"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

Habiba Farzand
University of Glasgow, UK

Karola Marky
University of Glasgow, UK
Leibniz University Hannover, Germany

Mohamed Khamis
University of Glasgow, UK

Abstract

Shoulder surfing is a prevailing threat when accessing smartphone information at different locations. Prior work has proposed numerous mechanisms to combat the threat, however, when and what mechanism to use while maintaining appreciable user experience and usability remains a challenge. Further, the subjective interpretation of sensitive content adds to the challenge of protecting users' privacy and security. In this poster, we present preliminary findings on what users perceive as sensitive information in the context of shoulder surfing from an online survey with N=40 participants. We found that the need for the protection mechanism varies with the context of use. Users consider location and relationship with the observer when hiding content from unconsented observations. Based on the findings, we propose a typology of perceived sensitive content considering social aspects in shoulder surfing scenarios. Our typology can be used as a baseline for designing personalized shoulder surfing protection mechanisms.

1 Introduction & Background

Shoulder surfing refers to directly observing a target user's screen without permission [4, 18]. It makes use of the human capability of making observations to reveal the information while the user interacts with the system. Shoulder surfing is not only restricted to authentication [1, 10, 11, 13] but its evidence is also found in content-based shoulder surfing [4,5]. Prior work has proposed a number of mechanisms to combat shoulder surfing e.g., Dimming Filters [10] for content-based shoulder surfing. However, having the filters applied to the entire screen would hinder user interaction and also disturb system usability. Multiple attacks [9] would further cause hindrance in device interaction and prevent the user from completing their task. Therefore, it is important to protect the sensitive content only instead of applying the mechanism at every shoulder surfing detection. This directs towards developing an understanding of sensitive content. This can be done by examining privacy perceptions. The concept of privacy has been investigated thoroughly in wide contexts [14, 17], however, the definition of privacy changes as the context changes. For example, privacy means transparency in data collection in the case of Contact Tracing Apps [6] and on the other side, privacy means protecting one's smartphone content from being observed by someone without permission i.e. in the case of shoulder surfing [5].

In this paper, we explore what kind of data participants perceive to be privacy-sensitive in shoulder surfing incidents by distributing a survey to N=40 participants. Prior work has investigated that the perceived sensitive content depends on the location and the relationship with the observer [5]. Therefore, we explore the users' perspective on hiding privacy-sensitive content considering the location of the incident and the relationship with the observer. The study also noted the specific task users perform with their devices at the highlighted red zones of shoulder surfing [4]. We found that privacy-sensitive content is not considered to be static, instead it varies based on the relationship with the observer. Gathering this information, helped to us to shape what content requires most protection against shoulder surfing and led to a typology of perceived sensitive content.

Contribution Statement: In this paper, we contribute a typology of perceived sensitive content in the context of shoulder surfing. Our proposed typology could be used (1) as a basis for designing novel protection mechanisms, and (2) as a method for prioritising content protection and delivering a personalized shoulder surfing protection to users.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

2 Methodology

The questionnaire mainly composed of Likert statements and open-ended questions that were structured similar in wording. Similar wording and Likert statements often have the possibility of random selection or response biases. To counter this, we used two attention check questions. All questions were randomized to avoid order effects. The study was approved by the Ethics Committee at our institute.

2.1 Participants

We recruited N=40 participants from Australia through Prolific [15]. Participants were on average 34.45 years old (min=18, max=54, SD=9.36). 24 of them self-identified as male, 15 as female, and one as non-binary. To better situate the perceived sensitive content in the context of shoulder surfing threat, we used five scales to define the users privacy attitude; Privacy Attitude Questionnaire [2] gave Mean=3.17, SD=0.29, Affinity for Technology Interaction Scale [7] resulted in Mean=3.89, SD=0.84, Marlowe Crowne Social Desirability Scale [16] resulted in Mean=10, SD=3.01, and Security Behavior Intentions Scale [3] produced Mean=3.45, SD=0.84. Further we used three sub-scales from IUIPC [12]; Awareness resulted with Mean=6.03, SD=0.87, Control resulted with Mean=5.65, SD=0.87, and Collection resulted with Mean = 5.41, SD= 1.09.

2.2 Procedure & Data Analysis

The study initiated with information about the study followed by a consent form. After consent signing, participants were explained the concept of shoulder surfing using plain language and figures from prior work [4]. Participants were then asked about general interpretations of sensitive content in the context of shoulder surfing. Next, the participants were presented mutually exclusive location-specific questions based on previous work [4] to capture the perceived sensitive content. The responses were analyzed by an inductive coding approach. First, one researcher grouped similar answers into categories until no further categorization was possible. The categorization was discussed and verified with a second researcher. We then checked the saturation of the dataset by applying the method by Guest et al. [8]. The distinct themes for the base was 14 in our case. A coding scheme was collected. We then calculated the saturation ratio by splitting the new themes in the second run (0) by the number of distinctive themes in the base set (14). The quotient exhibited 0% new information. This falls under the <=5% threshold, therefore, we stopped collecting further data.

