Shoulder Surfing through the Social Lens: A Longitudinal Investigation & Insights from an Exploratory Diary Study

Habiba Farzand
habiba.farzand@glasgow.ac.uk
University of Glasgow
United Kingdom

Karola Marky
karola.marky@itsec.uni-hannover.de
Leibniz University Hannover
Germany
University of Glasgow
United Kingdom

Mohamed Khamis
mohamed.khamis@glasgow.ac.uk
University of Glasgow
United Kingdom

Figure 1: The figure shows some commonly occurring scenarios of shoulder surfing in everyday life of users resulting from the findings of the diary study. The diary study showed that user's privacy is compromised in the naturalistic settings. Content-based shoulder surfing is more frequent than authentication-based shoulder surfing. In the scenarios shown in the figure, the shoulder surfer (the person in the red shirt) is invading the user's privacy by observing the user's screen without their consent. Shoulder surfing can happen in private and/or public environments such as an individual's home, office, or shopping mall. Further, anyone could be a shoulder surfer; related or unrelated to the user, as it only requires observing someone's screen close in distance. Different observations are perceived differently by users, and users prefer different mechanisms in different contexts of shoulder surfing. (The figure was created using Canva [7] under Free Content License.)

ABSTRACT

Shoulder surfing is a prevailing threat when accessing information on personal devices like smartphones. Adequate mitigation requires studying shoulder surfing occurrences in people's daily lives. In this paper, we confirm and extend previous research findings on shoulder surfing occurrences using a new method; a one-month diary study (N=23). Our results provide evidence of shoulder surfing in public and private environments. Content-based shoulder surfing happens more frequently than authentication-based shoulder surfing. Participants experienced shoulder surfing at least twice during the study period and considered the closeness of relationships with the shoulder surfers when deciding how to respond to shoulder surfing incidents. Participants preferred unobtrusive alerting mechanisms over mitigation mechanisms for protection against shoulder surfing. Our work advocates moving away from one-size-fits-all privacy solutions and supports the design of user-centred shoulder surfing mitigation methods that consider social aspects. We conclude with directions for future research to assist security researchers and practitioners.

EuroUSEC 2022, September 29–30, 2022, Karlsruhe, Germany

ACM ISBN 978-1-4503-9700-1/22/09…$15.00
https://doi.org/10.1145/3549015.3554211

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; **Privacy protections**;

KEYWORDS

shoulder surfing, privacy, security

ACM Reference Format:
Habiba Farzand, Karola Marky, and Mohamed Khamis. 2022. Shoulder Surfing through the Social Lens: A Longitudinal Investigation & Insights from an Exploratory Diary Study. In *2022 European Symposium on Usable Security (EuroUSEC 2022), September 29–30, 2022, Karlsruhe, Germany*. ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3549015.3554211

1 INTRODUCTION

"Privacy isn't about something to hide. Privacy is about something to protect. And that's who you are. That's what you believe in. That's who you want to become. Privacy is the right to the self. Privacy is what gives you the ability to share with the world who you are on your own terms."

Edward Snowden, 2016

Shoulder surfing refers to the action of gaining private information by looking at the device screen of a user [30]. While shoulder surfing can also be done using cameras, binoculars, or mirrors, direct observation is the most frequently used method [20, 50]. Shoulder surfing through direct observation does not require special knowledge, since it is only a gaze at a person's device. Furthermore, shoulder surfers could be anyone, such as strangers, family members, friends, colleagues, or even intimate partners [13, 33, 36]. The ease of executing this attack and the fact that anyone could be a shoulder surfer makes shoulder surfing an ubiquitous threat. Several investigations in the literature underpin the existence of shoulder surfing in people's daily lives [13, 36, 43].

Related work proposed several mitigation methods aiming to protect users from shoulder surfing [39, 43, 47]. While such mechanisms deliver effectiveness, when and what mechanism is perceived suitable with respect to shoulder surfing incidents is not explored. Thus, informing the design and use of shoulder surfing mitigation mechanisms require a holistic knowledge of shoulder surfing incidents in people's daily lives.

In this paper, we contribute detailed shoulder surfing incidents through a one-month diary study with 23 participants. Through diary logging, we also captured methods that participants perceived to be appropriate for protecting the observed content based on their relationship to the observer. The results provided a comprehensive breakdown of the details of day-to-day incidents of shoulder surfing. For instance, we learned that our participants, on average, experienced shoulder surfing at least twice during the study period while the highest number of shoulder surfing incidents experienced is 8 per day during the study period. Our analysis of diaries confirms that shoulder surfing is mostly carried out by strangers in public spaces on smartphones during nighttime. Participants preferred privacy-oriented and interruption-free mitigation mechanisms and different mechanisms for different related shoulder surfers.

This paper aims to address the following research questions:

- **RQ1:** What social contexts account for shoulder surfing incidents in the daily lives of people?
- **RQ2:** What shoulder surfing protection mechanisms are preferred by users and why?
- **RQ3:** What are the implications of shoulder surfing?

2 BACKGROUND & RELATED WORK

Previous research related to our can be summarized based on: 1) reported shoulder surfing stories, and 2) shoulder surfing mitigation methods.

2.1 Shoulder Surfing Stories

Muslukhov et al. [36] studied shoulder surfing through interviews and online surveys to understand users' concerns about unauthorized access to their devices. They found that many users are concerned about unauthorized access by friends and other "insiders". More generically, and most relevant to our work, is a shoulder surfing investigation by Eiband et al. [13] which provided the first evidence of shoulder surfing incidents in the real world. The study collected 174 shoulder surfing stories through a one-time online survey. Participants shared their experiences based on their perspectives as observers, observees, and as third persons, i.e., people that observed a shoulder surfing situation while not being involved. Out of 174 stories, 84 were reported by observers, 58 by users and 22 by third persons. Strangers were found to be the most frequently reported observer (N=126 stories). The majority of these experiences were reported in public areas, such as public transport, or public buildings.

The most commonly reported activity during the shoulder surfing incident was being on the way, followed by commuting and working/studying. Smartphones are the most shoulder surfed devices. Other devices included handheld mobile devices and laptops. Texts and pictures accounted for most of the shoulder surfed content. The main motivations for shoulder surfing were curiosity, boredom and inadvertently. Despite this, shoulder surfing led to negative feelings on the users' side. Not only users, but the observers also experienced negative feelings.

The work by Saad et al. [43] documented triggers of shoulder surfing using 360-degree videos in virtual reality. The study focused on public transport and found that on average each participant glances on the screen's device on average 6.73 times. The study also found that sitting participants are more likely to gaze at a standing person's smartphone than vice versa. Regarding shoulder surfed content, 87.5% participants reported at least one out of four applications; WhatsApp, Facebook, Gallery, and games. Gallery and WhatsApp were among the most shoulder surfed content. Some participants also provided detailed information of the content, such as pictures found in the photo gallery, details of games, and WhatsApp messages. Moreover, all participants admitted that they have been shoulder surfers at least once. The results imply that shoulder surfing is not restricted to a particular group, hence, anyone can be a shoulder surfer.

