The Interplay between Personal Relationships & Shoulder Surfing Mitigation

HABIBA FARZAND, KINSHUK BHARDWAJ, KAROLA MARKY, and MOHAMED KHAMIS,
University of Glasgow, UK

Shoulder surfing refers to observing someone's device screen without their consent. Conspicuously switching off the screen upon noticing a friend observing private messages may create an embarrassing situation. Initial evidence indicates that users adopt strategies to mitigate shoulder surfing based on their relationship to the observer. However, the social implications of such mitigation strategies remain largely unexplored. We present findings from an interview study with 12 participants to address this. We analyze experiences with shoulder surfers of different relationships to the user and collect feedback on eleven state-of-the-arts strategies for mitigating shoulder surfing. We show that the user-observer relationship impacts the choice of mitigation methods and that users often do not want observers to know they were caught. Based on our results, we conclude with implications for designing socially acceptable privacy protection mechanisms on mobile devices.

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy**.

Additional Key Words and Phrases: shoulder surfing, privacy, security

ACM Reference Format:
Habiba Farzand, Kinshuk Bhardwaj, Karola Marky, and Mohamed Khamis. 2021. The Interplay between Personal Relationships & Shoulder Surfing Mitigation. In *Mensch und Computer 2021 (MuC '21), September 5–8, 2021, Ingolstadt, Germany*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3473856.3474006

1 INTRODUCTION

The ubiquity of mobile devices brings a lot of benefits to users, but it also exposes them to shoulder surfing. Shoulder surfing – a physical type of social engineering attacks [13] – refers to the act of observing the device screen of other people without their permission [5]. Shoulder surfing can occur anywhere where a device is used due to which anyone can be the shoulder surfer, such as strangers, family members, friends, colleagues, or intimate partners [5, 16, 18]. While shoulder surfing has been studied extensively by the HCI and security communities [4, 5, 14, 24], an under-investigated question is if the user's reaction to shoulder surfing is impacted by their relationship to the observer. For example, it is unclear whether users would still take actions to protect their privacy even if this could damage their relationship to the observer, who could be a friend, partner or work colleague. Addressing this gap is important; adverse effects on relationships could reduce adoption of mitigation methods which would in turn put user's privacy at risk. To understand the interplay between relationships and shoulder surfing, we conducted semi-structured interviews with 12 participants to study their perspectives on shoulder surfing impacting relationships, both as observers and users. The interview questions were grouped as 1) perspectives and past experiences on shoulder surfing impacting relationships, 2) perceived social implications of selective shoulder surfing mitigation strategies. For the second part, we selected eleven recent shoulder surfing mitigation methods proposed by HCI and security researchers [9, 21, 25].

The **contribution** of this work is threefold: 1) We show empirical evidence that user-observer relationship impacts choice of mitigation methods, 2) we discuss the social acceptability of 11 mitigation methods, and 3) we derive design implications for relationship-based shoulder surfing resilience methods for future research.

MuC '21, September 5–8, 2021, Ingolstadt, Germany

2 RELATED WORK

2.1 Relationships & Shoulder Surfing

Most related to our work is that of Eiband et al. [5] who reported surveying 174 participants on their experiences with shoulder surfing as users, as observers, and as bystanders. They found evidence that shoulder surfing occurs in daily scenarios but often goes unnoticed. Most of the captured cases were opportunistic rather than malicious but still had negative consequences. One of the main findings from their survey was the preliminary evidence that the way users cope with shoulder surfing seem to depend on observers. For instance, one participant responded humorously to shoulder surfing by their partner, whereas those observed by strangers often switched off the screen or hid the phone.

Further research showed that users are concerned about unauthorized access by certain relationships. For example, Muslukhov et al. found through interviews and a survey that users are highly concerned by unauthorized access by insiders, such as friends and family [18]. In a survey by Marques et al. where they asked people to report on shoulder surfing incidents that involved someone they knew [16] and reported that the majority of cases involved the user's intimate partner (58%), whereas 24% of shoulder surfers were friends, 9% were family members, and 9% were co-workers. Similarly, Eiband et al. reported that out of 170 experiences of shoulder surfing, the observers were strangers in 126 experiences, followed by friends (N=11), acquaintances (N=10), colleagues (N=8), family (N=3), partners (N=3), and others (N=9) [5]. While prior work showed an association between relationships and the frequency of shoulder surfing, our work focuses on studying how relationships impact strategies users are willing employ against shoulder surfing.

