (2017), 1–69.

[10] Andrea Bianchi. 2010. Authentication on public terminals with private devices. In *Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction*. 429–430.

[11] Andrea Bianchi, Ian Oakley, Vassilis Kostakos, and Dong Soo Kwon. 2010. The phone lock: audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices. In *Proceedings of the fifth international conference on Tangible, embedded, and embodied interaction*. 197–200.

[12] Jürgen Bohn, Vlad Coroamă, Marc Langheinrich, Friedemann Mattern, and Michael Rohs. 2005. Social, economic, and ethical implications of ambient intelligence and ubiquitous computing. In *Ambient intelligence*. Springer, 5–29.

[13] Leon Bošnjak and Boštjan Brumen. 2020. Shoulder surfing experiments: A systematic literature review. *Computers & Security* 99 (2020), 102023.

[14] August Bourgeus, Laurens Vandercruysse, and Nanouk Verhulst. 2024. Understanding contextual expectations for sharing wearables' data: Insights from a vignette study. *Computers in Human Behavior Reports* 15 (2024), 100443.

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

[16] Saba Rebecca Brause and Grant Blank. 2024. 'There are some things that I would never ask Alexa'–privacy work, contextual integrity, and smart speaker assistants. *Information, Communication & Society* 27, 1 (2024), 182–197.

[17] Karoline Brehm and Yan Shvartzshnaider. 2023. Understanding privacy in virtual reality classrooms: A contextual integrity perspective. *IEEE Security & Privacy* 22, 1 (2023), 53–62.

[18] Frederik Brudy, David Ledo, Saul Greenberg, and Andreas Butz. 2014. Is anyone looking? mitigating shoulder surfing on public displays through awareness and protection. In *Proceedings of the international symposium on pervasive displays*. 1–6.

[19] Matteo Cardaioli, Mauro Conti, Gabriele Orazi, Pier Paolo Tricomi, and Gene Tsudik. 2023. BLUFADER: Blurred face detection & recognition for privacy-friendly continuous authentication. *Pervasive and Mobile Computing* 92 (2023), 101801.

[20] Chun-Yu Chen, Bo-Yao Lin, Junding Wang, and Kang G Shin. 2019. Keep others from peeking at your mobile device screen!. In *The 25th Annual International Conference on Mobile Computing and Networking*. 1–16.

[21] Yuxin Chen, Huiying Li, Shan-Yuan Teng, Steven Nagels, Zhijing Li, Pedro Lopes, Ben Y Zhao, and Haitao Zheng. 2020. Wearable microphone jamming. In *Proceedings of the 2020 chi conference on human factors in computing systems*. 1–12.

[22] Shaanan Cohney, Ross Teixeira, Anne Kohlbrenner, Arvind Narayanan, Mihir Kshirsagar, Yan Shvartzshnaider, and Madelyn Sanfilippo. 2021. Virtual classrooms and real harms: Remote learning at {US}. universities. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. 653–674.

[23] Mathieu Cunche. 2014. I know your MAC address: targeted tracking of individual using Wi-Fi. *Journal of Computer Virology and Hacking Techniques* 10, 4 (2014), 219–227.

[24] Sarah Delgado Rodriguez, Priyasha Chatterjee, Anh Dao Phuong, Florian Alt, and Karola Marky. 2024. Do you need to touch? exploring correlations between personal attributes and preferences for tangible privacy mechanisms. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–23.

[25] Sarah Delgado Rodriguez, Sarah Prange, Pascal Knierim, Karola Marky, and Florian Alt. 2022. Experiencing Tangible Privacy Control for Smart Homes with PriKey. In *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia*. 298–300.

[26] Tobias Dienlin and Sabine Trepte. 2015. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European journal of social psychology* 45, 3 (2015), 285–297.

[27] Youngwook Do, Jung Wook Park, Yuxi Wu, Avinandan Basu, Dingtian Zhang, Gregory D Abowd, and Sauvik Das. 2021. 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 (2021), 1–21.

[28] Malin Eiband, Mohamed Khamis, Emanuel Von Zezschwitz, Heinrich Hussmann, and Florian Alt. 2017. Understanding shoulder surfing in the wild: Stories from users and observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 4254–4265.

[29] Michael P Escudier, Jorge A Tricio, and Edward W Odell. 2014. Student Acceptability of High-Stakes e-Assessment in Dental Education: Using Privacy Screen Filters to Control Cheating. *Journal of dental education* 78, 4 (2014), 558–566.