Another stream of research investigated the vulnerability of authentication patterns and PIN entry methods to shoulder surfing. Many of these works involve participants watching videos of users as they authenticate [2]. In a study by Aviv et al. [2], they found PINs are less vulnerable to attacks than unlock patterns. They also found that observation angles and distances impact the effectiveness of shoulder surfing.

In summary, related work that investigated shoulder surfing stories revealed specific scenarios in which shoulder surfing is more likely to occur compared to others. Either the related work

was focused on one specific location in which shoulder surfing could occur, or collected experiences in a one-time survey. This paper uses the information gained by related work to design a diary study that is conducted over a period of one month. This allows us to extend the results from related work to develop a more coherent understanding of what social contexts account for shoulder surfing incidents in the daily lives of people.

2.2 Shoulder Surfing Mitigation Methods

Over the past years, security and HCI researchers have proposed numerous shoulder surfing mitigation mechanisms. These mechanisms can be classified as "alerting" or as "mitigating" mechanisms. Alerting mechanisms only alert the user about shoulder surfing and lets the user decide what to do next. Whereas, a mitigation mechanism protects privacy by hiding the content [16].

Examples of mitigation mechanisms offering protection from shoulder surfing of personal photos can be based on graphic filters that distort the pictures in galleries [47]. To protect textual content, researchers proposed using customized fonts to copy users' handwriting to make the text more difficult to read for observers [14]. Following a similar direction, EyeSpot [26] and PrivateReader [39] track the user's eyes to hide content that is not being looked at. Further methods for safeguarding include selective showing [51], selective hiding [51], fake text filters [26], grayscale filter [51], lowering brightness [41], showing alert icon [41, 51], crystallize filters [26], dimming filters [26], showing a front camera preview [41], flashing the front LED [41], flashing borders [6], showing the shoulder surfer's silhouette [6], showing the shoulder surfer's gaze direction with a silhouette [6], and hiding content using a white screen [22]. In sum, a variety of mitigating mechanisms has been proposed and investigated in the literature. The mechanisms differ based on the protected content. However, it is yet to be discovered what mechanism is socially acceptable in the context of each shoulder surfing incident occurring in the daily lives of people. Social acceptability of shoulder surfing mechanisms is crucial because it has been shown that the appropriateness and choice of a mechanism are dependent on the relationship with the observer [16]. It is also crucial because low social acceptability also poses an effect on the user's self and external image [29] with further impact on the user experience as well [49].

Contribution Statement: The contribution of this work is threefold: **1)** We confirm and extend research on occurrences of shoulder surfing reported in prior work and provide evidence for scenarios in which user privacy is likely to be violated through direct observation based on real-world data, **2)** we advocate and provide evidence for the need of context-aware and configurable protection against shoulder surfing, and **3)** we propose research questions for content-based shoulder surfing based on stories from users. Our work can be leveraged to inform the design of configurable and context-aware shoulder surfing mitigation mechanisms.

3 METHODOLOGY

In our study, we investigate the occurrences of shoulder surfing in people's daily lives through a one-month diary study. Diary studies are more precise than other research methods [1]. They complete the missing pieces in the research methods between observation in a naturalistic environment, observation in a fixed lab, and surveys [23]. Moreover, diaries are increasingly gaining attention in HCI research [8, 15, 45] and are frequently used by social researchers [40]. To collect a rich corpus of shoulder surfing episodes, we used a qualitative approach; the diary method places minimal limits on the richness of what can be captured, allowing participants to record and reflect on meaningful events.

3.1 Study Design

Diary Design: We used the survey provider Qualtrics [37] to build the questionnaire and as a medium to log diary entries. The questions for the diary study were informed by prior work on shoulder surfing occurrences such as time, location, activity, and alike [13]. We asked participants to report the incidents of shoulder surfing from the perspectives of observers, observees, and third persons. We opted for collecting free-text responses to avoid biasing the participants. The diary format can be found in the Appendix A.

Relationship Classification: Personal relationships and shoulder surfing share a two-sided connection [16]. Hence, it is important to understand how the choice of protection mechanism forms and changes with respect to changes in the level of relationship. For this purpose, we used the 12-item relationship closeness scale [12].

Selected Combating Mechanisms & Methods: Images showcasing mitigation methods were included in the diary logging format to gain insight on which method is preferred and socially acceptable with respect to the closeness of relationship and appropriateness of the social context. We selected 15 mechanisms which can be found in the Appendix A.

3.2 Recruitment & Participants

We recruited 23 participants (N=20 from Australia, N=3 from New Zealand) through social media channels and SIGCHI mailing lists. This number of participants was chosen as prior work has reported rich data collection with either 23 participants or less using diary studies [15, 45]. 19 participants self-identified as male, two as female, and two as non-binary/third gender. The participants were on average 26 years old (SD=4.37, Min=20, Max=35). Thirteen participants were employed, six were students, and four participants reported to be unemployed.

3.3 Procedure

The study was approved by the Ethics committee at our institute. The study commenced with an information page followed by a consent form. At this point in the study, participants were informed that the study aims to explore how unnoticed technological interactions are shaping relationships and personal sentiments. After expressing their consent, participants were then presented with a short questionnaire that inquired about their basic demographic details. Following this, the participants were emailed a link to the diary study. They were asked to log incidents whenever they found someone looking over their devices' screen without their consent. Phrases like *"shoulder surfing", "attacker"* were avoided to offset the social desirability biases [46]. The diary study lasted over a period of 29 days starting from 8th May 2021 to 5th June 2021. Diary logging reminders were sent to participants every three days.

After 29 days, participants were thanked and reimbursed with $7 (Australian $) Amazon vouchers.

3.4 Data Analysis

Overall, the participants reported N=62 stories. Out of the N=62 stories, N=11 stories indicated that on that specific day there was "Nothing to report", because participants did not experience shoulder surfing. These stories were removed from the analysis. Nine (N=9) responses were further removed as they did not provide any meaningful data, for example, "I don't know" and alike. For the remaining N=42 stories, we performed inductive coding [34].

To determine whether further data collection is required, we calculated information saturation using the method proposed by Guest et al. [19] that sets the information threshold at <=5%. Following the proposed approach, we first checked the distinct themes for the base which in our case was 54. A codebook was formulated after the first round of revisions and then filtered until no further adjustments were required to be made. We then calculated the saturation ratio by dividing the new themes in the second run (0) by the number of distinctive themes in the base set (54). The quotient exhibited 0% new information. This falls under the <=5% threshold, therefore, we stopped collecting further data. Validity of the results was verified through discussions among the two researchers during the coding process and by steps taken to iteratively refine the codebook. Due to the qualitative and exploratory nature of the study, we intentionally do not report measures of inter-rater agreement [35]. This resulted in the refinement of the codebook. The codebook that denotes the categories can be found in the Appendix B.

We report the number of times a code occurred to give the readers the impression of how often the particular category appeared. However, we do not quantify the frequency of the category reported and hence, it should be not considered as quantitative analysis.