2.2 Shoulder Surfing Mitigation Mechanisms

Users of mobile devices protect themselves from shoulder surfing by tilting the device [5, 12], turning off the screen [5], or using privacy screens that block viewing from certain angles [19]. Tilting was shown to be ineffective, as it prevents bystanders from shoulder surfing PINs only at 70 degrees or higher [12]. Privacy screens are also not effective at several angles [19]. Researchers have proposed alternative methods to resist shoulder surfing such as by distorting sensitive pictures [23], or customizing fonts to be unreadable by bystanders [6]. Both approaches above make the content less clear to observers but understandable by users. Other approaches hide the content completely, such as EyeSpot [9] and PrivateReader [20] which only show content the user gazes at. Zhou et al. [25] and Saad et al. [21] compared the design of multiple widgets to communicate to users that a shoulder surfer is present, or to mitigate shoulder surfing. These methods assume a shoulder surfer has been detected, for example, by head pose estimation [1], or eye tracking [8].

The above works focused on protecting users of mobile devices from shoulder surfing of content such as text, pictures, etc. A large proportion of shoulder surfed content are authentication credentials (e.g. PINs and usernames/passwords) [5]. Hence, a large body of work addressed shoulder surfing of authentication [2, 3, 10, 11, 22].

A mitigation mechanism that is both usable and secure may still be less likely to be employed by users if they find it too embarrassing to use, if it has negative social implications, or if it impacts their relationships with their peers. This underlines the need to understand the social acceptability of these mechanisms. We fill this gap by studying how the user-observer relationship impacts the shoulder surfing mitigation strategy and the social viewpoint of 11 mechanisms (detailed in next section) for mitigating and alerting from shoulder surfing.

3 METHODOLOGY

To address the identified gap, we conducted semi-structured interviews with 12 English speaking participants (M=6, F=6; self identified) recruited through word of mouth, aged 20-48 years (M=25, SD=8).

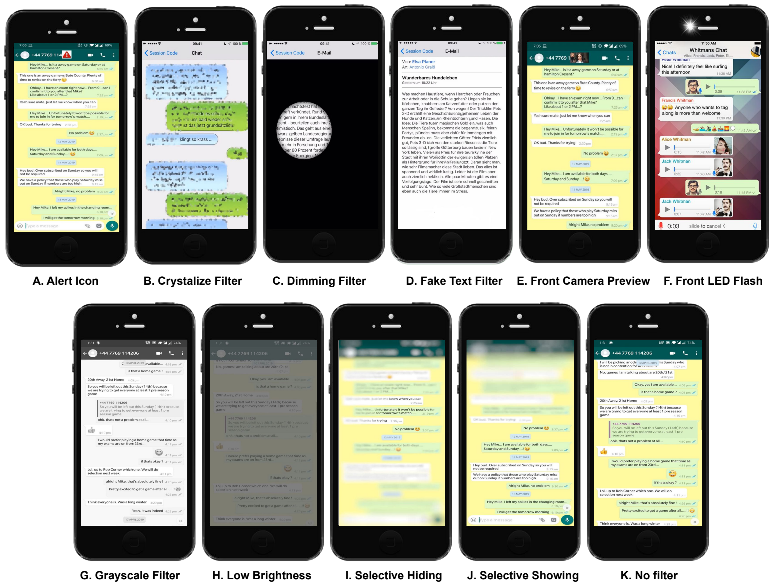


Fig. 1. Eleven alerting and mitigating methods from prior work [9, 21, 25] that we considered in our study.