[30] Cori Faklaris, Francesco Cafaro, Asa Blevins, Matthew A O'Haver, and Neha Singhal. 2020. A snapshot of bystander attitudes about mobile live-streaming video in public settings. In *Informatics*, Vol. 7. MDPI, 10.

[31] Habiba Farzand. 2025. *Understanding shoulder surfing and informing the design of protection mechanisms*. Ph. D. Dissertation. University of Glasgow.

[32] Habiba Farzand, Kinshuk Bhardwaj, Karola Marky, and Mohamed Khamis. 2021. The interplay between personal relationships & shoulder surfing mitigation. In *Proceedings of Mensch und Computer 2021*. 338–343.

[33] Habiba Farzand, Shaun Macdonald, Karola Marky, and Mohamed Khamis. 2024. " What you think is private is no longer"–Investigating the Aftermath of Shoulder Surfing on Smartphones in Everyday Life through the Eyes of the Victims. *arXiv preprint arXiv:2411.18265* (2024).

[34] Habiba Farzand, Karola Marky, and Mohamed Khamis. 2022. Shoulder surfing through the social lens: A longitudinal investigation & insights from an exploratory diary study. In *Proceedings of the 2022 european symposium on usable security*. 85–97.

[35] Habiba Farzand, Karola Marky, and Mohamed Khamis. 2024. SoK: Privacy Personalised–Mapping Personal Attributes\& Preferences of Privacy Mechanisms for Shoulder Surfing. *arXiv preprint arXiv:2411.18380* (2024).

[36] Simone Fischer-Hübner and Farzaneh Karegar. 2024. *The Curious Case of Usable Privacy: Challenges, Solutions, and Prospects*. Springer.

[37] Nina Gerber, Paul Gerber, and Melanie Volkamer. 2018. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security* 77 (2018), 226–261.

[38] Alejandra Gómez Ortega, Renee Noortman, Jacky Bourgeois, and Gerd Kortuem. 2024. Dataslip: Into the Present and Future (s) of Personal Data. In *Proceedings of the Eighteenth International Conference on Tangible, Embedded, and Embodied Interaction*. 1–14.

[39] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. {It's} a hard lock life: A field study of smartphone ({Un) Locking} behavior and risk perception. In *10th symposium on usable privacy and security (SOUPS 2014)*. 213–230.

[40] Mohamed Khamis, Malin Eiband, Martin Zürn, and Heinrich Hussmann. 2018. Eyespot: Leveraging gaze to protect private text content on mobile devices from shoulder surfing. *Multimodal Technologies and Interaction* 2, 3 (2018), 45.

[41] Hobin Kim, Wonho Song, Joseph Seering, and Min Suk Kang. 2025. Understanding User Privacy Perceptions in Video Conferencing: Insights from a Feature-Specific User Study. *Proceedings on Privacy Enhancing Technologies* (2025).

[42] Mehrdad Koohikamali, Natalie Gerhart, and Mohammadreza Mousavizadeh. 2015. Location disclosure on LB-SNAs: The role of incentives on sharing behavior. *Decision Support Systems* 71 (2015), 78–87.

[43] Kat Krol, Eleni Philippou, Emiliano De Cristofaro, and M Angela Sasse. 2015. "They brought in the horrible key ring thing!" Analysing the Usability of Two-Factor Authentication in UK Online Banking. In *USEC Workshop on Usable Security at the Network and Distributed System Security Symposium*.

[44] Romina Kühn, Mandy Korzetz, and Thomas Schlegel. 2019. User strategies for mobile device-based interactions to prevent shoulder surfing. In *Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia*. 1–5.

[45] Priya C Kumar, Michael Zimmer, and Jessica Vitak. 2024. A roadmap for applying the contextual integrity framework in qualitative privacy research. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1 (2024), 1–29.

[46] Charles E Lance, Marcus M Butts, and Lawrence C Michels. 2006. The sources of four commonly reported cutoff criteria: What did they really say? *Organizational research methods* 9, 2 (2006), 202–220.

[47] Juan Lang, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas. 2016. Security keys: Practical cryptographic second factors for the modern web. In *International Conference on Financial Cryptography and Data Security*. Springer, 422–440.

[48] Mengyuan Li, Yan Meng, Junyi Liu, Haojin Zhu, Xiaohui Liang, Yao Liu, and Na Ruan. 2016. When CSI meets public WiFi: Inferring your mobile phone password via WiFi signals. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 1068–1079.

[49] Sonia Livingstone. 2008. Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New media & society* 10, 3 (2008), 393–411.

[50] Dominique Machuletz, Stefan Laube, and Rainer Böhme. 2018. Webcam covering as planned behavior. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–13.