4 LIMITATIONS & FUTURE WORK

In this paper, we include user quotes from the diary to support enhanced understanding and improved clarity. However, there is no traceability to the participants' identities. Our study followed the guidelines provided by the Ethics Committee at our institute. Second, while we recruited an adequate number of participants for our study and ensured information saturation, participants may not be representative of the entire population. Our recruited sample was slightly biased towards males. Further, participants of our studies belonged to technologically advanced countries where privacy and security knowledge is more common and accessible as compared to developing countries. Moreover, the privacy perception varies as we move across different socioeconomic and cultural groups [44]. It will be interesting to investigate how the reporting of shoulder surfing and its implications vary between different cultures. In future work, we propose to build user-centred shoulder surfing mitigation mechanisms that are context-aware, configurable, and are considerate of social aspects.

5 FINDINGS

In our study, participants reported N=42 stories of shoulder surfing. Out of these, N=23 (54.76%) were observer stories, N=13 (30.95%) were observee stories, and N=6 (14.29%) were third person stories (i.e., story by those who saw a shoulder surfing situation). Fig 2 showcases the time and location reported in the diary log of shoulder surfing incidents.

5.1 The Observer's Side of the Story

Out of the N=42 stories logged, N=23 storied were reported by observers. In the observers' opinion, the user noticed the unconsented observation of the screen in almost half of the times (N=12), remained unnoticed in a few stories (N=9), but they were also unsure in some incidents (N=2). The observers explained that the reason for observing the screens was mainly curiosity (N=7), boredom (N=4), common interest (N=1), relevancy to the conversation with the user (N=1). It was also because the screen was in the line of sight of the observer (N=5). Further, the observers reported that they mainly shoulder surfed smartphones of friends (N=14), strangers (N=4), and family members (N=2). Observers noticed that the user was scrolling through the smartphone (N=8), reading text (N=5), or playing a game on the smartphone (N=5). Further, other activities such as watching videos (N=1) and performing web search (N=1) were also reported as shoulder surfed activities. Notes of the specific applications that the users interacted were also taken and consisted of mainly messaging (N=9), game (N=5), social media (N=4), and emails (N=3). Based on the observed content, the observers estimated the importance of the task the user was performing. The task was perceived as important in one third of stories (N=7). The same importance of the task might not be reflected from the user's perspective but this shows the interest of the observer conveying what content is most likely to be shoulder surfed. During the shoulder surfing situations, the observer and user were found to be chatting (N=8), having food (N=3), or riding transport (N=2). In some situations, they were also playing games (N=2), watching television (N=1), and casually checking their phones (N=1). This shows that shoulder surfing occurs in the naturalistic settings and does not account for an attack setup.

Public transport was the most reported location for shoulder surfing incidents (N=9) followed by public locations for dining and drinking (N=7), work (N=4), and private environments (N=3). Nighttime was when most of the shoulder surfing incidents took place (N=11), followed by afternoon (N=6), evening (N=3), and morning (N=2). A single person was reported to be involved as an observer in N=10 stories, whereas two people were involved as observers in five stories and three people in four stories. This provides evidence that shoulder surfing through multiple observers is experienced by users [25]. These findings assist in answering **RQ 1**.

Key Take Away #1: According to observer stories collected, anyone (related or unrelated) could be a shoulder surfer at any time of the day, but it occurs mostly at the nighttime. Public transport is the highlighted red zone for shoulder surfing. In most cases, shoulder surfing is done by one observer but sometimes shoulder surfing can also be done by multiple observers.

5.2 The User's Side of the Story

5.2.1 Shoulder Surfing Experiences: Out of N=42 stories logged, N=13 stories were reported by participants who experienced shoulder surfing by someone. Smartphones were reported as the most

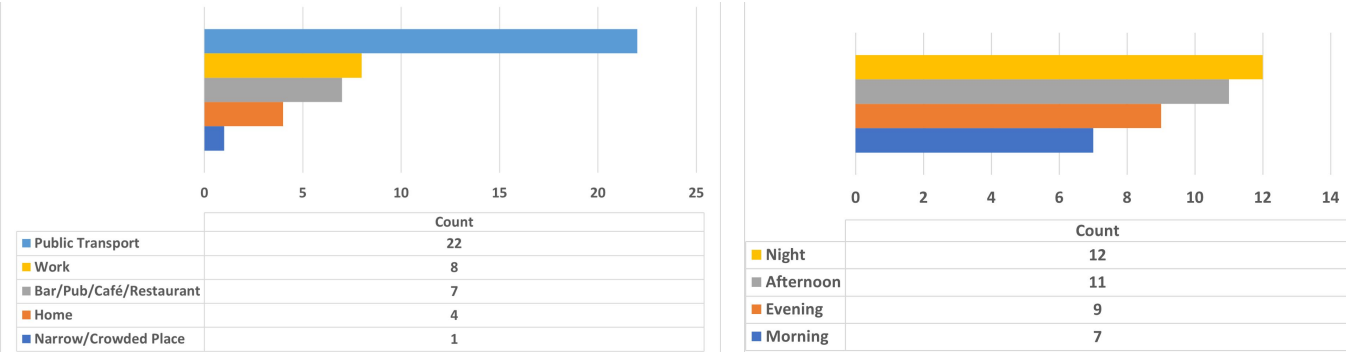

Figure 2: Location (left) and time (right) of shoulder surfing incidents experienced by participants of diary study either as observer, observee, or as third person.

shoulder surfed device (N=12) followed by Tablet-PCs (N=1). This shows mobile devices are the most shoulder surfed devices. The pervasiveness and the ability to collect data about users such as personal information [21], makes mobile phones most vulnerable to privacy and security invasions. Users experienced shoulder surfing incidents in the evening (N=5). Other times reported include mornings (N=3), afternoons (N=2), and at night (N=1). Similar to observer stories, participants experienced shoulder surfing mostly in public transport (N=8), followed by workplaces (N=3), homes (N=1), and narrow/crowded places (N=1). Friends and strangers were the most frequently mentioned shoulder surfers (N=6 each) and family was reported in the N=1 story. The reason for observing was mainly curiosity (N=6) followed by boredom (N=3) and common interest (N=2). The incident of shoulder surfing was reported when the participant was either on their way (N=3), checking phones (N=3), working (N=1) or waiting (N=1). Reading was the main activity being carried out on the device (N=5). Texting (N=3) was the second most reported followed by scrolling (N=1), and video calling (N=1). The apps being used on the device were messaging apps (N=4), email apps (N=4), and video calling apps (N=1). 66% of participants agreed that the task carried out on the device during the shoulder surfing incident was *"important"* to them. 25% of participants reported having time lost due to the privacy intervention. The users' side of stories contributed to addressing **RQ 1**.

5.2.2 Choice for Shoulder Surfing Protection Mechanisms: 50% of participants expressed willingness to have a mechanism while 41.66% of participants were found to be neutral. Participants mentioned that they would like the mechanism to alert (N=3), remind (N=2), automatically lock the screen (N=1), or blurry the screen from side angles (N=1). Participants were then presented with the mechanisms from related work along with a short description, and asked to choose the most suitable according to the situation and the observer. According to our participants, flashing borders [41] were seen as the most appropriate mechanism (27.27%). The second most voted choices include blank screens and selective showing (18.18% each). This was followed by dimming filters, front camera previews, selective hiding, and low brightness (9.1% each). Participants also proposed modifications to the mechanisms, including blurring of faces in photos [27, 31] and reduced notifications.