Procedure. The interview aimed to understand 1) observers' and users' perspective on shoulder surfing and its impact on relationships, 2) existing solutions in use to deter shoulder surfing, 3) possible future solutions against shoulder surfing in the user's opinion, and 4) views about 11 state-of-the-art mechanisms to deal with shoulder surfing (see **supplementary material**). The study was approved by our Ethics committee. Eleven interviews were held face to face and one was held online in January 2020. First, the participants were asked to read and sign a consent form and a demographic questionnaire that collected information on participant's relationships. The responses to these questions helped us shape and personalize the questions of the interview. Two sets of the same interview questions were drafted: one covering the user perspective, and another set covering the observer perspective. Half participants started with the user set, while the other half started with the observer set to balance out potential sequential effects.Throughout the interview, examples were avoided to prevent confirmation biases. Participants were informed that the study explores how relationships are influenced by smartphone interactions. Negative terms like "shoulder surfing", "observers" were not used to avoid potential biases, e.g., social desirability bias [17].

Next, the participants were interviewed about the following specific mitigation mechanisms: 1) Alert Icon [21, 25] (Figure 2A), 2) Crystallize Filter [9] (Figure 2B), 3) Dimming Filter [9] (Figure 2C), 4) Fake Text [9] (Figure 2D), 5) Front Camera Preview [21] (Figure 2E), 6) Front LED Flash [21] (Figure 2F), 7) Grayscale [25] (Figure 2G), 8) Low Brightness [21] (Figure 2H), 9) Selective Hiding [25] (Figure 2I), 10) Selective Showing [25] (Figure 2J), and 11) No Filter (Figure 2K). The participants were shown videos that started with a scene of a person shoulder surfing another, and was followed by a video of the respective mitigation mechanism in action. The videos were played on the experimenter's laptop during the face to face interviews, and via screen sharing to the remote interviewee. 7 relationships were chosen based on shoulder surfing research [5, 16]: Parent, Child, Sibling, Partner, Friends, Professional Fellow, and Strangers.

Data Analysis. We employed methods inspired from grounded theory [7] for analysis as it allows discovering and constructing theory from data systematically. Three researchers worked together during data analysis. First, two researchers independently reviewed all transcripts and notes proposing a codebook. Next, they agreed on a final codebook. Second, a third researcher coded all interviews and transcripts by applying the codebook. Finally, similar topics of codes were related to each other through axial coding to develop overarching categories.

Limitations. Considering the aims of the study, sample specificity, quality of dialog, and analysis strategy, our sample size (N=12) was found suitable [15]. Only 7 out of 12 participants allowed audio recording of the interview. Though the researcher took notes but some details may have been missed. While the relationship can be the same across pairs of people, the closeness of relationship does not necessarily have to be the same. Our work undertakes the first exploratory step of identifying how the relationship type impacts choice of shoulder surfing mitigation methods, but we leave the study of other relationship factors open for future work.

4 FINDINGS & DISCUSSION

Perceived Sensitive Content. Participants' opinions about what content they would try to hide the most varied greatly. Memes (P1), posts with sexual content (P1,P5), banking details/apps (P2, P3), dating apps (P5), social media (P11), personal details (P9), pictures (P11, P12), and chat logs (P6, P11, P12) were found to be the most sensitive content. The types of content perceived to be most sensitive and most shoulder surfed are in line with previous work [5, 16]

Perception of Shoulder Surfing is Impacted by Relationships. Incidents in which certain relationship dynamics influenced the implications of shoulder surfing negatively and the means by which users react to it were reported. E.g., P1 narrated an incident where she was shoulder surfed by her uncle who was, in her case, an authoritative figure. Shoulder surfing by her uncle i.e. an authoritative person led to awkwardness and fight. In other cases, neither the user nor the observer had an authority. For example, P4 reported an experience where there was no power relationship between the user and the observer yet it caused an argument. P4 stated *"There was one more time him looking at mine, caused an argument one time but it wasn't intense"*. Shoulder surfing was reported to have negative social implications including fights, awkwardness, and arguments.