[51] Dominique Machuletz, Henrik Sendt, Stefan Laube, and Rainer Böhme. 2016. Users protect their privacy if they can: Determinants of webcam covering behavior. In *Proceedings of the European Workshop on Usable Security at the Privacy Enhaning Technologies Symposium (EuroSEC'16)(EuroUSEC'16). Internet Society, Reston, VA. https://doi. org/10.14722/eurousec*.

[52] Nathan Malkin. 2022. Contextual integrity, explained: A more usable privacy definition. *IEEE Security & Privacy* 21, 1 (2022), 58–65.

[53] Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luís Carriço, and Konstantin Beznosov. 2016. Snooping on mobile phones: Prevalence and trends. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX, Denver, USA, 159–174.

[54] Mary L McHugh. 2012. Interrater reliability: the kappa statistic. *Biochemia medica* 22, 3 (2012), 276–282.

[55] Vikram Mehta. 2019. Tangible interactions for privacy management. In *Proceedings of the Thirteenth International Conference on Tangible, Embedded, and Embodied Interaction*. 723–726.

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

[57] Jason Nicholson, George E Higgins, and Catherine D Marcum. 2025. How much protection is enough? Predicting the use of webcam protective measures through the lens of low self-control and social learning. *Security Journal* 38, 1 (2025), 2.

[58] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[59] Rebecca S Portnoff, Linda N Lee, Serge Egelman, Pratyush Mishra, Derek Leung, and David Wagner. 2015. Somebody's watching me? assessing the effectiveness of webcam indicator lights. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 1649–1658.

[60] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. 2019. A Usability Study of Five Two-Factor Authentication Methods. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 357–370. https://www.usenix.org/conference/soups2019/presentation/reese

[61] Joshua Reynolds, Trevor Smith, Ken Reese, Luke Dickinson, Scott Ruoti, and Kent Seamons. 2018. A tale of two studies: The best and worst of yubikey usability. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 872–888.

[62] Sarah Delgado Rodriguez, Sarah Prange, and Florian Alt. 2021. Take Your Security and Privacy Into Your Own Hands! Why Security and Privacy Assistants Should be Tangible.. In *MuC (Workshopband)*.

[63] Alia Saad, Jonathan Liebers, Uwe Gruenefeld, Florian Alt, and Stefan Schneegass. 2021. Understanding bystanders' tendency to shoulder surf smartphones using 360-degree videos in virtual reality. In *Proceedings of the 23rd International Conference on Mobile Human-Computer Interaction*. 1–8.

[64] Mariah Schrum, Muyleng Ghuy, Erin Hedlund-Botti, Manisha Natarajan, Michael Johnson, and Matthew Gombolay. 2023. Concerning trends in likert scale usage in human-robot interaction: Towards improving best practices. *ACM Transactions on Human-Robot Interaction* 12, 3 (2023), 1–32.

[65] Mariah L Schrum, Michael Johnson, Muyleng Ghuy, and Matthew C Gombolay. 2020. Four years in review: Statistical practices of likert scales in human-robot interaction studies. In *Companion of the 2020 ACM/IEEE International Conference on Human-Robot Interaction*. 43–52.

[66] Sujay Shalawadi, Christopher Getschmann, Niels van Berkel, and Florian Echtler. 2024. Manual, Hybrid, and Automatic Privacy Covers for Smart Home Cameras. In *Proceedings of the 2024 ACM Designing Interactive Systems Conference*. 3453–3470.

[67] Sarah Spiekermann. 2009. RFID and privacy: what consumers really want and fear. *Personal and Ubiquitous Computing* 13 (2009), 423–434.

[68] Desney S Tan and Mary Czerwinski. 2003. Information voyeurism: Social impact of physically large displays on information privacy. In *CHI'03 extended abstracts on Human factors in computing systems*. 748–749.

[69] Brian Jay Tang and Kang G. Shin. 2023. Eye-Shield: Real-Time Protection of Mobile Device Screen Information from Shoulder Surfing. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 5449–5466. https://www.usenix.org/conference/usenixsecurity23/presentation/tang

[70] Jenny Tang, Lujo Bauer, and Nicolas Christin. 2025. Misuse, Misreporting, Misinterpretation of Statistical Methods in Usable Privacy and Security Papers. (2025).

[71] Devin Tebbe, Yosr Aissa, Braeden Burger, and Douglas Zytko. 2025. " Like, Are You Okay With Being Recorded?": Understanding and Designing for Consent to Recording and Livestreaming. In *Companion Publication of the 2025 Conference on Computer-Supported Cooperative Work and Social Computing*. 504–508.