Using a mechanism may impact the relationship between the user and the observer [16]. Considering this, participants were asked if they think having a mechanism will impact their relationship with the observer. 63.63% of participants voiced that they consider the mechanism will not impact their relationship in any way. While the remaining 36.36% neither agreed nor disagreed. Fig 3 shows the results for preference of mechanism, mechanism impact on the relationship, time wastage due to privacy invasion, and importance of task during the situation of shoulder surfing.

For strangers, participants reflected values between 1.00 to 4.08 (Mean=2.42, SD=1.56) on the relationship closeness scale [12] showing low - medium relationship closeness. Mechanisms preferred for observers belonging to this range of closeness included dimming filters (N=1), flashing borders (N=1), selective showing (N=1), and low brightness (N=1). Dimming filters were preferred they prevent from *"peeking"* (P11). Flashing borders were chosen as it *"doesn't interrupt flow of activity"* (P4). Selective showing was regarded as *"maintaining privacy"* (P4, P5) as well as letting the user continue the main task. Low brightness was favoured as it helps in making the people in the pictures unidentifiable. Overall, participants preferred privacy maintaining and interruption-free mechanisms.

For friends, the relationship closeness scale [12] reported values between 4.00 to 6.58 (Mean=5.33, SD=0.97). Mechanisms preferred for observers belonging to this range of closeness of relationship included flashing borders (N=2), selective hiding (N=1), front camera preview (N=1), selective showing filter (N=1), and blank screen (N=1). Overall, the mechanisms were preferred based on their ability to *"maintain privacy"* (P5). For family members (relationship closeness scale: Mean=3.58, SD=), blank screen was favoured as it was seen *"..safer"* (P6). The selected method for the reported stories was found to be adequate by 63.63% of observees. 63.63% disagreed that having a mechanism will impact the relationship with the observer. Suggestions to improve selected mechanisms included fewer notifications and blurring of faces found in photos [27]. Overall, 36.36% of participants voiced to have the user interface as the controller of the mechanisms while 36.36% of participants wished to control the mechanism themselves. However, 27.27% of participants favoured that both should have control over the mechanism. These findings contributed towards **RQ 2**.

Key Take Away #2: In the light of observee stories, users experience shoulder surfing mostly in the evening and when using public transport. Shoulder surfing exists in public and as well as in private environments such as an individual's accommodation. Smartphones

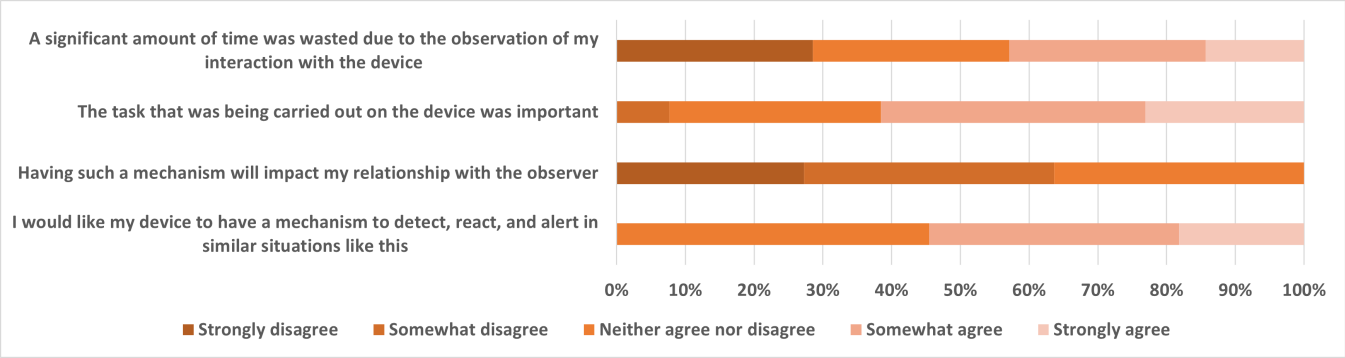

Figure 3: The responses received on a 5-point Likert scale for the impact of shoulder surfing on interaction time wastage, the importance of the task, preference for mechanisms, the impact of mechanism on relationship perceived by observees of the diary study.

are the most shoulder surfed device, hence, demands the most protection against visual privacy invasions. Visual privacy invasions such as shoulder surfing are not just invading the user's privacy but also result in user device interaction time wastage. Participants prefer different mechanisms for different levels of the closeness of the relationship with the observer. Hence, one protection mechanism cannot offer a "one-size-fits-all" solution.

5.3 Stories from 3rd Persons

Six stories of shoulder surfing were reported by third persons, i.e. they witnessed someone observing the screen of another person without consent. Afternoon (N=3) was the most reported time of the day of shoulder surfing incidents followed by mornings (N=2) and evenings (N=1). Public transport (N=5) was once again mentioned as the shoulder surfing location incident followed by workplaces (N=1). Participants described the act of observing as *"peeking at CAS's cellphone"* (P3) or as *"..looking at someone else's device ..."* (P7) (N=5). Participants reported that the users of the devices did not notice being observed in 83.33% of stories. Participants considered curiosity (N=3) and boredom (N=3) as the reasons for observation. Smartphones were once again found to be the most shoulder surfed devices (N=5) followed by tablet-PCs (N=1). Participants mentioned that the relations between users and observers were observed to be strangers in four stories, friends in one story, and colleagues in one story. Further, participants were inquired to report on how many people were involved in the situation. Two people were reported to be involved in five stories and three people in one story. Stories from 3rd person perspectives further contributed to the exploration around **RQ 1**.

Key Take Away #3: Our results indicated that shoulder surfing often goes unnoticed by the victim user. It mostly happens in public transport followed by workplaces. Smartphones are the most commonly observed devices. Observers' way of observing is similar to peeking at someone's device i.e. a quick look.

6 DISCUSSION

In this section, we discuss the results of the diary study with 23 participants that guide us towards context-aware and configurable content-based shoulder surfing protection. Based on the results, we discuss possible future research directions.

6.1 Shoulder Surfing in Everyday Life - An Overview

The diaries showed that participants experienced shoulder surfing at least twice during the study period. The highest reported number of shoulder surfing stories was 8 in a day with 13 being the highest reported incidents by single participant during the study period. Based on the results of the diary study, shoulder surfing in everyday life can be summarized as below:

Who is the shoulder surfer? Strangers may observe a user's screen in public places, such as public transport. Friends or colleagues may observe a user's screen in social gatherings. Family members may observe the screen in private environments.

What does the shoulder surfer benefit from? Strangers may observe the user's screen as it appears to be in their line of sight or due to boredom. Friends and colleagues may observe due to curiosity or common interests. Family members may also observe due to curiosity. The shoulder surfer may try to obtain personal and sensitive information through observation.