Not all Shoulder Surfers are Equal. Participants voiced that they are more uncomfortable when the shoulder surfer is an authoritative figure. P1 was particularly concerned about parents' shoulder surfing and outlined *"because sometimes I am saying rude things"*. P2 and P3 were concerned by strangers but not by friends. P7 expressed that he does not mind it when his parents shoulder surf him as he trusts them, but feels uncomfortable in the case of coworkers due to the dichotomy between personal and work-space, and was least comfortable with strangers due to lack of trust. P9 communicated that they are *"not comfortable with [being shoulder surfed by] parents"*. P11 voiced similar thoughts on discomfort when shoulder surfed by parents, but also by coworkers due to the differentiation between work and personal life and least comfortable with strangers. P8 and P10 stated they are least comfortable when shoulder surfed by strangers irrespective of content. Finally, P12 stated discomfort when shoulder surfed by academic fellows as they disliked them, and the highest discomfort when shoulder surfed by strangers due to the same reason as expressed by P11: lack of trust and importance of the privacy to the participant. Some participants expressed their concerns about their partners. P4's partner usually does not mind being shoulder surfed by P4, but in this particular scenario, P4 stated that *"it escalates because if you see things you don't understand and then ask questions and that comes in between you"*.

Participants Try to Hide Private Content in an Inconspicuous Way. Participants mentioned using different ways to cope with shoulder surfing. P1 uses a privacy screen protector that blocks observations from certain angles. P7 adjusts their position when being shoulder surfed. Similar to this strategy, P10 reported moving the screen away or covering it without the observer noticing. This is inline with previous work [5], which showed that people try to inconspicuously hide their private content. These measures are however limited. Tilting the phone or hiding it prevents the user from interacting, and privacy protection screens impact usability while not offering full protection [19].

Participants Propose Mechanisms that are Hard to Notice. When asked openly about what kind of mechanisms they prefer for dealing with shoulder surfing by someone related to them, five participants suggested a text message notification. P1 suggested a pop-up message *"because if I am looking at my screen [..] I will be able to see the pop-up message in that precise moment"*. Rather than a modification to the whole screen, P1 preferred a tiny sized notification [21] or a subtle change like applying a grayscale filter [25]. P2, P3, and P5 also suggested a pop-up or a text message. P6 preferred a notification of a blank new message. One participant expressed no need for a mechanism. P11 suggested vibrations could also be a way of alarming the user. Participants proposed mechanisms that are hard to notice so that it does not affect their interpersonal relationship with the observer.

Choice of Given Mechanisms for Family: Strategies to avoid shoulder surfing or alert users of it vary as the level of authority in the relationship changes. For authoritative family relationships like parents, the mechanisms; grayscale (P1, P10, P11), alert icon (P10, P11), fake text (P10), and low brightness (P10) were common choices. The reasons behind these choices included non-obviousness to the observer (P1), and being subtle and effective (P10). Other choices included low brightness, selective hiding, and selective showing (P11). Some participants also opted for no filter for parents as they have nothing to hide (P2, P10) and do not mind them looking over their screen (P12). For less authoritative observers like siblings and partners, choices ranged from the alert icon (P11), grayscale (P5, P6), crystallize filter (P5, P11), text message (P5), and dimming filter (P11). Dimming and crystallize filters were considered means for conveying to the sibling to stop the invasion of privacy (P11). One participant opted for no filter (P2).

Choice of Given Mechanisms for Friends: Level of understanding was found to be a consideration when opting for a suitable mechanism. P6 opted for Crystallize filter for friends and Grayscale for siblings. P6 clarified that their choice was because friends are able to quickly read through the screen as they are assumed to be more likely *"on the same level of understanding"* and crystallize filter would make it difficult for them to do so. Whereas, her sibling who is a child and shares a different level of understanding, will require some amount of time to read through the screen and hence, a less strict mechanism, i.e., Grayscale, would be appropriate. P11 found Dimming and Crystallize filters suitable for friends. P11 thought that noticeable filters communicate to observers that their act is not appreciated by the user.