[72] Marc Teyssier, Marion Koelle, Paul Strohmeier, Bruno Fruchard, and Jürgen Steimle. 2021. Eyecam: Revealing relations between humans and sensing devices through an anthropomorphic webcam. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–13.

[73] Yaacov Trope and Nira Liberman. 2010. Construal-level theory of psychological distance. *Psychological review* 117, 2 (2010), 440.
[74] Ellen Van Gool, Joris Van Ouytsel, Koen Ponnet, and Michel Walrave. 2015. To share or not to share? Adolescents' self-disclosure about peer relationships on Facebook: An application of the Prototype Willingness Model. *Computers in Human Behavior* 44 (2015), 230–239.
[75] Emanuel Von Zezschwitz, Sigrid Ebbinghaus, Heinrich Hussmann, and Alexander De Luca. 2016. You can't watch this! privacy-respectful photo browsing on smartphones. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 4320–4324.
[76] Mengyuan Wang, Hongbo Jiang, Peng Peng, and Youhuan Li. 2023. Accurately estimating frequencies of relations with relation privacy preserving in decentralized networks. *IEEE Transactions on Mobile Computing* 23, 5 (2023), 6408–6422.
[77] Meredydd Williams, Jason RC Nurse, and Sadie Creese. 2016. The perfect storm: The privacy paradox and the Internet-of-Things. In *2016 11th International Conference on Availability, Reliability and Security (ARES)*. IEEE, 644–652.
[78] Pamela J Wisniewski and Xinru Page. 2022. Privacy theories and frameworks. In *Modern socio-technical perspectives on privacy*. Springer International Publishing Cham, 15–41.
[79] Yanlai Wu, Xinning Gui, Pamela J Wisniewski, and Yao Li. 2023. Do streamers care about bystanders' privacy? an examination of live streamers' considerations and strategies for bystanders' privacy management. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1 (2023), 1–29.
[80] Heng Xu, Hock-Hai Teo, Bernard CY Tan, and Ritu Agarwal. 2012. Research note—effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services. *Information systems research* 23, 4 (2012), 1342–1363.
[81] Bo Zhang, Mu Wu, Hyunjin Kang, Eun Go, and S Shyam Sundar. 2014. Effects of security warnings and instant gratification cues on attitudes toward mobile websites. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. 111–114.
[82] Songheng Zhang, Dong Ma, and Yong Wang. 2023. Don't Peek at My Chart: Privacy-preserving Visualization for Mobile Devices. In *Computer Graphics Forum*, Vol. 42. Wiley Online Library, 137–148.

A Questionnaires

A.1 Initial Privacy Attitudes and Previous Experiences

Table 6: General privacy experiences (reported in Table 2 and in section 4.1) and privacy perceived contexts (reported in Table 3) at pre-intervention phase

Index	Question	Categories	Type	Scale
General privacy experiences	How often do you actively think about who can see your screen when using your phone in a public space?		Scale	1 = Never, 10 = Always
	How often do you do something to cover your screen to feel more comfortable in public spaces?		Scale	1 = Never, 10 = Always
	How often have you chosen to postpone or avoid using your phone due to privacy concerns in a public space?		Scale	1 = Never, 10 = Always
	Do you change the use of your smartphone depending on who is around?		Scale	1 = Never, 10 = Always
	How important is it to you that the information on your phone is only shared with people you choose?		Scale	1 = Not important at all, 10 = Very important
	When you use your phone in social situations, do you tend to feel self-conscious about what is on your screen?		Scale	1 = Never, 10 = Always
	When you use your phone in social situations, do you tend to change how you use your phone depending on who is around you?		Scale	1 = Never, 10 = Always
	Have you previously used a screen filter for privacy in the past?		Single choice	1 = Never in the past, 2 = Once in the past, 3 = Occasionally, 4 = Regularly, 5 = Always
	Have you ever covered your phone's camera?		Single choice	1= Never, 2 = Rarely, 3 = Sometimes, 4 = Often, 5 = Always
Privacy perceived contexts	In a public space, how sensitive do you consider the following information on your screen?	Texts/Calls Banking info Pictures/Videos Social media Study/Work info Notes/Calender Shopping info	Scale	1 = Not sensitive at all, 10 = Very sensitive for each category
	How often do you use your smartphone in the following social/public settings?	Library Lecture hall Common area Street or park Coffee shop Study room Public transport Gym	Scale	1 = Never, 10 = Always for each category
	How comfortable are you using your smartphone in the following settings?	Library Lecture hall Common area Street or park Coffee shop Study room Public transport Gym	Scale	1 = Less comfortable, 10 = Highly comfortable for each category

A.2 Questionnaires asked during pre and post interventions.

