"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

HABIBA FARZAND, University of Bristol, UK
SHAUN MACDONALD, University of Glasgow, UK
KAROLA MARKY, Ruhr University Bochum, Germany
MOHAMED KHAMIS, University of Glasgow, UK

This paper investigates how experiencing shoulder surfing impacts smartphone users: Through an in-depth survey in the UK (N=91), we specifically investigate how shoulder surfing affects (a) the privacy perceptions of victim users and (b) their interactions with smartphones. We found that the impact of being shoulder-surfed is highly individual. First, shoulder surfing is perceived as *unavoidable* and frequently occurring, leading to an increased time to complete tasks. Second, users are concerned about their own and other people's privacy and even consider shoulder surfing a gateway to more serious threats (e.g., identity or device theft). Users are willing to alter their behaviour and use software-based protective measures to prevent shoulder surfing. Finally, we captured a set of user-defined criteria essential to software-based protective measures. Based on our results, we discuss future work directions for user-centred shoulder surfing mitigation.

CCS Concepts: • **Human-centered computing → Ubiquitous and mobile computing**; **Empirical studies in ubiquitous and mobile computing**;

Additional Key Words and Phrases: Shoulder surfing, out-of-device privacy, privacy

ACM Reference Format:
Habiba Farzand, Shaun Macdonald, Karola Marky, and Mohamed Khamis. 2025. *"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. In *24th International Conference on Mobile and Ubiquitous Multimedia (MUM '25), December 01–04, 2025, Enna, Italy*. ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/3771882.3771900

1 Introduction

Everyday life scenarios – like using a smartphone on a bus to check timetables or messages – are susceptible to shoulder surfing (cf. [21, 22, 24–26]). In such scenarios, a person observes information displayed on the smartphone either by direct sight or a camera. Consequently, shoulder surfing can lead to invasions of the users' privacy, potentially resulting in uncomfortable feelings between the users and the shoulder surfers [21]. It has also been shown that shoulder surfing could impact users personally or professionally [28]. For example, a senior UK civil servant lost their position because someone photographed their laptop screen [17]. Furthermore, confidential details of US customers of a Bank of America branch office in St. Petersburg were visible to passersby outside the office [28]. In the firm Ernst & Young, a call centre accidentally provided screenshots of internal systems to fraudsters [28]. These examples illustrate the potential consequences of shoulder surfing.

Authors' Contact Information: Habiba Farzand, habiba.farzand@bristol.ac.uk, University of Bristol, Bristol, UK; Shaun Macdonald, University of Glasgow, Glasgow, UK, shaun.macdonals@glasgow.ac.uk; Karola Marky, Ruhr University Bochum, Bochum, Germany, karola.marky@rub.de; Mohamed Khamis, University of Glasgow, Glasgow, UK, mohamed.khamis@glasgow.ac.uk.

© 2025 Copyright held by the owner/author(s).
Manuscript submitted to ACM

Research on shoulder surfing has provided in-depth insights into the anatomy of shoulder surfing, revealing how, when, and where it can happen using multiple methods such as surveys [21, 24, 31, 42], diary studies [25], interviews [23], focus groups [56] and even virtual reality simulations [2, 3]. It has also been shown that users respond to shoulder surfing by physically manipulating their devices (e.g., by tilting [36], turning them off [21]), or using a privacy screen [48]. HCI researchers have proposed various software-based mechanisms to combat shoulder surfing, such as alerting the user using icons [53], implementing overlay filters [35], grayscaling [64], lowering screen brightness [53], or gaze-based mechanisms that limit the observer's view [12].

This paper continues this line of research by exploring the impact of shoulder surfing on the daily lives of victims and their interactions with smartphones, specifically investigating the following research questions:

RQ$_1$: How does experiencing shoulder surfing impact the perception of shoulder surfing victims towards protecting their personal information, situational awareness, and willingness to adopt protective mechanisms?
RQ$_2$: How does shoulder surfing impact victims' social interactions with others and willingness to use smartphones?

To address these research questions, we conducted an in-depth qualitative survey of 91 individuals who had experienced smartphone-based shoulder surfing in the UK. We collected their experiences of how shoulder surfing has impacted their social interactions and device use. We further asked participants about their current knowledge of protection against shoulder surfing and their future willingness to use such measures.

Participants held diverse perspectives on the impact of shoulder surfing. On the one hand, shoulder surfing was seen as unavoidable and omnipresent, and participants could not always avoid using their smartphones in settings where they had previously been shoulder-surfed, as smartphones were essential to their daily lives (e.g., public transportation or workspaces). A few participants expressed that being shoulder-surfed by children could potentially harm the child. On the other hand, our results indicate that shoulder surfing increased participants' situational awareness, causing them to monitor changes in their surroundings. Overall, the main concern about shoulder surfing was privacy, particularly the privacy of others whose data is visible while they are being shoulder-surfed. These concerns led participants to adopt available privacy tools, such as screen protectors that prevent viewing from certain angles. Additional mechanisms were perceived to provide participants with a sense of security. However, their adoption depended on factors such as the level of interruption during interaction, the mechanism's financial cost, effectiveness, and ease of use. Finally, shoulder surfing was seen as a gateway to more serious attacks, such as stalking, unauthorised access, identity theft, device theft, or blackmail.

Our participants had no formal training or education on protecting themselves from shoulder surfing, hence they shared measures that they had been practising for protection. Some participants, however, considered shoulder surfing harmless, considering additional protection mechanisms unnecessary. This perception was primarily held by a subset of participants who had fewer shoulder-surfing incidents and generally avoided accessing sensitive information in public. To this end, we make the following contributions:

Research Contribution.

(1) We present in-depth insights into the impact of everyday life shoulder surfing on the social interactions and device use of victims of shoulder surfing, explaining *why* and *how* shoulder surfing impacts users,

(2) Our research bridges the gap between investigations of shoulder surfing in the wild and the need for privacy protection methods. We discuss and provide recommendations to address the challenges in mitigating the negative impact of shoulder surfing on diverse users, including vulnerable user groups such as children.

2 Background

2.1 The Prevalence of Shoulder Surfing

Shoulder surfing — observing someone's device screen without permission — occurs unintentionally or intentionally and happens most frequently on smartphones [21]. A study by Marques et al. [43] presents evidence that people who own a smartphone are more likely to engage in shoulder surfing others. Shoulder surfing, sometimes also referred to as "snooping on other people's phones", has been reported to be done by 1 in every 5 adults in the US and is most prevalent among young users [43]. Prior work around shoulder surfing can be grouped under investigations around content being shoulder surfed and investigations around shoulder surfers, which is summarised below.

Shoulder surfing can reveal two categories of information: (1) security-critical information (e.g., PINs or passwords) and (2) user content (e.g., text or photos). Most prior research has focused on security-critical information [5, 13, 19, 30, 59] and proposed multiple mitigation mechanisms like fingerprint [7] or EOG-based authentication [51]. However, protection against content-based shoulder surfing is critical, as it violates the user's privacy and can leak personal information. It has been shown that user content is more frequently shoulder surfed in comparison to security-critical information, which makes addressing content-based shoulder surfing more urgent [21, 25].

Among the shoulder-surfed content, text, photos, and games are the most shoulder-surfed content [21, 25]. Within the text category, messages are most frequently reported, followed by social media, email, and news. Saad et al. [54] compared four apps of varied content types, including Facebook, WhatsApp, games, and photo galleries. Following authentication, WhatsApp was most frequently observed, while the photo gallery was the second most frequently observed. In the same line of research, Abdrabou et al. [3] reported that games and videos are more often shoulder-surfed in comparison to text.