What capabilities does the shoulder surfer has? The shoulder surfer is close to the user and is often found as "looking over" "staring", or "peeking" at mostly smartphones. The shoulder surfer may try to obtain personal and sensitive information by observing the screen content such as photos, messages, emails, video calls, games, or social media content. A more powerful shoulder surfer may try to carry out the observation for a longer period or may join hands with other shoulder surfers to carry out the observation attack; making it a multiple observation.

6.2 The Prevalence of Content-Based Shoulder Surfing

Shoulder surfing is a threat targeting two aspects; 1) security, and 2) privacy. While the security attack utilizing shoulder surfing is frequently investigated in security literature [28, 38, 50], privacy attacks resulting from shoulder surfing are less investigated but more frequently experienced by users [13, 16]. The security aspects

of shoulder surfing look into protecting authentication information such as PINs and passwords [2]. With the advancement in technology, we have biometric systems such as fingerprint authentication [4] or EOG-based authentication [38] that offer protection against shoulder surfing while maintaining system usability and requiring less user effort. On the other hand, privacy aspects of shoulder surfing look into protecting the visual privacy of the content found on devices such as gallery photos. While multiple mechanisms have been proposed for content-based shoulder surfing, which mechanism is most suitable and socially acceptable is unexplored. Hence, the issue of content-based shoulder surfing remains unsolved. During our study period, participants only experienced content-based shoulder surfing, and each participant experienced it at least twice. Further, the highest number of reported shoulder surfing incidents in a single day was 8. Previous work also recorded content-based shoulder surfing incidents more than authentication-based shoulder surfing incidents [13]. Privacy aspects of shoulder surfing are crucial to address as privacy is for everyone and a right of every user. Privacy is the liberty to share what the users wish and with whom the users prefer in different situations [10, 48]. Privacy provides a personal space that is vital for human growth [9]. The following user quotes from the diaries explain the user perception of content-based shoulder surfing:

"... It felt very awkward and then I just lowered my phone's brightness and stopped texting." (P5)
"... the people next to me keep staring at my mobile phone, which makes me uncomfortable." (P3)
"... It's very unacceptable for someone to peek into your privacy." (P2)
"... I cover it with my hand and probably walk away." (P18)

The liberty of privacy is the supreme reason for investigating shoulder surfing and designing user-centred solutions to combat shoulder surfing. Similar to authentication scenarios, content-based shoulder surfing is also a breach of users' privacy as highlighted by our participants and is a cause of discomfort. This discussion addresses **RQ 3**.

Q. What shoulder surfing protection mechanisms are socially acceptable by users?

6.3 Principal Lesson Learned

Shoulder surfing is not only limited to public environments [13, 43] but its evidence is also found in private environments as seen in the results of the diary study and prior literature [20]. However, most shoulder surfing takes place on public transport. Shoulder surfing is mostly done by friends followed by strangers and during nighttime.

Smartphones, due to their ubiquity, are the most shoulder surfed device [13]. The content found to be most shoulder surfed is dominated by messaging (N=13), games (N=8), emails (N=7), social media (N=4), and video calls (N=1). Shoulder surfing stories captured in our study inferred various content types. To offer protection against the shoulder surfed content, social aspects need to be considered such as the user-observer relationship. As shown in the results, users prefer different mechanisms for different user-observer relationships. This is because the need to protect shoulder surfed content varies with the relationship between the observer and the user [16]. The design of future shoulder surfing protection mechanisms should consider the relationship with the observer and the content types.

The diaries reveal that it is during casual activities when shoulder surfing mostly happens such as *"having lunch"*, *"watching TV"* and alike. Due to casual activities, shoulder surfing is commonly due to common interest, curiosity, or boredom. Despite this, it is still not preferred by the users as it is similar to invading the personal space [13]. Our diary study participants held the view that the task being carried out on the device was important. Some participants also mentioned the loss of device interaction time due to the privacy invasion.

The diaries also provide evidence of multiple people being involved in shoulder surfing incidents. For example, two people were reported to be involved in N=5 stories and three people were involved in N=4 stories. This directs us to include observations not only by a single observer but also by multiple observers. Shoulder surfing by multiple observers has been studied in prior work and it was found that multiple observers are better at guessing passwords as compared to a single observer [25]. However, that study was only limited to passwords rather than device content.

The "Nothing to report Stories" direct us in two directions: (1) shoulder surfing did not happen, (2) it happened but the participant did not notice. The higher number of stories from observers suggests that shoulder surfing is often unnoticed and thus more attacker than user stories are reported. Similar observation can be made from previously reported logs of shoulder surfing [13]. Goucher et al. [18] suggest that shoulder surfing often goes unnoticed due to the user's involvement with the task being carried out on the device. Overall, it should be noted that we collected shoulder surfing stories from western culture. The perception of shoulder surfing may vary as we move across different cultures. Our study provided a holistic view of everyday occurrences of shoulder surfing. The results can be seen as the current situation around shoulder surfing. The next step involves looking into the future of shoulder surfing i.e. what happens after shoulder surfing - the aftereffects of shoulder surfing.

Q. Does realizing being shoulder surfed impact the user's device interaction and task completion?
Q. Why does shoulder surfing often go unnoticed?

6.4 Single or Multiple Mechanisms for Content-Based Shoulder Surfing?

A huge range of content is found on smartphones that is prone to shoulder surfing. For example, in our study, participants reported photos, emails, games, social media, and messages amongst the numerous shoulder surfed content. Our study also showed that participants prefer mechanisms to protect their privacy. On the other side, content requiring protection against shoulder surfing needs to be prioritized since there exists so many content types, having a mechanism applied on all content types may hinder user experience [32] and system usability [5]. Farzand et al. [17] developed a typology of perceived privacy sensitive content in shoulder surfing scenarios highlighting what content needs to be protected

most. The next step in this direction is to discover if the same mechanism can be used across all content types or if preference for a mechanism varies with the content type.

Q. Does different content require different types of protection mechanisms?

6.5 Context-Aware & Configurable Shoulder Surfing Protection Mechanisms

The relationship closeness scale helped in grouping various shoulder surfers based on their closeness of relationship with the user. Relationship with the observer appeared to be an important aspect of selecting protection mechanisms as shoulder surfing can give rise to awkward situations and impact close relationships [13, 16]. The observers were grouped into three groups; 1. strangers (not at all close), 2. friends (moderately close), and 3. family (very close). While users' preference for mechanisms varied for strangers, it shows that any mechanism delivering protection is suitable in the case of a stranger shoulder surfer. However, since anyone can be the shoulder surfer, the mechanism for protection against friends and family is selective and highly dependent on the user. Overall, unobtrusive mechanisms that do not interrupt the device interaction were favoured by the participants. When it comes to context-aware and configurable shoulder surfing protection, here arises another important research question:

Q. How can the user-observer relationship information be used to inform the design of shoulder surfing protection mechanisms?