Choice of Given Mechanisms for Professional Colleagues: Choices ranged from crystallized filter (P2, P11), text message/warning icon (P5), dimming (P11), to fake text (P12). Crystallize filter was preferred as shoulder surfers *"can't read anything"* (P2), and because like the dimming filter, the crystallize filter makes it obvious to the observer that their inappropriate action was detected (P11). Fake text was liked and found suitable because it displays irrelevant information in unavoidable situations due to mutual working space (P12).

Choice of Given Mechanisms for Strangers: Fake text was a commonly selected option for strangers as it would give strangers false and irrelevant information in unavoidable shoulder surfing situations. Several participants argued that it is best to let observers see irrelevant information (P10, P11, P12). Other choices for strangers included crystallize filter and front camera preview (P10). P10 also suggested that these mechanisms should be designed and incorporated in a way that they can be switched on and off to save the phone's battery.

Social Viewpoint of the Mechanisms. Methods for dealing with shoulder surfing can be classified to alerting and mitigation mechanisms. Some participants preferred being alerted and leaving it up to them to decide how to act. Others preferred systems that actively mitigate shoulder surfing by hiding content. Participants were more inclined towards alert mechanisms (22 votes): Alert Icon (10), Front Camera Preview (4), Front LED Flash (1), Fake Text (3), Gray Scale (2), Low Brightness (2). Fewer votes went to mitigation mechanisms (9 votes): Selective Hiding (1), Selective Showing (1), Crystallize Filter (5), Dimming Filter (2).

Overall, the alert icon was mainly selected for its *"discreetness"*, *"tiny sized"*, and as it *"was not something big as other mechanisms"*, implying that using unnoticeable methods is desired (P3, P4). It was also called *"ideal"* for not straining the eyes and suitable for scenarios where the participant is surrounded by known people (P9). A suggested modification in the Alert Mechanism was placing it in the notification bar so that it does not alert the observer but only the user (P9).

Unobtrusiveness was another considered factor when choosing mechanisms to protect against shoulder surfing. P7 liked front LED flash, front camera preview, and alert icon for all relationships as they are *"less intrusive and [more] useful"* in indicating that someone is looking over their shoulder. Customizable vibration patterns were proposed by P7 as an additional solution for alerting of shoulder surfing (P7). Concerns about limited viewing from certain angles were expressed for Dimming Filter (P8). For friends, siblings, and partners, any mechanism would be suitable according to P12 as only an alarm about the attack is needed to convey the message to the user. P12 was also apprehensive that these mechanisms could cause considerable *"strain on eyes"* and would *"hinder"* phone usage. To sum up, the alert icon, for its various characteristics was the most preferred the choice for many relationships.

Implications for Designing Shoulder Surfing Resilience Mechanisms for Mobile Devices.

(1) **Empower Users to deal with shoulder surfers the way they see fit**: The interplay between relationships and shoulder surfing differs greatly among people. Some find shoulder surfing by authoritative figures (e.g., parents) to be very uncomfortable, while others do not mind it. Users should be able to customize alerting and mitigating methods according to their needs.
(2) **Offer Alerting and Mitigation methods that are Unnoticeable by Shoulder Surfers:** Methods that are not obvious to the observer have several advantages: 1) they prevent potentially awkward situations or confrontations with the observer, and 2) they give the user more control of the situation; they can decide whether to subtly avoid or to engage with the observer. Thus, allowing users to choose an unnoticeable method may help them cope with some shoulder surfing scenarios.
(3) **Mechanisms should convey Privacy Invasion to Observers that are on Same Level of Understanding as Users:** Level of understanding plays a role when indirectly conveying privacy invasion to the observer such as when observed by friends.
(4) **Methods conveying Irrelevant Information to Observers into thinking their Observations were Successful are Needed:** Due to the incapacity of changing location in situations of shoulder surfing (e.g., in mutual work-spaces or public areas), it is useful to have mechanisms that convey irrelevant information (P12).

5 CONCLUSION

We presented results from 12 interviews that uncovered how relationships impact and are impacted by shoulder surfing, and most suitable relationship-based mitigation mechanisms. Users prefer non-obvious mechanisms for authoritative figures to avoid discomfort, screen distorting filters for siblings and friends to convey invasion of privacy, and conveying irrelevant information for professional fellows and strangers.