Shoulder surfing requires only being in close proximity to the user, making it highly "accessible" for anyone [22]. Shoulder surfing is not just done by outsiders (such as strangers); anyone can do it. Prior work presents a list of user-observer relationships that have either shoulder-surfed someone or been observed. The user-observer relationship spectrum includes strangers, acquaintances, friends, colleagues, family members, and partners [21, 23, 25]. Similar to the variety in user-observer relationships, shoulder surfing can happen anywhere, including in public (e.g., workspace, educational institutes, restaurants) and private environments (e.g., at home) [21, 23, 25, 32]. Despite the broad list of locations, public transport is one of the most frequently observed locations, and strangers are the most common type of user-observer relationship [21]. The threat of shoulder surfing is also globally recognized [33], showing the need to investigate how shoulder surfing affects users' social interactions and device use, which motivates our study's focus.

2.2 Users Responses to Privacy Violations & Shoulder Surfing

One of the main risks of privacy violations is the leakage of personal data, especially Personally Identifiable Information (PII), a significant concern among users [40]. To safeguard PII, users hold their belongings close to them or restrict access, especially for electronic devices, by using authentication systems, such as biometrics or pattern locks [7, 40]. Users even reported using outdated mobile phones to protect their devices from device theft [40] or not storing financial information, such as credit card data, on their devices [40].

Users adopt several measures to protect their information from shoulder surfing, like putting the device down, turning it off, covering the screen with their hands [21, 23, 25] or responding with an angry look or a conversation [21]. Users also reported using a privacy screen that hides content from certain angles [23] or tilting of the device [37].

Shoulder surfing has led to negative feelings between users and observers, such as uneasiness, embarrassment, harassment, anger, and spying [21]. Cross-cultural examinations have provided evidence that shoulder surfing can have more serious negative consequences for low socio-economic groups in comparison to high socio-economic groups due to the exaggerated fears of one's own privacy and fragile trust among users [55].

Research Gap

In sum, prior work has explored users' responses to shoulder surfing by capturing real-world stories [21, 25]; however, it provides limited insight into how users' responses affect their perception of protecting information from shoulder surfing and how this impacts their device and social interactions. As evident from related work, users employ various strategies to mitigate and combat shoulder surfing. However, the emotional and behavioural responses reveal deeper concerns about its impact on daily device interactions. Thus, understanding how these emotional and behavioural responses affect user behaviour is important for developing effective mitigation strategies. Related work investigated shoulder surfing, focusing on the context (e.g., location), the user-observer relationship, or users' responses. This paper specifically considers the overall impact of having experienced shoulder surfing on the users' smartphone routines. Furthermore, we capture the origin of the users' mitigation strategies in capturing whether these are intuitive or by training.

3 Method

To capture the impact of shoulder surfing, we conducted an online survey study as we aimed to collect data from a diverse pool of users in terms of gender and professional status.

3.1 Questionnaire Design

To answer our research questions, we specifically formulated questionnaire items that focused on social interactions, device interaction and task completion. Along with open-ended questions, Likert items capturing the users' agreement or disagreement were also included. We used Qualtrics - an online survey builder platform, to build the survey questionnaire [50] and recruited participants via Prolific [49]. The questionnaire is appended in Appendix A.

3.2 Study Procedure

Stage 1: Screening Survey: First, we conducted a shortlisting study on Prolific (N = 180) and asked participants if they had experienced shoulder surfing on smartphones as a victim. Participants were presented with the definition of shoulder surfing to help them understand the term. Participants who responded as being victims of shoulder surfing were invited for Stage 2 of the study.

Stage 2: Main Study: The study procedure of our online survey study was as follows:

(1) **Step 1: Information & Consent:** Participants were welcomed and explained the aim of the study, i.e. to capture their experiences and concerns about shoulder surfing on smartphones. Participants were then presented with the consent form and asked to accept it.

(2) **Step 2: Setting the Scene:** Next, we presented participants with the definition of shoulder surfing and asked them to recall their most recent experience of shoulder surfing on a smartphone as a victim.
(3) **Step 3: Eliciting Details:** In this part, we asked participants about the impact of shoulder surfing using Likert items, followed by an explanation of the rating. To answer RQ1, we asked questions about concerns arising from shoulder surfing, their personal privacy perceptions, opinions on breaching the trust of their friend whose content was seen by the shoulder surfer, and their willingness to use protective measures. To answer RQ2, we asked questions about the impact on device interaction, focusing on disruptions during device interaction and on using the device in the same setting as the shoulder surfer. Finally, we asked whether participants had received any training or education on safeguarding against shoulder surfing.
(4) **Step 4: Demographics:** We concluded the survey by collecting demographic information on age, gender, and employment status, and then redirected participants to the recruitment platform for reimbursement.

3.3 Pilot Testing

We pilot-tested our questionnaire with two researchers from Usable Security and Privacy at our institute, and based on their feedback, we refined the wording of the questions to improve their clarity. This helped ensure that the formulated questions were easily understandable and adequately answered the research questions.

3.4 Recruitment & Participants

The Ethics Committee at our institution approved the study. 100 participants residing in the UK completed the questionnaire. We used completion time as a measure of participants' attentiveness, similar to prior work (cf. [20]). The participants took an average of 11.34 minutes (std = 7.39). For our analysis, we excluded the data of 8 participants, as they completed the questionnaire in less than half the average time. To assess the participants' attentiveness and understanding of the study's goal, we asked them to describe their most recent experience of shoulder surfing. We further removed the data of one participant, as they had responded from the perspective of observers.

The final sample included N=91 participants. 47.25% self-identified as male, and 52.74% self-identified as female. Participants aged between 22 and 73 years (mean=38.23, std =10.15). Most participants (65.93%) were employed full-time, 24.17% employed part-time, 3.30% students, 3.30% homemakers, 2.20% unemployed and 1.10% retired. Participants from both study stages were compensated at £17.14 per hour for the first stage and £11.59 per hour for the second stage.

3.5 Data Analysis

Two usable security and privacy researchers, with expertise in qualitative data analysis, analysed the survey responses using a thematic analysis approach [10, 11]. First, one researcher familiarised themselves with the data and applied open coding across the full dataset to propose a codebook. The second researcher independently coded a subset of the data (25%), resulting in a second codebook. Both researchers then discussed the codes, and any coding disagreements were resolved in a meeting, resulting in a unified codebook applied to the dataset. This helped in verifying the coding through discussion. After this, the codes were grouped into categories until no meaningful grouping was possible through discussions between the two researchers [44]. Following the guidelines of previous work [9, 45, 62], we refrain from reporting inter-rater reliability to support a qualitative coding approach based on discussion and merging of results. We present the results based on the categories derived. To give the reader an impression on how often a particular topic came up, we use the guidelines presented in Figure 1. However, we do not quantify the frequency of the reported codes, and therefore, it should not be considered a quantitative analysis. Prior research has provided evidence that shoulder

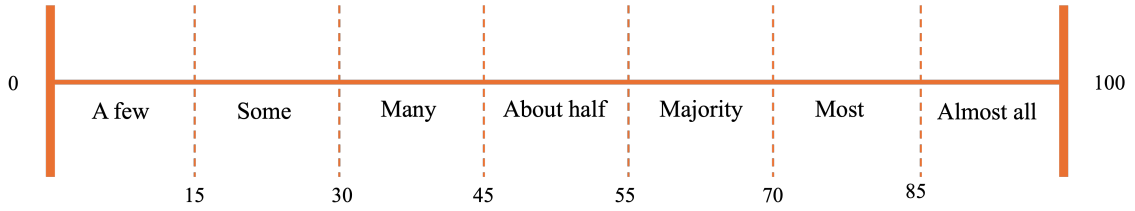

Fig. 1. The overview of the qualifiers and respective frequencies of codes throughout our results. All occurrences of the respective qualifiers always refer to the same portion of the number of times codes are used.

surfing impacts victim users differently based on their cultural ecosystem [55]. In line with this research, we specifically focus on the users in the UK. Drawing comparisons based on gender, age, education, or geographical location is out of the scope of this paper.