6.6 Detecting Shoulder Surfing

Mitigating shoulder surfing requires successful detection of shoulder surfing as the first step. Bâce et al. [3] recently proposed a novel mechanism to detect shoulder surfing, PrivacyScout, that uses visual features from the face detected by the front camera of smartphones. However, this approach was evaluated in lab-based settings. It is yet to be explored how well this approach can work in the wild. On a general level, shoulder surfers can be detected in two ways; using face detection [11] and through gaze estimation [42]. Face detection works on the principle of notifying the user of shoulder surfing as soon as an extra face is detected. This approach is ineffective as it is not always true that the extra face detected is a shoulder surfer. On the other side, gaze estimation is a promising approach [42] but brings along the challenge of bystander gaze privacy issues [24]. This challenge is currently under exploration and needs to be addressed for successful mitigation of shoulder surfing. We re-emphasize the importance of research on the detection of shoulder surfing.

Q. When detecting bystanders, how can we preserve the gaze privacy of the bystander?

7 CONCLUSION

Privacy preferences vary from user to user which makes it difficult to achieve standard privacy protection for all users. To offer personalized privacy protection against shoulder surfing, we revisited the important line of research and conducted a diary study (N=23) to explore in-depth the day-to-day shoulder surfing incidents. Our results say that content-based shoulder surfing is more frequent than authentication-based shoulder surfing and it mostly happens in public environments and is also reported in private environments. Users wish to opt for a mechanism that is tailored to their needs and preference for hiding the content. By analysing the results, we presented an overview of everyday shoulder surfing. We argue that social aspects and personal privacy preferences should be considered when designing effective and usable mechanisms against shoulder surfing. Based on the findings, we present research directions to be investigated to protect user privacy from everyday visual privacy invasions.

ACKNOWLEDGMENTS

This publication was supported by an Excellence Bursary Award by the University of Glasgow, by an EPSRC New Investigator Award (grant number EP/V008870/1), and by the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which is also funded by the UK EPSRC under grant number EP/S035362/1. Figure 1 was created using Canva [7] under Free Content License.

REFERENCES

[1] Andy Alaszewski. 2006. *Using diaries for social research.* Sage.
[2] Adam J Aviv, John T Davin, Flynn Wolf, and Ravi Kuber. 2017. Towards baselines for shoulder surfing on mobile authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference*. 486–498.
[3] Mihai Bâce, Alia Saad, Mohamed Khamis, Stefan Schneegass, and Andreas Bulling. 2022. PrivacyScout: Assessing Vulnerability to Shoulder Surfing on Mobile Devices. *Proceedings on Privacy Enhancing Technologies* 1 (2022), 21.
[4] 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).
[5] John Brooke. 1996. Sus: a "quick and dirty'usability. *Usability evaluation in industry* 189, 3 (1996).
[6] 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.
[7] Canva. 2022. Canva. https://www.canva.com
[8] Caroline Claisse, Bakita Kasadha, Simone Stumpf, and Abigail C Durrant. 2022. Investigating Daily Practices of Self-care to Inform the Design of Supportive Health Technologies for Living and Ageing Well with HIV. In *CHI Conference on Human Factors in Computing Systems*. 1–19.
[9] Julie E Cohen. 2013. What privacy is for. https://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf Retrieved Aug 17, 2021.
[10] Mary J Culnan and Pamela K Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science* 10, 1 (1999), 104–115.
[11] Google Developers. 2022. Detect faces with ML Kit on Android. https://developers.google.com/ml-kit/vision/face-detection/android Retrieved June 08, 2022.
[12] Jayson L Dibble, Timothy R Levine, and Hee Sun Park. 2012. The Unidimensional Relationship Closeness Scale (URCS): Reliability and validity evidence for a new measure of relationship closeness. *Psychological assessment* 24, 3 (2012), 565.
[13] 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.
[14] Malin Eiband, Emanuel von Zezschwitz, Daniel Buschek, and Heinrich Hußmann. 2016. My scrawl hides it all: protecting text messages against shoulder surfing with handwritten fonts. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. 2041–2048.
[15] Felix Anand Epp, Anna Kantosalo, Nehal Jain, Andrés Lucero, and Elisa D Mekler. 2022. Adorned in Memes: Exploring the Adoption of Social Wearables in Nordic Student Culture. In *CHI Conference on Human Factors in Computing Systems*. 1–18.
[16] Habiba Farzand, Kinshuk Bhardwaj, Karola Marky, and Mohamed Khamis. 2021. The Interplay between Personal Relationships & Shoulder Surfing Mitigation. In *Proceedings of the Mensch und Computer 2021 (MuC '21)*.
[17] 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. In *Proceedings*