A QUESTIONNAIRE

A.1 Pre-Interview Questions

(1) Relationship status (e.g. married, divorced, in a relationship)
(2) Professional status (e.g. student, employed, retired, etc)
(3) Siblings: Yes/No
(4) Live with Parents: Yes/No

A.2 Interview Questions

A.2.1 Attacker's Perspective.

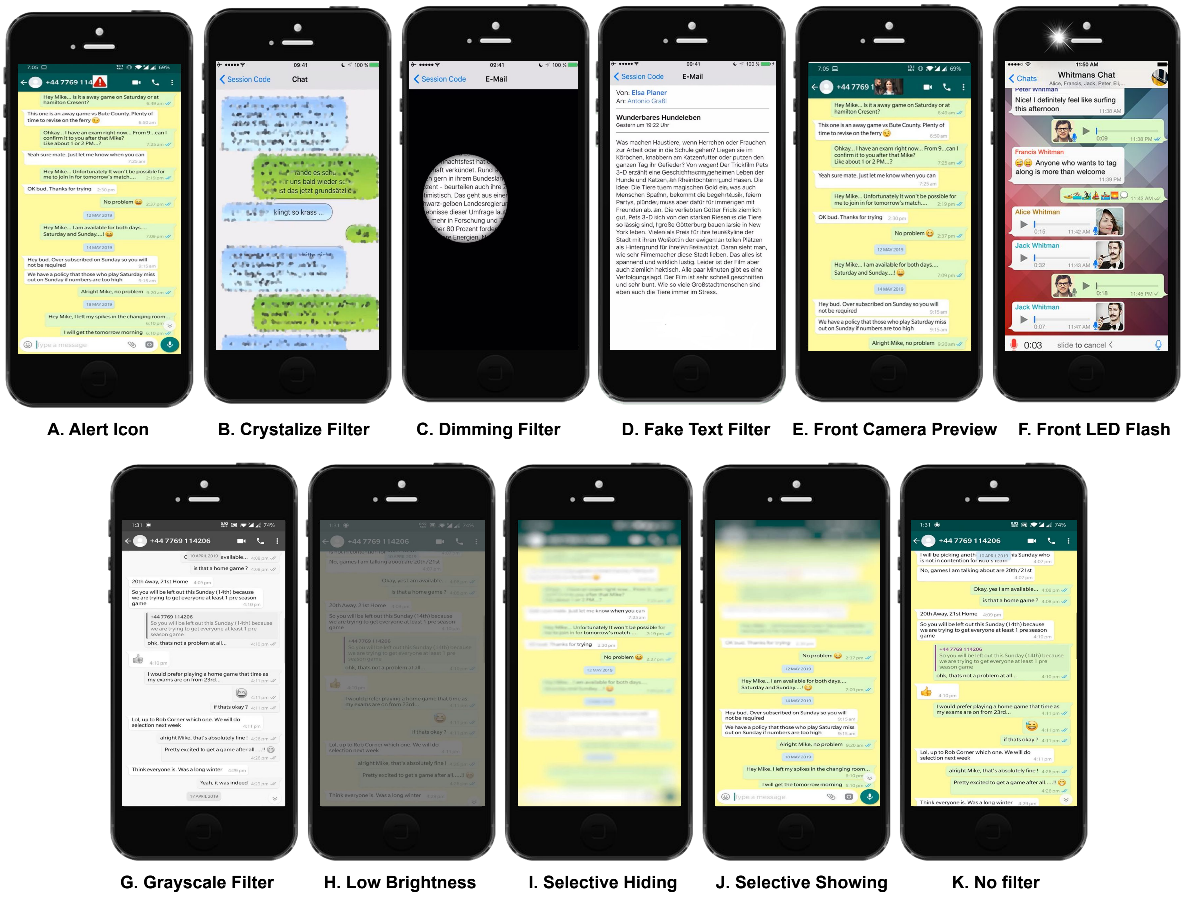
(1) Do you recall a situation where your (relation 1) was using a phone and they were not aware that you are able to see the content on the screen?
(2) Did your (relation 1) realize that you were looking over their phone? If yes, how did your (relation 1) respond?
(3) How did your (relation 1)'s reaction make you feel?
(4) How did you act to the reaction?
(5) Did you feel any change in your relationship with your (relation 1)?
(6) Do you worry about what the person would think about you when they see you looking at their phone?
(7) Has this situation or similar affected your relationship in any way in the past?
(8) Do you think such things affect relationships? What are your thoughts?