4 Findings

Participants were presented with five Likert-style questions around shoulder surfing to which they were asked to indicate their degree of agreement or disagreement (1 = strongly disagree, 5 = strongly agree) (as shown in Figure 2). Participants tended to disagree that they are shoulder surfed almost daily (mean=2.36, st dev=1.12, median=2). Participants leaned towards agreement that they would continue using the smartphone and accessing information in the same setting where they were shoulder-surfed (mean=3.63, st dev=1.31, median=4) and that shoulder surfing impacted their perceptions of privacy (mean=3.58, st dev=1.05, median=4). Participants agreed that if someone sees their friend's content on their screen (e.g., a picture or message from of their friend), it feels like a breach of their friend's trust in them to keep their content private (mean=3.40, st dev=1.15, median=4). Similarly, participants also felt that experiencing shoulder surfing prevented them or slowed them down from what they wanted to do on the device (mean=3.40, st dev=1.26, median=4) and expressed a preference for using additional protection mechanisms against shoulder surfing (mean=3.67, st dev=1.02, median=4). However, mixed views were found on whether shoulder surfing positively impacted their interaction with the device (mean=2.07, st dev=1.08, median=2) or negatively (mean=2.85, st dev=1.23, median=3). Below, we report the results of our study, grouped by the categories identified in the analysis.

4.1 Privacy

Almost all participants mentioned shoulder surfing as a privacy invasion that makes them highly concerned, "*I was already pretty aware that we now live in a society with significantly less privacy that we used to enjoy*" (P22).

Many participants perceived it as a negative experience, and about half were also concerned about the privacy of others whose content was observed on their device by shoulder surfers, such as private photos or messages. This was seen as letting the other person down, as the message was sent only for the intended recipient. The observed information could only be interpreted correctly by sender and receiver, but appeared inappropriate to any other person, "*I may have been sent something inappropriate for others but a private joke between me and my friend.*" (P12). Participants expressed to expect their friends to keep their content safe. If they cannot do so, it breaches privacy and trust as it is seen as worse than the invasion of one's own privacy, (P19: *"I would keep my friends and family privacy to be safe. They are my most dear relations and I want to keep their information safe. They have immense trust on me and i want to think of their safety first."*). To counteract this risk, some participants only access content in a location where only they can see it.

The loss of privacy resulted in various negative emotional responses for many participants, including discomfort, disrespect, untrustworthiness, and annoyance. Participants felt uncomfortable continuing to use their devices and worried about accessing them in the shoulder-surfing environment. Participants also felt that it was unethical or rude to look at someone's device without permission, "*It's risky as it doesn't gives privacy. It's quite uncomfortable and unacceptable behaviour. It takes away peace of mind as there is no privacy.*" (P19). Some participants mentioned that they became concerned about their personal information after experiencing shoulder surfing. They felt a loss of agency in using their devices, and shoulder surfing slowed their interaction down. Participants felt more cautious, distracted, and unsafe when using their devices in public. Shoulder surfing was perceived as a threat to personal information by many participants, and many participants mentioned considering using a privacy screen as they value their privacy highly, "*I am looking into applying a privacy screen on my phone*" (P7). They also mentioned to prefer having additional mechanisms just to protect their privacy.

4.2 Contextual Privacy

Contextual privacy, referring to privacy that depends on contextual factors such as location, shoulder-surfed information, and the like, was mentioned by many participants [47]. They mentioned using the device in the same setting as shoulder surfed, but with alterations such as switching to "*...safer apps like music instead of messenger...*" (P4). Participants ensured they did not access any sensitive information, such as banking apps, and switched to other non-sensitive apps or scrolled quickly through controversial posts and news stories. Similarly, the level of concern participants felt for the privacy of those they were messaging was context dependent, as illustrated by P20: "*...the situation, the type of discussion, lots of factors need to take into consideration...*". For example, participants were not concerned if the shoulder-surfed information was social media posts, but "*...a private message would be more serious..*" (P33). Participants also mentioned that they do not access private and sensitive information in public, and as a result, shoulder surfing of non-sensitive information is not a concern for them. They also mentioned that they would be open to additional protection mechanisms if shoulder surfing becomes a significant issue, and this would depend on the environment and their level of concern when others view their screens without permission.

Participants mentioned location-specific and information-specific privacy needs. A few participants emphasised the need for location-specific protection, particularly in public settings like public transportation, while many others highlighted the importance of information-specific privacy, including concerns about shoulder surfing of sensitive information, such as banking details, biographical data, and private messages. Personal photos, medical information, passwords, and contact information were among the types of information that made participants concerned about shoulder surfing. Even among the named categories of information, participants mentioned specific information that made them highly concerned about shoulder surfing, such as "*....I'd be concerned someone could see how much money is in my account*" (P10). The different categories of information and the precise information within each category indicate users' preference for contextual and content-specific privacy.

4.3 Perceived Situational Awareness

Most participants mentioned that experiencing shoulder surfing raised their awareness about their surroundings. They wanted to check their surroundings before engaging in a task that required accessing sensitive information and know who was around them. The experience of shoulder surfing was like a lesson and, therefore, the impact of shoulder surfing was perceived as positive. The lessons from shoulder surfing taught them about awareness of their surroundings and device use, including who was watching them, what they could be sharing unintentionally, and what notifications

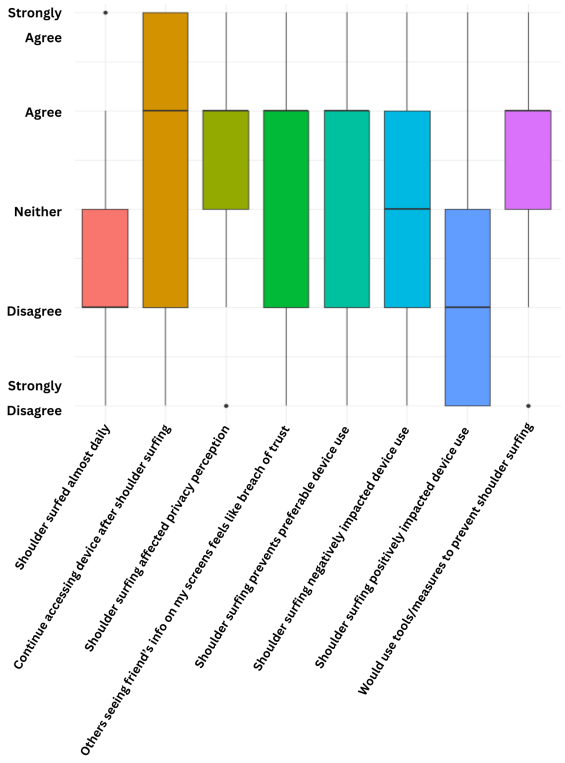

Fig. 2. Responses of participants to the questions centred around the impact of shoulder surfing.

they wanted to appear on their phones. The realisation of shoulder surfing prompted participants to stay more alert and to quickly complete their tasks; it made them cautious, careful, and thoughtful about accessing specific apps that could contain sensitive information. Participants felt that they were now more aware of where to sit in public transport or to be more cautious about their general surroundings. "*....ill just be more vigilant to my surroundings.*" (P18).