Table 7: Common questionnaires at Pre/Post-Intervention (reported in section 4.1 and in section 4.1)

Index	Question	Categories	Type	Scale
Privacy Perception	How concerned are you about unauthorized use of your phone's camera?		Scale	1= Not concerned, 10 = Very concerned
	How worried are you that people around you can see your screen?		Scale	1 = Not worried at all, 10 = Very worried
	How often do you actively think about who can see your screen when using your phone in a public space?		Scale	1 = Never, 10 = Always
	How often have you felt uncomfortable or regretted using your smartphone in a public space due to privacy concerns?		Scale	1 = Never, 10 = Always
	Are there any types of activities or apps you avoid using your phone in public spaces?		Multiple choice	Video calls, Social media, Banking, Online shopping, Dating apps
	In a public space, how sensitive do you consider the following information on your screen?	Texts/Calls Banking info Pictures/Videos Social media Study/Work info Notes/Calender Shopping info	Scale	1 = Not sensitive at all, 10 = Very sensitive for each category
Behavioural Adaptation	How often do you take steps to cover your screen to feel more comfortable in public spaces?		Scale	1 = Never, 10 = Always
	How often have you chosen to postpone or avoid using your phone due to privacy concerns in a public space?		Scale	1 = Never, 10 = Always
	How comfortable are you using your smartphone in the following settings?	Library Lecture hall Common area Street or park Coffee shop Study room Public transport Gym	Scale	1 = Less comfortable, 10 = Highly comfortable for each category

A.3 Continuation of Post-Intervention Questionnaires

(1) How much did you enjoy using the screen filter in general during this period? (Options: 1 = Disliked, 10 = Liked very much) [mean=6, sd=2.7, median=6]
(2) How often did you open/close the camera cover daily during this period? (Options: 1 = Never, 2 = 1-4 times per day, 3 = 5-10 times per day, 4= 11-20 times per day, 5 = More than 20 times per day) [mean=2.8, sd=1.18, median=3]
(3) How much did you enjoy using the camera cover in general during this period? (Options: 1 = Didn't like it at all, 10 = Liked it very much) [mean=4.5, sd=3, median=5]
(4) How did you feel the privacy filter affected the flow of information from your phone to others? (Options: 1 = No impact at all, 10 = Great impact) [removed since "flow of information" was misunderstood by the participants]
(5) Did you find that the privacy tools changed how others reacted to your phone use in public spaces? (Options: 1 = No change at all, 10 = Big change) [removed from the questionnaire and asked during the interview - see question 4 Appendix B.2]
(6) Did the privacy filter make you feel safer when using your phone in public settings? (Options: 1 = Not safer at all, 10 = Very much safer) [mean=5.5, sd=2.7, median=6]
(7) Did the camera cover make you feel safer about the privacy of your smartphone? (Options: 1 = Not at all safer, 10 = Very much safer) [mean=5.3, sd=2.8, median=6]
(8) Will you continue to use these tools in the future? (Options: 1 = Yes, the privacy filter, 2 = Yes, the camera cover, 3 = Yes, both, 4 = No, both, 5 = Not sure) [removed from the questionnaire and asked during the interview - see question 7 Appendix B.2]
(9) What is the main reason for your decision? (Options: 1 = Increased security, 2 = Increased awareness of privacy, 3 = Impractical to use, 4 = Made no real difference, 5 = Other) [removed from the questionnaire and asked during the interview - see question 7 Appendix B.2]

B Interview Questions

B.1 Pre-Intervention Interview Questions

(1) Can you describe a situation where you felt uncomfortable with someone being able to see the screen of your phone? How did you react?
(2) What strategies, if any, do you use to maintain privacy when using your phone in public?
(3) When using your phone in public places, do you tend to choose specific seats (e.g. back against the wall, away from others)? Why or why not?
(4) Are you conscious of who might be looking at your screen when using your phone in a public or social setting?
(5) Have you ever avoided certain activities (eg, reading private messages, checking bank apps) in a social/public setting due to privacy concerns?
(6) How do you feel about people using privacy tools such as screen filters or camera covers?

B.2 Post-Intervention Interview Questions

(1) What was it like for you to use these tools during the period?
(2) Did you notice any changes in how you used your phone in public and/or social settings? If yes, in what way?
(3) Were there situations where you found these tools particularly useful or inconvenient?
(4) How did others react to you using these tools?
(5) Did the tools affect social interactions, for example how often you checked your phone in social situations? If yes, in what way?
(6) To what extent were you self-conscious about using the tools? Did this change over time?
(7) Will you continue to use these tools in the future? Why / why not?