A.2.2 Victim's Perspective.

(1) Have you been in a situation where someone is looking over your phone?
(2) Does it concern you what (relation 1) would think about you by looking at your phone screen?
(3) Which relation from the following would make you the most uncomfortable if you see them looking at your phone while you are interacting with it?
    - Parent
    - Child
    - Sibling
    - Partner
    - Friends
    - Professional Fellow
    - Strangers
(4) What content would you hide the most or try to secure the most?
(5) How would you like your system to notify you about such a moment?

A.2.3 Selected Eleven Mechanisms Questions.

(1) If you find out your (relation 1) is looking over your phone, which mechanism would you opt to hide content?
    (a) Alert icon on top of the screen: as shown in Figure 1 A, a red icon appears on top of the screen to alert the user of the presence of a observer [21, 25]. This method *alerts* the user of observers but does not directly mitigate attacks.
    (b) Crystallize filter: a crystallize filter is applied on the content to distort it while maintaining contextual data (e.g., conversation bubbles and colors). The user's gaze point is used to reveal only the content the user is looking at as shown in Figure 1 B [9].
    (c) Dimming filter: as shown in Figure 1 C, the screen is dimmed except for the part the user is gazing at [9].
    (d) Fake text filter: the screen's content is replaced by fake text as shown in Figure 1 D [9].
    (e) Front camera preview on top of the screen: this allows the user to spot any bystanders as shown in Figure 1 E [21].
    (f) Front LED flash: the front LED flashes when a bystander is detected as shown in Figure 1 F [21].
    (g) Grayscale filter: the color of the screen's content is converted to grayscale as shown in Figure 1 G [25].
    (h) Lowering Brightness: the screen's brightness is reduced as shown in Figure 1 H [21].
    (i) Selective hiding: where the user selects the areas of the screen that they want to hide from the attacker as shown in Figure 1 I [25].
    (j) Selective showing: in contrast to the previous one, here the user selects the parts of the screen to be displayed and the rest of it would be blurred out as shown in Figure 1 J [25].



A. Alert Icon
B. Crystalize Filter
C. Dimming Filter
D. Fake Text Filter
E. Front Camera Preview
F. Front LED Flash
G. Grayscale Filter
H. Low Brightness
I. Selective Hiding
J. Selective Showing
K. No filter

Fig. 2. The Selected 11 Mechanisms

.

(k) No protection (baseline): The screen's content was not modified in any way as shown in Figure 1 K.

(2) Why do you think this would be the most appropriate choice?

(3) Would you like to modify this mechanism in any way?

ACKNOWLEDGMENTS

This publication was supported by the Excellence Bursary Award by University of Glasgow, the Royal Society of Edinburgh (Award number #65040), and by an EPSRC New Investigator Award (EP/V008870/1).

REFERENCES

[1] Mohammed Eunus Ali, Anika Anwar, Ishrat Ahmed, Tanzima Hashem, Lars Kulik, and Egemen Tanin. 2014. Protecting Mobile Users from Visual Privacy Attacks. In *Proc. of UbiComp '14 Adjunct* (Seattle, Washington) *(UbiComp '14 Adjunct)*. ACM, New York, NY, USA, 1–4.