Shoulder surfing prompted a few participants to reconsider accessing sensitive information in public, such as banking details. Furthermore, some participants mentioned that because shoulder surfing made them aware of their surroundings, it interrupted their interaction with the device. "*It made me stop what I was doing and therefore stop my funny conversation with my friend and instead turn my trip into an angry one. However, it has made me more aware that this happens*" (P3). Shoulder surfing made participants "*... stop messaging my friend at the time to wait until people had passed by*" (P4), which aroused feelings of anger, frustration and annoyance. Shoulder surfing also restricted the use of smartphones, for example, "*.... log into my bank app to make a transaction while i am being shoulder surfed*" (P5). Shoulder surfing prompted participants to discontinue device use, wait until the situation passed, switch to non-sensitive applications, or perform tasks more discreetly.

Experiencing shoulder surfing made a few participants rethink their device interaction, such as they "*..may not want to do this anymore in the same setting.*" (P1). Participants held the opinion that shoulder surfing should not stop them from continuing to use their devices, especially because they are not doing anything illegal, while others thought about

changing the way they use their devices, "*I don't do anything illegal or unsavoury so i am happy to continue using it...*" (P50). One of the participants mentioned always carrying a book with them, which meant they did not always have to look at their devices.

After experiencing shoulder surfing, many participants perceived it as a ubiquitous threat "*It makes me realise that just because you think people aren't bothered or interested enough to care about what you're viewing, there will be and you don't know where or when*" (P2). Participants were aware that their screen was visible to others: "*it seemed like a lot of people were doing it*" (P4) and some expressed surprise at being shoulder surfed "*Well you'd like to think that other people aren't interested in what one's doing on a phone but clearly they are. And one has to be aware that some are up to no-good*" (P13). As a result of this new awareness, participants felt that "*privacy is definitely compromised*" (P70) because of shoulder surfing and "*What you think is private is no longer*" (P14). Some participants felt shoulder surfing was unavoidable because they were either shoulder surfed by a family member, such as their partner or were shoulder surfed in a work environment (such as an office) or a pub where they did not have much choice in changing their location.

4.4 Protective Measures

A few participants mentioned that shoulder surfing made them more careful around their surroundings, which has equipped them with protective measures:"*Following incidents like this, I am much more conscious of what information I view on my phone in busy environments. I no longer access personal, private information.*" (P27). The majority of participants adjusted their behaviour in the setting where they were shoulder surfed. For example, they changed their seating location on the bus and preferred to avoid easy sightlines to the seats behind them. Furthermore, they restricted access to apps that contain sensitive information in three ways: (1) shifted to using non-sensitive apps, such as a music player, (2) put the phone away, or (3) waited to get out of that setting and then accessed their phones "*...when I am at work I will use my phone in the bathroom so nobody can see my screen*" (P39). Participants also took steps to protect their privacy, such as repositioning themselves, readjusting their phone at work, discontinuing its use, or reducing the screen brightness. One of the participants applied a privacy screen - a screen protector that obstructs the view from certain angles - to help against shoulder surfing. Participants considered repositioning themselves or their phones or looking for a less busy location. Locking the screen upon realising shoulder surfing was also mentioned by participants as a way to protect their information.

As discussed above, some participants opted for selective information access, such as not accessing sensitive apps or scrolling quickly and switching to non-sensitive apps. On the other hand, a few participants avoided using their devices as a way to protect themselves from shoulder surfing. Participants could not avoid using smartphones in the shoulder-surfed settings, but they took action to protect their privacy.

Participants were asked to report if they knew of any technology or security feature that helps mitigate shoulder surfing. About half of the participants were not aware of any technology; many mentioned a privacy screen, and a few mentioned turning off the device, lowering screen brightness, changing the font size of the device, using automatic screen lock, and using a fingerprint scanner. A few participants specifically mentioned banking apps where the user has to long-press a button to reveal the PIN code, which is not visible otherwise. Almost all participants stated that they had not received any education or training on protecting their data from shoulder surfing. A few mentioned sitting beside a wall to avoid being observed, using selective access to apps in public, and learning about shoulder surfing and how to protect against it online. A few participants expressed a preference for using additional mechanisms to protect their privacy and to prevent such issues; however, they were not willing to go out of their way to obtain them. A few

participants voiced that they are currently not aware of any protection mechanisms, but they would like to be aware "*Not aware or thought of any additional privacy methods other than putting a shield around my head*" (P94). Participants preferred additional protection measures for application-specific use only, such as online banking apps. Further, ease of use, invasiveness, reliability, effectiveness, and functionality were cited by a few participants as key conditions for using a protection mechanism against shoulder surfing. The financial cost of the mechanism was also reported by a few participants as a factor they would consider before opting for a mechanism (P39: *"I value my privacy very highly it would depend on what those measures were and if they cost/how much they cost"*).

4.5 Worries Over the Consequences of Shoulder Surfing

Shoulder surfing was seen as leading to not only privacy and safety threats but also as a threat to negatively impact interpersonal relationships and the self-image of users. A few participants mentioned identity theft, data insecurity, information theft, other people's privacy, revealing of inappropriate content, invasion of personal space, misuse of personal information, risk of a potential stalker, unauthorised access and blackmail (P22: *"loss of data that could lead to theft/hacking/identity theft etc"*). A few participants also raised concerns about shoulder surfing by children, with participants reporting that they had to stop interacting with their devices to prevent it ("*My child was reading my messages over my shoulder as I was typing them to a friend. I told him it's rude to and he pretended to look away but I could see he was still watching me*" (P44)). A few participants expressed concern about suffering social judgment or stigma as a result of the content seen on their device. They felt that someone might judge them or form the wrong impression based on the content others see on their devices, which could lead to embarrassment. Participants felt that if a shoulder surfer reads a message related to them, it could result in social awkwardness. Participants also shared that experiencing shoulder surfing made them think that the shoulder surfer did not trust the participant and therefore had to discreetly shoulder surf them, "*...I feel like even though i have nothing to hide it feels like there is a lack of trust towards me.*" (P88). Such situations were seen as bringing threats to the relationship between the user and the bystander, which could be particularly harmful if the bystander is a coworker, friend or family member, "*...a friend/relative getting the wrong impression of me*" (P82) and "*offending someone- maybe i said something about someone and if i am with them they might see*" (P20).

4.6 Shoulder Surfing as Inconsequential

Despite the varied negative impacts and concerns raised, shoulder surfing was, in the end, seen as inconsequential by about half of the participants, and they continued using their devices in their respective situations. This was primarily because they were either shoulder surfed by a known person (such as a family member) or they felt they had nothing to hide. Participants also mentioned that they have to rely on interacting with their device when travelling on public transport, and therefore, they continued using the device. Participants also said that they do not access sensitive information in public and only access non-sensitive information, such as watching videos, which makes them unconcerned about shoulder surfing.