of the Eighteenth USENIX Conference on Usable Privacy and Security. USENIX Association, USA.
[18] Wendy Goucher. 2011. Look behind you: the dangers of shoulder surfing. *Computer Fraud & Security* 2011, 11 (2011), 17–20.
[19] Greg Guest, Emily Namey, and Mario Chen. 2020. A simple method to assess and report thematic saturation in qualitative research. *PloS one* 15, 5 (2020), e0232076.
[20] 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.
[21] Michael Hölzl, Michael Roland, and René Mayrhofer. 2017. Real-world Identification for an Extensible and Privacy-preserving Mobile eID. In *IFIP International Summer School on Privacy and Identity Management*. Springer, 354–370.
[22] HP. 2020. Stop shoulder surfers with the HP EliteBook x360. https://www.linkedin.com/posts/activity-6544966289893408768-jLDf Retrieved February 11, 2021.
[23] Jette Hyldegård. 2006. Using Diaries in Group Based Information Behavior Research: A Methodological Study. In *Proceedings of the 1st International Conference on Information Interaction in Context* (Copenhagen, Denmark) *(IIiX)*. Association for Computing Machinery, New York, NY, USA, 153–161. https://doi.org/10.1145/1164820.1164851
[24] 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.
[25] Mohamed Khamis, Linda Bandelow, Stina Schick, Dario Casadevall, Andreas Bulling, and Florian Alt. 2017. They are all after you: Investigating the Viability of a Threat Model that involves Multiple Shoulder Surfers. In *Proceedings of the 16th International Conference on Mobile and Ubiquitous Multimedia*. 31–35.
[26] 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.
[27] Mohamed Khamis, Habiba Farzand, Marija Mumm, and Karola Marky. 2022. DeepFakes for Privacy: Investigating the Effectiveness of State-of-the-Art Privacy-Enhancing Face Obfuscation Methods. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces* (Frascati, Rome, Italy) *(AVI 2022)*. Association for Computing Machinery, New York, NY, USA, Article 21, 5 pages. https://doi.org/10.1145/3531073.3531125
[28] Mohamed Khamis, Karola Marky, Andreas Bulling, and Florian Alt. 2022. User-centred multimodal authentication: securing handheld mobile devices using gaze and touch input. *Behaviour & Information Technology* (2022), 1–23.
[29] Shamus Khan. 2020. Erving Goffman, The Presentation of Self in Everyday Life (1959). *Public Culture* 32, 2 (2020), 397–404.
[30] Katharina Krombholz, Heidelinde Hobel, Markus Huber, and Edgar Weippl. 2015. Advanced social engineering attacks. *Journal of Information Security and applications* 22 (2015), 113–122.
[31] Karen Lander, Vicki Bruce, and Harry Hill. 2001. Evaluating the effectiveness of pixelation and blurring on masking the identity of familiar faces. *Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition* 15, 1 (2001), 101–116.
[32] Bettina Laugwitz, Theo Held, and Martin Schrepp. 2008. Construction and evaluation of a user experience questionnaire. In *Symposium of the Austrian HCI and usability engineering group*. Springer, 63–76.
[33] 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* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, Article 589, 13 pages.
[34] Philipp Mayring et al. 2004. Qualitative content analysis. *A companion to qualitative research* 1, 2 (2004), 159–176.
[35] 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.
[36] Ildar Muslukhov, Yazan Boshmaf, Cynthia Kuo, Jonathan Lester, and Konstantin Beznosov. 2013. Know your enemy: the risk of unauthorized access in smartphones by insiders. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*. 271–280.
[37] Qualtrics. 2021. 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, 2021.
[38] Kirill Ragozin, Karola Marky, Jie Lu, and Kai Kunze. 2022. EyeMove-Towards Mobile Authentication using EOG Glasses. In *Augmented Humans 2022*. 10–14.
[39] Kirill Ragozin, Yun Suen Pai, Olivier Augereau, Koichi Kise, Jochen Kerdels, and Kai Kunze. 2019. Private reader: Using eye tracking to improve reading privacy in public spaces. In *Proceedings of the 21st International Conference on Human-Computer Interaction with Mobile Devices and Services*. 1–6.
[40] John Rieman. 1993. The diary study: a workplace-oriented research tool to guide laboratory efforts. In *Proceedings of the INTERACT'93 and CHI'93 conference on Human factors in computing systems*. 321–326.
[41] 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.
[42] Alia Saad, Dina Hisham Elkafrawy, Slim Abdennadher, and Stefan Schneegass. 2020. Are they actually looking? identifying smartphones shoulder surfing through gaze estimation. In *ACM Symposium on Eye Tracking Research and Applications*. 1–3.
[43] 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. (2021).
[44] Mennatallah Saleh, Mohamed Khamis, and Christian Sturm. 2019. What About My Privacy, Habibi?. In *IFIP Conference on Human-Computer Interaction*. Springer, 67–87.
[45] Wally Smith, Greg Wadley, Sarah Webber, Benjamin Tag, Vassilis Kostakos, Peter Koval, and James J Gross. 2022. Digital Emotion Regulation in Everyday Life. In *CHI Conference on Human Factors in Computing Systems*. 1–15.
[46] Roger Tourangeau and Ting Yan. 2007. Sensitive questions in surveys. *Psychological bulletin* 133, 5 (2007), 859.
[47] 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.
[48] Alan F Westin. 1968. Privacy and freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.
[49] Julie R Williamson. 2012. *User experience, performance, and social acceptability: usable multimodal mobile interaction*. Ph.D. Dissertation. University of Glasgow.
[50] Xingjie Yu, Zhan Wang, Yingjiu Li, Liang Li, Wen Tao Zhu, and Li Song. 2017. EvoPass: Evolvable graphical password against shoulder-surfing attacks. *Computers & Security* 70 (2017), 179–198.
[51] 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.

A DIARY STUDY FORMAT

In this section, we present the diary format used in Study I. Use the below space to record your recent experience of unnoticed observations on personal devices (such as smartphone, laptop, tablet etc). You are required to make a note of every incident when you found someone related/unrelated to you looking over on your personal device (such as a smartphone etc) without your permission or when you encountered a situation where you had a chance to look over someone's personal device (such as smartphone/laptop) without being noticed by them. You may be a third person who observed the observer and the observee.

A pictorial example is also shown below for the clearer meaning. In this sketch, you see Cas and Vic. Cas is using a mobile device (like a smartphone or tablet) and is **not aware** of Vic looking and seeing what's on the screen of the device (e.g. text, pictures, passwords/PINs, maps, videos, apps, games, websites etc.). To help you get started with noting down, here are some clues you might consider: time, location, the task involved, relationship with the observer etc.

Please answer the following questions in regards to your experience which you just logged on the previous page

(1) *"The task that was being carried out on the device was important"*
(2) How many people (excluding you) were involved in the event?
(3) How would you describe the relationship between yourself and the observer/observee? (e.g., family member, friend, stranger)

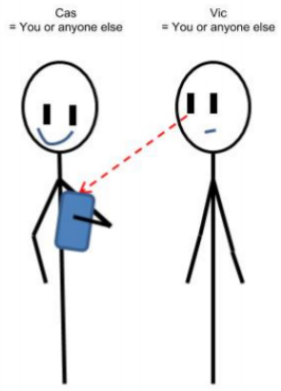

Figure 4: (The image was taken from the work by Eiband et.al. [13] on shoulder surfing to better illustrate the meaning of shoulder surfing.)

(4) Considering the relationship identified in the previous question, answer the following questions (strongly disagree to strongly agree):
   (a) My relationship with my ..... is close.
   (b) When we are apart, I miss my ..... a great deal.
   (c) My ..... and I disclose important personal things to each other.
   (d) My ..... and I have a strong connection.
   (e) My ..... and I want to spend time together.
   (f) I'm sure of my relationship with my .....
   (g) My ..... is a priority in my life.
   (h) My ..... and I do a lot of things together.
   (i) When I have free time I choose to spend it alone with my .....
   (j) I think about my ..... a lot.
   (k) My relationship with my ..... is important in my life.
   (l) I consider my ..... when making important decisions.

(5) Were you the observer, the observee, or a third person?

(6) *"A significant amount of time was wasted due to the observation of my interaction with the device"*

(7) *"I would like my device to have a mechanism to detect, react, and alert in similar situations like this"*

(8) What would you like the device to do?

(9) *"Having such a mechanism will impact my relationship with the observer"*

(10) How do you think having such a mechanism will impact your relationship in any way?

(11) Below are some examples of proposed mechanisms. Please choose the one which you think would be most suitable to have in the situation you described earlier.

(12) *"The selected method is adequate for use in the situation I described earlier"*

(13) In your opinion, who should be in control of activating this mechanism?
   (a) User
   (b) The User Interface
   (c) Both

(14) Why do you think the selected method is most appropriate in your situation?

(15) Would you like to amend the selected mechanism in any way?