[2] Andrea Bianchi, Ian Oakley, Vassilis Kostakos, and Dong Soo Kwon. 2010. The Phone Lock: Audio and Haptic Shoulder-Surfing Resistant PIN Entry Methods for Mobile Devices. In *Proceedings of the Fifth International Conference on Tangible, Embedded, and Embodied Interaction* (Funchal, Portugal) *(TEI '11)*. Association for Computing Machinery, New York, NY, USA, 197–200.

[3] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. 2011. Spinlock: A Single-Cue Haptic and Audio PIN Input Technique for Authentication. In *Haptic and Audio Interaction Design*, Eric W. Cooper, Victor V. Kryssanov, Hitoshi Ogawa, and Stephen Brewster (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 81–90.

[4] Leon Bošnjak and Boštjan Brumen. 2020. Shoulder Surfing Experiments: A Systematic Literature Review. *Computers & Security* (2020), 102023.

[5] 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* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 4254–4265.

[6] 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 *Proc. of CHI EA '16* (San Jose, California, USA) *(CHI EA '16)*. ACM, New York, NY, USA, 2041–2048.

[7] Barney G Glaser, Anselm L Strauss, and Elizabeth Strutzel. 1968. The discovery of grounded theory; strategies for qualitative research. *Nursing research* 17, 4 (1968), 364.

[8] Mohamed Khamis, Florian Alt, and Andreas Bulling. 2018. The Past, Present, and Future of Gaze-Enabled Handheld Mobile Devices: Survey and Lessons Learned. In *Proceedings of the 20th International Conference on Human-Computer Interaction with Mobile Devices and Services* (Barcelona, Spain) *(MobileHCI '18)*. Association for Computing Machinery, New York, NY, USA, Article 38, 17 pages.

[9] 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, Article 45 (2018).

[10] Mohamed Khamis, Mariam Hassib, Emanuel von Zezschwitz, Andreas Bulling, and Florian Alt. 2017. GazeTouchPIN: Protecting Sensitive Data on Mobile Devices Using Secure Multimodal Authentication. In *Proceedings of the 19th ACM International Conference on Multimodal Interaction* (Glasgow, UK) *(ICMI 2017)*. ACM, New York, NY, USA, 446–450.

[11] Mohamed Khamis, Tobias Seitz, Leonhard Mertl, Alice Nguyen, Mario Schneller, and Zhe Li. 2019. Passquerade: Improving Error Correction of Text Passwords on Mobile Devices by using Graphic Filters for Password Masking.. In *Proceedings of the 37th Annual ACM Conference on Human Factors in Computing Systems* (Glasgow, UK) *(CHI '19)*. ACM, New York, NY, USA.

[12] 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.

[13] Katharina Krombholz, Heidelinde Hobel, Markus Huber, and Edgar Weippl. 2015. Advanced social engineering attacks. *Journal of Information Security and applications* 22 (2015), 113–122.

[14] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. 2007. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on Usable privacy and security*. 13–19.

[15] Kirsti Malterud, Volkert Dirk Siersma, and Ann Dorrit Guassora. 2016. Sample size in qualitative interview studies: guided by information power. *Qualitative health research* 26, 13 (2016), 1753–1760.

[16] 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.

[17] Diogo Marques, Ildar Muslukhov, Tiago Guerreiro, Luís Carriço, and Konstantin Beznosov. 2016. Snooping on Mobile Phones: Prevalence and Trends. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 159–174.

[18] 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* (Munich, Germany) *(MobileHCI '13)*. Association for Computing Machinery, New York, NY, USA, 271–280.

[19] 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.

[20] 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* (Taipei, Taiwan) *(MobileHCI '19)*. Association for Computing Machinery, New York, NY, USA, Article 18, 6 pages.

[21] 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* (Cairo, Egypt) *(MUM 2018)*. Association for Computing Machinery, New York, NY, USA, 147–152.

[22] 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* (Seoul, Republic of Korea) *(CHI '15)*. ACM, New York, NY, USA, 1403–1406.

[23] 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* (Santa Clara, California, USA) *(CHI '16)*. ACM, New York, NY, USA, 4320–4324.

[24] Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. 2006. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the working conference on Advanced visual interfaces*. 177–184.

[25] 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* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1362–1373.