3 Findings & Outlook

Most reported privacy-sensitive content in the context of shoulder surfing included text messages (N=25), photos (N=18), banking info (N=19), authentication credentials (N=15), and emails (N=11). Other reported answers included web browsing (N=4), videos (N=2), and contacts (N=2). Some participants also mentioned concrete contents, such as bank transactions, social media, calendars, x-rated content, bank names, addresses, government accounts, work affiliated content, and health info. When for a personal definition of sensitive content, participants defined the content to be *"personal"*, anything that could be *"embarrassing"*, or could be used as a *"personal threat"* or a *"security threat"*. Next, the participants were asked to report on who is likely to accompany them at specific locations and report on what they prefer to hide. Participants who did not visit a specific location were not presented with next location related specific questions and were skipped to the next location's section.

Private Environments. 16 out of 40 participants shared their accommodation with their partner, seven with relatives, six with children, four with siblings, two with friends, and five participants reported having no shared accommodation. N=29 participants agreed that they use apps that display sensitive information in their private accommodation.

Lecture Halls. Two participants reported to visit lecture halls once a week, three participants visited 2-3 times a week, one participant visited once a month, and 34 participants mentioned as never visiting lecture halls. Participants visiting lecture halls reported having been accompanied by colleagues (N=3), partners (N=1), siblings (N=1), or strangers (N=1). Further, four participants used smartphones in lecture halls and two of them also mentioned using smartphone apps with sensitive content.

Theatre Halls. Three participants reported to visit theatre halls once in a month and one participant reported to visit once a week. While 36 participants mentioned not visiting theatre halls. Among the visitors, N=3 used smartphones at theatre halls and one participants reported to use apps with sensitive content. Participants mentioned being accompanied by partner (N=2) and strangers (N=1).

Narrow/Crowded Places. N=17 participants visited narrow/crowded places once a month. Seven visited 2-3 times a week, five visited once a week, two 4-6 times a day, and two visited daily. Amongst the visitors, N=20 reported to use smartphones and N=10 reported to use apps with sensitive content. Participants mentioned visiting narrow/crowded places either with children (N=1), colleagues (N=1), friends (N=2), or partner (N=3). N=26 participants mentioned being surrounded by strangers when they visited such places.

Location	Application	Content Type	Mean Score
Narrow/Crowded Places	Messaging	Entire screen	83
		Messages list	76
	Social Media	Messages list	100
		Message body	100
		Photos	65
		Entire screen	55
	Email	Subject line	82
		Body text	82
	Entertainment	ID/Password	36
		Account Name	36
	Banking	Top	51
		Money	93
University	Web Browser	ID & Password	30
		Entire Screen	30
Lecture Halls	Social Media	Photos	86
	Email	ID & Password	73
Public Transport	Email	Body Text	77
	Messaging	Body Text	83
		Messages list	52
	Social Media	Messages list	80
		Body Text	78.4
Workplace	Gallery	Entire Screen	83
	Email	Body Text	69
	Browser	Entire screen	5
	Social Media	Photos	83
		Message body	79.75
		Messages list	75
	Banking	ID/Password	97
		Transactions	97
		Entire Screen	97
		Money	95.5

Table 1: Typology of Perceived Sensitive Content against Shoulder Surfing Threat (Part I).

Public Transport. Fourteen participants used public transport once in a month, four participants used 2-3 times a week, three participants used 4-6 times a week, three participants used daily, and two participants reported to use public transport once a week. Fourteen participants reported to have never used public transport. Twenty-five participants mentioned being surrounded by strangers in public transport while one participant mentioned being surrounded by children. Amongst the users of public transport, N=24 participants used mobile phone while on public transport and N=8 reported to use applications containing sensitive content.

Cafe/Bar/Restaurant. Fourteen participants visited cafe/bar/restaurant at least once a month. Twelve participants visited once a week, N=5 participants visited 2-3 times a week, N=5 participants visited 4-6 times a week, and N=2 participants visited daily. Two participants also mentioned never going to cafe/bar/restaurant. Participants visiting cafe/bar/restaurant were usually surrounded by strangers (N=14) followed by partner (N=12, friends (N=6), siblings (N=4), or relatives (N=2). Fourteen participants mentioned being surrounded by strangers when they visit cafe/bar/restaurant. N=26 participants reported to use smartphone and N=13 reported to use applications with sensitive content.