Shoulder surfing was a frustrating experience, but participants made arrangements and were able to overcome it quickly, "*as I've already said It is frustrating how limiting it can be but is also something I already make adjustment for*" (P22). Efforts included putting the phone away and similar. More than the experience itself, participants were focused on the bystander. One example of shoulder surfing being perceived as harmless involved participants communicating with a bystander about the content being observed, for example, the score of a sports match. Participants mentioned that the negative impact was often a short-lived experience that was easily forgotten. For some, the experience of being

shoulder surfed was even viewed as positive, as it forced participants to put their phones down, which they considered a positive outcome, (P44: *"It was probably a good thing that I put my phone down. I don't need to constantly be looking at it."*).

Some participants viewed shoulder surfing from a purely practical perspective and did not consider it problematic. They held the opinion that they are "*... aware of the limitations of privacy when I am somewhere like the tube. I wouldn't expect to access any information I want to keep private and mainly keep to stuff like games*" (P79). Moreover, many participants perceived that shoulder surfing did not significantly impact their privacy perceptions, as it is not a surprising occurrence and happens frequently, making it unavoidable. Participants perceived it to be harmless and marked people as generally "nosy".

Many participants did not consider shoulder surfing a breach of trust in protecting the content being viewed on their device, so long as they believed it was unintentional and not their fault, "*it isn't a breach of trust because it's not been done intentionally*" (P10). The observer invaded participants' personal space without their consent; therefore, participants did not perceive the incident as a breach of trust. They voiced that they can not have complete control over their surrounding environment, but can expect other people to respect their privacy. Some participants were seen as less concerned about other people's privacy. This was due to multiple reasons, including the fact that the bystander did not know the participants' friends, and therefore it made no difference whether the bystander viewed information. Since participants' friends were unknown to the shoulder surfer, they felt there were no real consequences associated with viewing their friends' content without permission. Participants took a pragmatic view that if anything is posted online, having it viewed by the public is an expected possibility and thus anything important or private should not be posted online. They also voiced that a passing glimpse is unavoidable, and their friends should understand this. Participants regarded shoulder surfing as a minor breach which happens all the time, (P84: *"It is a small breach but it happens all the time"*). Since shoulder surfing was not perceived as a concern by these participants, they also considered protective measures unnecessary. This was because they avoided accessing personal information in public settings or did not have anything to hide, and therefore did not feel the need to have additional protection mechanisms, "*I don't think it's all that necessary for me, as I don't open sensitive info on the tube next to people*" (P11). Instead, situational awareness and common sense were referred to as ways to prevent shoulder surfing.

5 Discussion & Directions for Future Work

5.1 RQ_1: How does experiencing shoulder surfing impact the perception of shoulder surfing victims towards protecting their personal information, situational awareness, and willingness to adopt protective mechanisms?

The results show that users hold diverse perspectives on shoulder surfing that can be grouped into three categories: (1) privacy-concerned individuals, (2) contextual-privacy seekers, and (3) unconcerned yet careful users. Privacy-concerned individuals regarded shoulder surfing as an invasion of their personal space and perceived it as a threat to their and other people's privacy, whose content was seen by the bystanders. They believed they had violated the trust of their friends or family members, whose content was observed by bystanders, as it was their responsibility to keep it private. A few participants were seen concerned for the safety of bystanders, such as children, in case they observe things they do not understand. Participants regarded shoulder surfing as not just casual screen observation, but were concerned about the outcomes of shoulder surfing, which might lead to social awkwardness or to even more serious threats to safety and privacy, such as identity theft, stalking, and blackmail. The contextual-privacy seekers valued their privacy against

shoulder surfing, but the extent of this value depended on the information being viewed and by whom. Similar to the contextual need for privacy, they preferred protection mechanisms depending on the context. The unconcerned yet cautious group of users did not perceive shoulder surfing as a concern, as they only accessed non-sensitive information in public. Users also believe that since they have nothing to hide, being shoulder-surfed by anyone does not warrant any harm. Therefore, they marked protection mechanisms as unnecessary. The varied perspectives of users provide evidence for personalised mechanisms.

Answer to RQ$_1$ Shoulder surfing is a privacy concern for users, affecting not only their personal privacy but also the privacy of others. Users can be classified as (1) privacy-concerned individuals, (2) contextual-privacy seekers, and (3) unconcerned yet careful users. The varied level of perceived need for privacy highlights the need for personalised protection mechanisms. Users are willing to opt for additional mechanisms, but their decision depends on factors such as reliability, efficiency, functionality, and financial cost.

5.2 RQ$_2$: How does shoulder surfing impact victims' social interactions with others and willingness to use smartphones?

Due to shoulder surfing, participants had to either switch off their devices, switch to non-sensitive applications, or wait until they were out of the shoulder surfing situation to protect the leakage of personal information. While such efforts might have resulted in the protection of users' personal information, they also hindered their interaction with the devices and may have taken longer to complete the tasks they were performing on them. The threat of shoulder surfing leads to the selective use of applications in high-risk situations, resulting in reduced freedom to use devices. Participants were also concerned about what others would think about them after observing their device screens, which may make them reluctant to use their devices in the presence of others. On the other hand, having protection mechanisms against shoulder surfing could potentially increase the agency of these users by removing restrictions on their interaction.

Answer to RQ$_2$ Shoulder surfing makes users more reluctant and selective in their smartphone use. Users opt for various privacy techniques, such as scrolling quickly and switching to non-sensitive apps, to protect their privacy. While such techniques may help the user for the time being, they cannot be considered effective, efficient, or useful in all potential shoulder surfing settings, as shoulder surfing often goes unnoticed.

5.3 Shoulder Surfing as the Stepping Stone to Other Serious Threats

Shoulder surfing is not just about observing someone's device screen but also about giving the observer the opportunity to misuse the information in any possible way. In our study, participants were concerned about shoulder surfing leading to other threats such as identity or device theft [65], potential stalking or blackmailing. Another study focused on collecting shoulder-surfing experiences reported a story from a participant who expressed concerns about being followed by a bystander who had looked at her Google Maps address [21]. This suggests genuine concern about shoulder surfing, which poses a significant threat. However, given the limited evidence, future work should investigate whether these concerns are valid.

Future Research Direction: To what extent is shoulder surfing responsible for leading to other threats like device or identity theft?

5.4 Shoulder Surfing by Children Puts Them at Risk

One of the novel concerns raised in the study is that when children shoulder surf, they may encounter something inappropriate that they do not fully understand, which puts them at risk and further pressures users not to view age-inappropriate content, thereby impeding their interaction possibilities. Shoulder surfing by children is concerning as it could negatively impact children's perspectives, views, or behaviour. Furthermore, children may attempt to shoulder-surf authentication credentials, such as PINs, to gain access to their parents' devices. Observing such information can not only give unauthorised access to their parents' devices, but they could also share it with others either involuntarily or through social engineering or exploitation, which would bring even more harm to the parties involved. When children have access to their parents' devices, they can be manipulated into accessing and sharing sensitive information with others. A series of negative events occurring one after another can be seen as a consequence of children's shoulder-surfing.