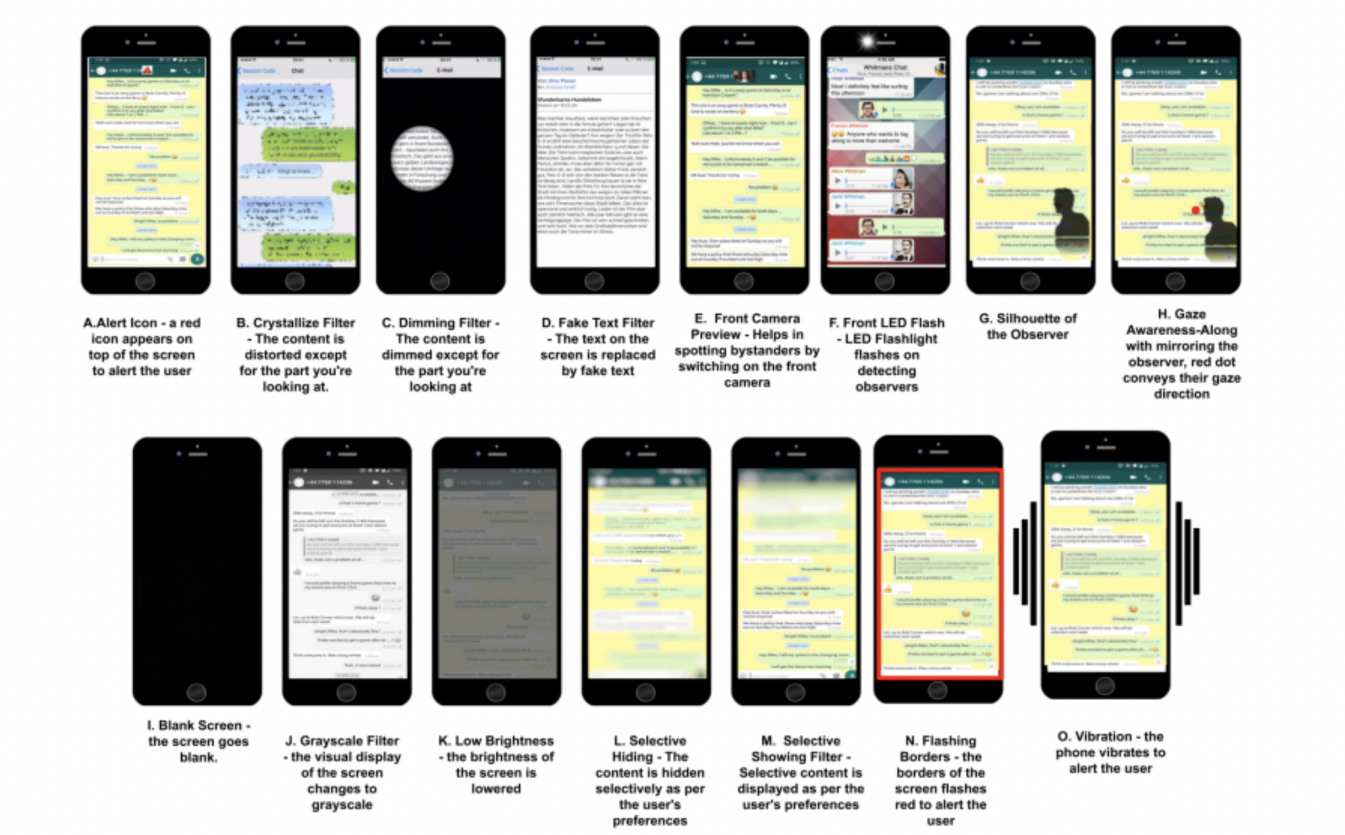

Figure 5: Presented Mechanisms to choose from that either alert the user giving the choice to the user to decide if he wants to have protect the view or mitigating the shoulder surfed content by applying an overlay or a filter

B CODEBOOK FOR THE DIARY STUDY

In this section, we provide the codebook used during the diary study analysis.

Category	Code	Description & Examples
Location	Public Transport	A mode of transportation such as bus, train, taxi and alike
	Work	Workplace such as "office"
	Narrow/Crowded Place	Locations with dense number of people such as "malls"
	Cafe/Bar/Restaurant	Social hangout places such as cafe, pub, bar, or restaurant
	Personal environment	Private environment such as "home"
Time of Day	Morning	Time between 04:00 and 11:59 such as 06:27, 08:16
	Afternoon	Time between 12:00 to 17:00 such as 12:55, 14:29
	Evening	Time between 17:00 and 20:00 such as 18:15
	Night	Time between 20:00 and 04:00 such as 8-9PM
User & Observer Activity	Chatting	The act of verbal conversation such as "talking"
	Watching TV	The act of watching television,
	Playing game	The act of playing game
	Lunching/Dinning	The act of having food
	Checking phones	The act of navigating the screen of phones such as "checking phone", "looking at phone"
	On the way	The act of commuting such as riding the train, sitting in the bus
Observer Motivation	Boredom	Boredom describing words such as "bored"
	Curiosity	Curiosity describing words such as "curiosity"
	Line of sight	Referring to line of sight such as "was shown and line of sight"
	Common Interest	Interest describing phrases such as "interesting", "common interest in game"
Action of Observation	Peeking	Act of quickly looking such as "peeking"
	Looking over	Phrases describing the observation such as "watching", "looked", "look- ing over"
	Snooping	Act of trying to find out something such as "snooping"
	Leaning over	Describing the positioning of the observer such as "leaning over the front of the seat"
	Sneak a peak	A secretive look such as "peek into privacy"
	Starring	A fixed look such as "starring"
Reaction	Angry	Feeling or showing annoyance such as "angry"
	Uneasy	Causing or feeling discomfort such as "uneasy"
	Uncomfortable	Causing or feeling awkward such as "makes me uncomfortable"
	Lowered Brightness	Act of decreasing brightness of the screen such as "lowered my phone's brightness"
	Feeling bad	A non-appreciative feeling such as "Felt bad but couldn't help"
Device	Smartphone	Describing smartphones such as mobile, phone
	Tablet	Describing tablet such as "tablet"
Activity on Device	Reading	Act of reading such as "reading something"
	Scrolling	Act of navigating screens of the device such as "checking messages"
	Texting	Action of sending messages on smartphone such as "texting"
	Video call	Call made with a camera and a screen such as "Zoom meeting"
	Playing game	Act of1p8laying game such as "playing game"

Table 1: Codebook used to analyze the Diary Study (1/2)

Category	Code	Description & Examples
Application on Device	Email	Email application such as "reading email"
	Messaging	Messaging application such as "Checking messages"
	Texting	Any messaging platform such as "texting"
	Video call	Application offering call services with a camera and a screen such as "Zoom" (video call)
	Social Media	Social media applications such as "Facebook", "YouTube" and alike
	Gallery	The photos application on the phone such as "photo album"
	Game	Gaming applications such as "playing game"
Proposed Features of Mechanisms	Alert	Quick notice such as a "warning"
	Blurry	Unclear such as "blurry"
	Automatic Lock	Involving no direct human control such as "automatic screen lock"
	Remind	Causing to remember such as "remind me that someone is watching my screen"
	Unsure	Uncertain such as "not sure"
Mechanism Impact on Relationship	Not matter	Conveying unimportant such as "it does not matter"
	Privacy Protection	Privacy defence such as "maintain my privacy"
	Positive	Contentment such as "happy"
Mechanism Execution	Less Notifications	Low number of notifications such as "Too many triggering points..might get annoyed"
Mechanism Visualization	Blurring	Making unclear such as "blur faces"

Table 2: Codebook used to analyze the Diary Study (2/2).