University. Four participants participants reported to go to university once in a month. N=2 participants reported to visit university once a week and N=2 participants visited 2-3 times a week. One participant reported to visit 4-6 times a week. N=7 participants reported to use smartphones at university and none participant expressed agreement on using applications with sensitive content. Participants mentioned being surrounded by strangers (N=3), friends (N=3) or colleagues (N=3).

Location	Application	Content Type	Mean Score
Private Environment	Messaging	Messages list	82.25
	Email	Body Text	65
	Web Browser	Entire Screen	85.5
		URL	52
	Social Media	Entire Screen	100
		Messages list	78
	Gallery	Entire Screen	60
		Central	52
	Banking	Transactions	100
		Money	90.14
		Entire Screen	77.5
		ID/Password	78.5
		Banking info	74
		Central	65
Theatre Halls	Banking	Entire Screen	97
	Social Media	Photos	66
	Messaging	Entire Screen	49
Cafe/Bar/Restaurant	Gallery	Entire Screen	95
	Messaging	Contact Info	100
		Messages list	92
	Social Media	Message body	100
		Entire Screen	100
		Messages list	53.33
	Banking	Top	100
		Entire Screen	85.5
		ID/Password	72

Table 2: Typology of Perceived Sensitive Content against Shoulder Surfing Threat (Part II).

Work. Twenty three participants reported to be employed and going to work. Ten participants visited workplace 4-6 times a week, N=7 participants visited 2-3 times a week while N=5 participants visited daily. One participant reported to visit office once in a month. All participants (N=23) mentioned to be surrounded by colleagues in workplaces. N=22 mentioned using smartphones at workplaces with N=15 participants agreeing to use smartphone applications with sensitive content.

Sensitive Content. Participants were asked to name one application they are likely to use at the indicated location and the content of that particular application that they consider to be sensitive. Along with this, participants were also asked to provide a magnitude of how much they consider it to be sensitive on a scale of 0-100. The individual magnitudes of similar applications and their sensitive content were combined to give a mean value. The results were used to create a typography of content sensitivity which we present in Table 1 and 2.

4 Conclusion & Future Work

We surveyed N=40 participants to reveal what users perceive as privacy-sensitive content in the context of shoulder surfing. We found that privacy perceptions for hiding content from observers vary as the user-observer relationship and location varies. Our findings reveal that not every content found on smartphones needs a protection mechanism against shoulder surfing. Further, the smartphone content could be divided into different levels accounting for a different levels of protection. Organizing the perceived sensitive content resulted in a typology of privacy-sensitive content. Despite the cultural limitation of having Australian participants only recruited for this study, our typology serves as the basis for personalized protection and assists the design of mechanisms that protect privacy-sensitive content while not affecting the user experience and system usability due to mechanism activation during unneeded times. For future work, we propose to design mechanisms in the light of the typology, providing targeted content protection and evaluate the user experience, system usability, and privacy preservation satisfaction.

Acknowledgments

This publication was supported by the 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 has also been funded by the UK EPSRC under grant number EP/S035362/1.

References

[1] Farid Binbeshr, ML Mat Kiah, Lip Yee Por, and Aws Alaa Zaidan. A systematic review of pin-entry methods resistant to shoulder-surfing attacks. *computers & security*, 101:102116, 2021.

[2] Mark H Chignell, Anabel Quan-Haase, and Jacek Gwizdka. The privacy attitudes questionnaire (paq): initial development and validation. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 47, pages 1326–1330. SAGE Publications Sage CA: Los Angeles, CA, 2003.

[3] Serge Egelman and Eyal Peer. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pages 2873–2882, 2015.

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

[5] Habiba Farzand, Kinshuk Bhardwaj, Karola Marky, and Mohamed Khamis. The interplay between personal relationships & shoulder surfing mitigation. In *Proceedings of the Mensch und Computer 2021 (MuC '21)*, 2021.

[6] Habiba Farzand, Florian Mathis, Karola Marky, and Mohamed Khamis. Trust & privacy expectations during perilous times of contact tracing. In *Usable Security & Privacy Symposium*, 2022.

[7] Thomas Franke, Christiane Attig, and Daniel Wessel. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ati) scale. *International Journal of Human–Computer Interaction*, 35(6):456–467, 2019.

[8] Greg Guest, Emily Namey, and Mario Chen. A simple method to assess and report thematic saturation in qualitative research. *PloS one*, 15(5):e0232076, 2020.

[9] Mohamed Khamis, Linda Bandelow, Stina Schick, Dario Casadevall, Andreas Bulling, and Florian Alt. 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*, pages 31–35, 2017.

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

[11] Mohamed Khamis, Karola Marky, Andreas Bulling, and Florian Alt. User-centred multimodal authentication: securing handheld mobile devices using gaze and touch input. *Behaviour & Information Technology*, pages 1–23, 2022.