Previous work has explored safeguarding children from the harms of technology, focusing on various aspects, such as risks involved in the adoption of online services [60], privacy and security challenges with educational technologies [16], children's AI systems [61], parental concerns around social Virtual Reality [27] and much more. However, shoulder surfing is another concern associated with the use of technology for children, which has not yet been investigated. One way to mitigate shoulder surfing by children is to use gaze data to detect the observer's age, as recent research shows that age can be inferred from eye movements [39]. This appears to be a promising direction to protect children from unwanted device observations. It is worth noting that this approach presents the challenge of safeguarding bystanders' privacy [34]. Therefore, an approach to detect bystanders' ages without compromising their privacy should be explored and evaluated.

Future Research Direction: How can we safeguard children from the potential harms of shoulder surfing as a bystander?

5.5 Self-Equipping Users for Protection Against Shoulder Surfing

In our study, participants reported having no training or education on protecting their information from shoulder surfing. This finding is consistent with many related studies, in which participants reported receiving no training or education on protecting their visual privacy. For example, a white paper on visual data security found that 98% of respondents reported having no knowledge or training in protecting their visual privacy. This white paper was published in 2012, and our study conducted in 2024 provides the same results. This indicates a persistent trend of inadequate education and training on protecting users' privacy. Related work on educating users has shown promising results, enabling users to be more aware and informed about privacy practices. For example, Khan et al. [38] evaluated the course outcome of privacy threats related to tracking and Pervasive Personalisation in school classrooms, and the results showed that students developed transferable knowledge of the privacy implications. Similarly, Smith et al. [57] tested the efficacy of short videos for educating users about targeted advertising on Facebook and showed that videos significantly increased user engagement with Facebook advertising preferences. Albayram et al. [4] found that videos conveying risk communication and self-efficacy impact people's intention to use multi-factor authentication. In line with this research, a plethora of other studies focus on educating users through educational video interventions to promote secure behavior [8, 18]. Considering the workaround the success of training and educating users on various security and privacy issues, training users on shoulder surfing appears to be a promising solution to help mitigate the risk. It will be interesting to explore how training through various forms, such as posters on public transportation,

training videos, and similar methods, can help protect the privacy of users from shoulder surfing.

Future Research Direction: How can training and education on shoulder surfing equip users to safeguard their privacy against shoulder surfing?

5.6 User Awareness Alone Won't Prevent Shoulder Surfing Risks

Participants frequently mentioned increased awareness of their surroundings in various instances. Participants paid more attention to their surroundings and the information they accessed on their smartphones. User awareness appears to be a promising solution to mitigate shoulder surfing, as it empowers users to decide when protection is needed and when it is not. Prior work also suggests user awareness as the solution for a range of other threats that exist in the surroundings of the user as well, such as charging attacks, reflection-based attacks or smudge attacks [15, 46, 52, 63]. However, relying on user awareness may still not be a viable solution for several reasons, including that shoulder surfing often goes unnoticed due to the cognitive load induced by the task the user is performing [29]. The constant awareness of one's surroundings can also negatively impact people's ability to make free choices about what to do on their devices. Constantly looking out for surroundings may lead to user frustration and fatigue. More importantly, shoulder surfing is not the only threat that exploits user unawareness for privacy invasion; there exist many other threats that could be performed by exploiting the unawareness of users, such as reflection-based attacks [52], smudge attack [15] or thermal attacks [1, 6]. Considering the limitations of relying on users' awareness of their surroundings, it cannot be used to solve multiple attacks. Reliance on consistent, secure user behaviour has been criticised in prior work as an unreliable solution for mitigating threats [22, 41]. This instead motivates viable solutions that can be relied upon without the assumption of constant user awareness.

Future Research Direction: How can users be offered effective protection against shoulder surfing without relying on their awareness of the changes in the surroundings?

5.7 Limitations

The participants were located in the UK, a Western country, where shoulder surfing is reported to have less severe consequences than in Eastern countries [55]. This might have impacted participants' responses and opinions on shoulder surfing. Since shoulder surfing poses a global threat that transcends cultural boundaries, we suggest that future work replicate this study across cultures to gain a more comprehensive understanding. In our study, participants relied on their memory. This may have introduced recall bias as participants may not accurately remember the details, which is a natural trade-off of capturing a large sample via survey [58]. Accordingly, more ecological studies focusing on in-the-wild investigations should aim to verify the results reported in the paper. Lastly, we recruited participants from an online platform where users self-nominated to participate; we found our sample was balanced in terms of gender and employment status, with a majority employed full-time and a few in student status. This distribution of demographics addresses the limitations of many studies, which often consist of samples mainly comprised of students [14, 21].

6 Conclusion

In this paper, we investigated the aftermath of shoulder surfing with N=91 participants who had experienced the threat. Our results show that shoulder surfing poses a significant privacy risk, violating the privacy of both the user and others when data is being observed. Shoulder surfing was perceived as a privacy threat that could escalate to more

serious threats, such as identity theft or device theft. We also found that users received no training or education on protecting their data from shoulder surfing or other forms of protection. Participants held diverse perspectives on shoulder surfing that can be grouped into three categories: (1) privacy-concerned individuals, (2) contextual-privacy seekers, and (3) unconcerned yet careful users. This categorisation affects participants' preferences and choices of protection mechanisms against shoulder surfing. This work motivates the investigation and mitigation of everyday-life shoulder surfing through a user-centred design approach. It further paves the way for exploring the consequences of shoulder surfing with specific user groups, leading to more ethical and safer technology use.

Acknowledgments

We thank all participants of our study. This work was co-funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972. Professor Khamis's time was part-funded by UK Research and Innovation (UKRI) under the UK government's Horizon Europe Funding Guarantee [EP/Z000068/1] (AUGSOC -https://augsoc-project.org/).

References

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay cool! understanding thermal attacks on mobile-based user authentication. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. 3751–3763.

[2] 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.

[3] Yasmeen Abdrabou, Sheikh Radiah Rivu, Tarek Ammar, Jonathan Liebers, Alia Saad, Carina Liebers, Uwe Gruenefeld, Pascal Knierim, Mohamed Khamis, Ville Makela, et al. 2022. Understanding shoulder surfer behavior and attack patterns using virtual reality. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces*. 1–9.

[4] Yusuf Albayram, Mohammad Maifi Hasan Khan, and Michael Fagan. 2017. A study on designing video tutorials for promoting security features: A case study in the context of two-factor authentication (2fa). *International Journal of Human–Computer Interaction* 33, 11 (2017), 927–942.

[5] Florian Alt, Stefan Schneegass, Alireza Sahami Shirazi, Mariam Hassib, and Andreas Bulling. 2015. Graphical passwords in the wild: Understanding how users choose pictures and passwords in image-based authentication schemes. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*. 316–322.

[6] Paul Bekaert, Norah Alotaibi, Florian Mathis, Nina Gerber, Aidan Christopher Rafferty, Mohamed Khamis, and Karola Marky. 2022. Are thermal attacks a realistic threat? Investigating the preconditions of thermal attacks in users' daily lives. In *Nordic Human-Computer Interaction Conference*. 1–9.

[7] Rasekhar Bhagavatula, Blase Ur, Kevin Iacovino, Su Mon Kywe, Lorrie Faith Cranor, and Marios Savvides. 2015. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption. (2015).

[8] Jim Blythe, Jean Camp, and Vaibhav Garg. 2011. Targeted risk communication for computer security. In *Proceedings of the 16th international conference on Intelligent user interfaces*. 295–298.

[9] Xander Bouwman, Harm Griffioen, Jelle Egbers, Christian Doerr, Bram Klievink, and Michel Van Eeten. 2020. A different cup of {TI}? the added value of commercial threat intelligence. In *29th USENIX security symposium (USENIX security 20)*. 433–450.

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

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

[12] 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.

[13] Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2012. Increasing the security of gaze-based cued-recall graphical passwords using saliency masks. In *Proceedings of the SIGCHI conference on human factors in computing systems*. 3011–3020.

[14] Kelly Caine. 2016. Local standards for sample size at CHI. In *Proceedings of the 2016 CHI conference on human factors in computing systems*. 981–992.

[15] Seunghun Cha, Sungsu Kwag, Hyoungshick Kim, and Jun Ho Huh. 2017. Boosting the guessing attack performance on android lock patterns with smudge attacks. In *Proceedings of the 2017 ACM on Asia conference on computer and communications security*. 313–326.

[16] Jake Chanenson, Brandon Sloane, Navaneeth Rajan, Amy Morril, Jason Chee, Danny Yuxing Huang, and Marshini Chetty. 2023. Uncovering Privacy and Security Challenges In K-12 Schools. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–28.

[17] DailyMail. 2008. *The zzzzivil servant who fell asleep on the train with laptop secrets in full view.* Retrieved August 8, 2024 from https://www.dailymail.co.uk/news/article-1082375/The-zzzzivil-servant-fell-asleep-train-laptop-secrets-view.html

[18] Sanchari Das, Shrirang Mare, and L Jean Camp. 2020. Smart storytelling: Video and text risk communication to increase mfa acceptability. In *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 153–160.

[19] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now you see me, now you don't: protecting smartphone authentication from shoulder surfers. In *Proceedings of the sigchi conference on human factors in computing systems*. 2937–2946.

[20] 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 CHI Conference on Human Factors in Computing Systems*. 1–23.

[21] 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.

[22] Habiba Farzand, Melvin Abraham, Stephen Brewster, Mohamed Khamis, and Karola Marky. 2024. A Systematic Deconstruction of Human-Centric Privacy & Security Threats on Mobile Phones. *International Journal of Human–Computer Interaction* (2024).

[23] 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.

[24] Habiba Farzand, Karola Marky, and Mohamed Khamis. 2022. " I Hate When People Do This; There's a Lot of Sensitive Content for Me": A Typology of Perceived Privacy-Sensitive Content in Shoulder Surfing Scenarios. (2022).

[25] 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.

[26] Habiba Farzand, Karola Marky, and Mohamed Khamis. 2023. "... It's very unacceptable for someone to peek into your privacy." Chronicles of Shoulder Surfing: Exploring Deep into a Longitudinal Diary Study. (2023).

[27] Cristina Fiani, Pejman Saeghe, Mark McGill, and Mohamed Khamis. 2024. Exploring the Perspectives of Social VR-Aware Non-Parent Adults and Parents on Children's Use of Social Virtual Reality. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1 (2024), 1–25.

[28] European Association for Visual Data Security. 2012. *Visual Data Security White Paper*. Retrieved August 8, 2024 from https://multimedia.3m.com/mws/media/950026O/secure-white-paper.pdf

[29] Wendy Goucher. 2011. Look behind you: the dangers of shoulder surfing. *Computer Fraud & Security* 2011, 11 (2011), 17–20.

[30] Jan Gugenheimer, Alexander De Luca, Hayato Hess, Stefan Karg, Dennis Wolf, and Enrico Rukzio. 2015. Colorsnakes: Using colored decoys to secure authentication in sensitive contexts. In *Proceedings of the 17th international conference on human-computer interaction with mobile devices and services*. 274–283.

[31] 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.

[32] 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.

[33] Franziska Herbert, Steffen Becker, Leonie Schaewitz, Jonas Hielscher, Marvin Kowalewski, Angela Sasse, Yasemin Acar, and Markus Dürmuth. 2023. A world full of privacy and security (mis) conceptions? Findings of a representative survey in 12 countries. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–23.

[34] Christina Katsini, Yasmeen Abdrabou, George E Raptis, Mohamed Khamis, and Florian Alt. 2020. The role of eye gaze in security and privacy applications: Survey and future HCI research directions. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–21.

[35] 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.

[36] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2018. Evaluating Attack and Defense Strategies for Smartphone PIN Shoulder Surfing. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, Article 164, 10 pages.

[37] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2018. Evaluating attack and defense strategies for smartphone pin shoulder surfing. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–10.

[38] Sushmita Khan, Mehtab Iqbal, Oluwafemi Osho, Khushbu Singh, Kyra Derrick, Philip Nelson, Lingyuan Li, Emily Sidnam-Mauch, Nicole Bannister, Kelly Caine, et al. 2024. Teaching Middle Schoolers about the Privacy Threats of Tracking and Pervasive Personalization: A Classroom Intervention Using Design-Based Research. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–26.

[39] Jacob Leon Kröger, Otto Hans-Martin Lutz, and Florian Müller. 2020. What does your gaze reveal about you? On the privacy implications of eye tracking. In *IFIP International Summer School on Privacy and Identity Management*. Springer, 226–241.

[40] Michael Lutaaya, Khadija Baig, Sana Maqsood, and Sonia Chiasson. 2021. "I'm Not a Millionaire": How Users' Online Behaviours and Offline Behaviours Impact Their Privacy. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–7.

[41] Shaun Alexander Macdonald, Habiba Farzand, Norah Alotaibi, Md Shafiqul Islam, and Mohamed Khamis. 2023. Change Policy or Users? Mitigating the Security Risks of Thermal Attacks. (2023).

[42] Diogo Marques, Tiago Guerreiro, Luis Carriço, Ivan Beschastnikh, and Konstantin Beznosov. 2019. Vulnerability & blame: Making sense of unauthorized access to smartphones. In *Proceedings of the 2019 chi conference on human factors in computing systems*. 1–13.

[43] 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)*. 159–174.

[44] Philipp Mayring et al. 2004. Qualitative content analysis. *A companion to qualitative research* 1, 2 (2004), 159–176.

[45] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. *Proceedings of the ACM on human-computer interaction* 3, CSCW (2019), 1–23.

[46] Weizhi Meng, Wang Hao Lee, SR Murali, and SPT Krishnan. 2015. Charging me and I know your secrets! Towards juice filming attacks on smartphones. In *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*. 89–98.

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

[48] George Probst. 2000. *Analysis of the Effects of Privacy Filter Use on Horizontal Deviations in Posture of VDT Operators*. Master's thesis. Virginia Polytechnic Institute and State University.

[49] Prolific. 2024. Prolific | Online participant recruitment for surveys and market research. https://www.prolific.co/ Retrieved May 28, 2024.

[50] Qualtrics. 2024. Qualtrics - Leading Experience Management and Survey Software. https://www.qualtrics.com/uk/?rid=ip&prevsite=en&newsite=uk&geo=GB&geomatch=uk Retrieved February 11, 2024.

[51] Kirill Ragozin, Karola Marky, Jie Lu, and Kai Kunze. 2022. EyeMove-Towards Mobile Authentication using EOG Glasses. In *Augmented Humans 2022*. 10–14.

[52] Rahul Raguram, Andrew M White, Dibyendusekhar Goswami, Fabian Monrose, and Jan-Michael Frahm. 2011. iSpy: automatic reconstruction of typed input from compromising reflections. In *Proceedings of the 18th ACM conference on Computer and communications security*. 527–536.

[53] Alia Saad, Michael Chukwu, and Stefan Schneegass. 2018. Communicating Shoulder Surfing Attacks to Users. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia*. 147–152.