[12] Naresh K Malhotra, Sung S Kim, and James Agarwal. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information systems research*, 15(4):336–355, 2004.

[13] Peter Mayer, Nina Gerber, Benjamin Reinheimer, Philipp Rack, Kristoffer Braun, and Melanie Volkamer. I (don't) see what you typed there! shoulder-surfing resistant password entry on gamepads. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–12, 2019.

[14] Sameer Patil, Natalia Romero, and John Karat. Privacy and hci: methodologies for studying privacy issues. In *CHI'06 Extended Abstracts on Human Factors in Computing Systems*, pages 1719–1722, 2006.

[15] Prolific. Prolific | online participant recruitment for surveys and market research, 2021. Retrieved September 01, 2021.

[16] Robert Strahan and Kathleen C Gerbasi. Short, homogeneous versions of the marlowe-crowne social desirability scale. *Journal of clinical psychology*, 1972.

[17] Asimina Vasalou, Alastair J Gill, Fadhila Mazanderani, Chrysanthi Papoutsi, and Adam Joinson. Privacy dictionary: A new resource for the automated content analysis of privacy. *Journal of the American Society for Information Science and Technology*, 62(11):2095–2105, 2011.

[18] Xingjie Yu, Zhan Wang, Yingjiu Li, Liang Li, Wen Tao Zhu, and Li Song. Evopass: Evolvable graphical password against shoulder-surfing attacks. *Computers & Security*, 70:179–198, 2017.

5 Questionnaire Format

In this section, we provide the questionnaire format used in the study to explore perceived sensitive content in shoulder surfing incidents.

Narrative Sometimes we found someone related/unrelated to us looking over on our personal device (such as smartphone etc) without our permission or sometimes we encounter a situation where we get a chance to look over someone's personal device (such as a smartphone) without being noticed by them. An example of such a situation is shown below:

In this sketch, you see Cas and Vic. Cas is using a mobile device (like a smartphone) 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.).

Answer the following question while keeping the above narrative in mind.

In this sketch, you see Cas and Vic. Cas is using a mobile device (like a smartphone) 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.).

Answer the following question while keeping the above narrative in mind.

- What do you perceive as "sensitive content" on mobile phones in regards to the above situation described? Please note, there are no right or wrong answers. We are only interested in knowing your view.

- The succeeding questions inquire about the following locations. Please try to be as descriptive as possible.

  - a. Your accommodation
  - b. Public Transport
  - c. Theatre Halls
  - d. Lecture Halls
  - e. Work / University
  - f. Crowded / Narrow Places
  - g. Café / Restaurant / Bar

  If you are not a visitor of any of the public locations, you are free to skip the section and move to the next one.

- How often do you go to *insert location*?

  - Once a week
  - 2-3 times a week
  - 4-6 times a week
  - Daily
  - Once a month
  - Never

- Who is most likely to surround you at *insert location*?

  - Children
  - Partner
  - Siblings
  - Relatives
  - Friends
  - Colleagues
  - Strangers

- With your own definition of "sensitive content" in mind, "In this situation, I use apps with sensitive information", you:

  - Strongly disagree
  - Somewhat disagree
  - Neither agree nor disagree
  - Somewhat agree
  - Strongly agree

- Name one smartphone application that contains sensitive content and you're likely to use at *insert location*.

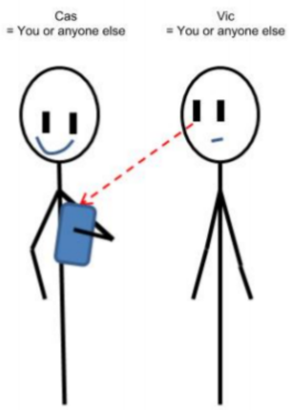
- With your own definition of "sensitive content" in mind, what specific part of the screen of this application you consider to be most sensitive at *insert location* when the person you mentioned previously can see your screen?

- On the following scale, drag the slider to represent how sensitive is the part of the screen you mentioned in the previous question.

  - The part of the screen mentioned in the previous question is *.....* sensitive: (0-100 horizontal slider scale)

- Please provide the following demographic details:

  - Please enter your age:
  - Gender
    - Male
    - Female
    - Prefer not to say
    - Prefer to self-describe
  - Which of these is the highest education you have achieved?
    - Secondary Education (eg GCSE)
    - High School Diplomas / A Levels
    - Technical / Community College
    - Undergraduate Degree (BS, BSc)
    - Graduate Degree (MA, MSc etc)



    - Doctorate Degree (PhD / other)
- Current country of residence:
- Please choose your employment status:
    - Not working
    - Working from home
    - Essential Worker
    - Student
    - Prefer to self describe