[54] 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.

[55] Mennatallah Saleh, Mohamed Khamis, and Christian Sturm. 2019. What about my privacy, Habibi? Understanding privacy concerns and perceptions of users from different socioeconomic groups in the Arab World. In *Human-Computer Interaction–INTERACT 2019: 17th IFIP TC 13 International Conference, Paphos, Cyprus, September 2–6, 2019, Proceedings, Part III 17*. Springer, 67–87.

[56] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. " Privacy is not for me, it's for those rich women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. 127–142.

[57] Garrett Smith, Sarah Carson, Rhea G Vengurlekar, Stephanie Morales, Yun-Chieh Tsai, Rachel George, Josh Bedwell, Trevor Jones, Mainack Mondal, Brian Smith, et al. 2024. " I Know I'm Being Observed:" Video Interventions to Educate Users about Targeted Advertising on Facebook. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–27.

[58] Timothy J Trull and Ulrich W Ebner-Priemer. 2009. Using experience sampling methods/ecological momentary assessment (ESM/EMA) in clinical assessment and clinical research: introduction to the special section. (2009).

[59] Emanuel Von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. Swipin: Fast and secure pin-entry on smartphones. In *Proceedings of the 33rd annual acm conference on human factors in computing systems*. 1403–1406.

[60] Ge Wang, Jun Zhao, Konrad Kollnig, Adrien Zier, Blanche Duron, Zhilin Zhang, Max Van Kleek, and Nigel Shadbolt. 2024. KOALA Hero Toolkit: A New Approach to Inform Families of Mobile Datafication Risks. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–18.

[61] Ge Wang, Jun Zhao, Max Van Kleek, and Nigel Shadbolt. 2022. Informing age-appropriate ai: Examining principles and practices of ai for children. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–29.

[62] Dominik Wermke, Noah Wöhler, Jan H Klemmer, Marcel Fourné, Yasemin Acar, and Sascha Fahl. 2022. Committed to trust: A qualitative study on security & trust in open source software projects. In *2022 IEEE symposium on Security and Privacy (SP)*. IEEE, 1880–1896.

[63] Jie Zhang, Zhanyong Tang, Meng Li, Dingyi Fang, Xiaojiang Chen, and Zheng Wang. 2019. Find me a safe zone: A countermeasure for channel state information based attacks. *Computers & Security* 80 (2019), 273–290.

[64] Huiyuan Zhou, Khalid Tearo, Aniruddha Waje, Elham Alghamdi, Thamara Alves, Vinicius Ferreira, Kirstie Hawkey, and Derek Reilly. 2016. Enhancing Mobile Content Privacy with Proxemics Aware Notifications and Protection. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. 1362–1373.

[65] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–15.

A Survey Format for the Impact Study

Shoulder Surfing refers to observing someone's device screen without permission. Shoulder surfing can happen anytime and by anyone, requiring no particular expertise or equipment, but careful observation. Among all devices, smartphones

are the most shoulder-surfed devices. For this reason, in this study, we focus on experiences of shoulder surfing on smartphones only. Considering this definition, please answer the following questions.

(1) When did you experience shoulder surfing most recently?
   - Yesterday or today,
   - A few days ago,
   - Less than a month ago,
   - A few months ago.

(2) For the statement, "I am shoulder surfed almost daily":
   - Strongly disagree
   - Somewhat disagree
   - Neither agree nor disagree
   - Somewhat agree
   - Strongly agree

(3) Please describe the latest shoulder surfing experience which you experienced. Please provide as much details as possible.

Considering the experience you just shared, please answer the following questions:

(4) For the statement: "I continue using the smartphone and accessing information in the same setting where I experienced shoulder surfing", you:
   - Strongly disagree
   - Somewhat disagree
   - Neither agree nor disagree
   - Somewhat agree
   - Strongly agree

   Please provide reasons for your answer in the previous question. Please provide as much details as possible.

(5) For the statement: "The shoulder surfing experience affected my perceptions towards my privacy", you:
   - Strongly disagree
   - Somewhat disagree
   - Neither agree nor disagree
   - Somewhat agree
   - Strongly agree

   Please provide reasons for your answer in the previous question. Please provide as much details as possible.

(6) For the statement, " If someone sees my friend's content on my screen (e.g., a picture or a message of my friend), it feels like a breach of my friend's trust in me to keep their content private", you:
   - Strongly disagree
   - Somewhat disagree
   - Neither agree nor disagree
   - Somewhat agree
   - Strongly agree

Please provide reasons for your answer in the previous question. Please provide as much details as possible.

(7) For the statement: “Experiencing shoulder surfing prevented me or slowed me down from what I wanted to do on the device”, you:
- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

Please provide reasons for your answer in the previous question. Please provide as much details as possible.

(8) For the statement: “Experiencing shoulder surfing impacted negatively the way I use my device”, you:
- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

Please provide reasons for your answer in the previous question. Please provide as much details as possible.

(9) For the statement: “Experiencing shoulder surfing impacted positively the way I use my device”, you:
- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

Please provide reasons for your answer in the previous question. Please provide as much details as possible.

(10) List your three biggest concerns around shoulder surfing. Please provide as much details as possible.

(11) Are you aware of any technology or security features that can help prevent or mitigate shoulder surfing? Please provide as much details as possible.

(12) Have you received any education or training on protecting yourself from shoulder surfing, personally or through your workplace or educational institution? Please provide as much details as possible.

(13) Have you used additional privacy protection measures to protect your privacy from shoulder surfing? Please provide as many details as possible.

(14) For the statement: "I would use additional privacy measures or tools to prevent shoulder surfing incidents", you:
- Strongly disagree
- Somewhat disagree
- Neither agree nor disagree
- Somewhat agree
- Strongly agree

Please provide reasons for your answer in the previous question. Please provide as much details as possible.

Contextual Privacy	
Codes	References
Contextual Privacy	39
Information Specific Concern	40
Location Specific Concern	9
Protection in Public Spaces	3

Personal Privacy	
Codes	References
Concerns	18
Leakage of Information Privacy	40
Need of Privacy Mechanisms	33
Negative Emotions	35
Negative Impact	39
Other People's Privacy	54
Personal Privacy	89

Protection Measures	
Codes	References
Altering Physical Setting	61
Availability of Protection Measures	1
Avoiding Device Use for Protection	13
Awareness of Protection Tools	5
Carefulness of Surrounding	10
Ease of Use of Mechanisms	3
Mechanism Invasiveness	5
Reliability, Effectiveness, Functionality	10
Prevention	5
Privacy Screen	7
Protection Mechanisms Financial Cost	9
Selective Information Access	29

Shoulder Surfing as Inconsequential	
Codes	References
Continued Use Without Change	53
No Effect of Device Usage	47
No effect on Task Completion	27
No Impact on Privacy Perceptions	39
Unintentional Breach	31
Unnecessary Measures	17

Situational Awareness	
Codes	References
Rethinking Accessing of Information	8
Surrounding Awareness	80
Task Interruption	29
Thoughts Reframing	9
Ubiquitous Shoulder Surfing	31
Unavoidable	16

Worries of Leading Threats	
Codes	References
Blackmailing	2
Child Safety	2
Identity Theft	12
Inappropriate Content	6
Information Theft	10
Misuse of Information	14
Self Perception from the Eyes of Others	13
Stalking	5
Unauthorised Access	4

Table 1. Codebook