



Farzand, Habiba (2025) *Understanding shoulder surfing and informing the design of protection mechanisms*. PhD thesis.

<https://theses.gla.ac.uk/85064/>

Copyright and moral rights for this work are retained by the author

A copy can be downloaded for personal non-commercial research or study, without prior permission or charge

This work cannot be reproduced or quoted extensively from without first obtaining permission in writing from the author

The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the author

When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given

Enlighten: Theses

<https://theses.gla.ac.uk/>
research-enlighten@glasgow.ac.uk

**Understanding Shoulder Surfing
&
Informing the Design of Protection Mechanisms**

Habiba Farzand

Submitted in fulfilment of the requirements for the
Degree of Doctor of Philosophy

School of Computing Science
College of Science and Engineering
University of Glasgow



University
of Glasgow

March 2025

Abstract

Shoulder surfing, the act of looking at the screen of someone's device without their consent, is a ubiquitous threat when accessing information on personal devices like smartphones. With the rapid increase in the use of smartphones, the threat of shoulder surfing is also increasing. This thesis first contributes a systematic literature analysis that focuses on the resources required for targeted attacks against mobile devices and finds that shoulder surfing, which belongs to the novice attacks category, is one of the most accessible attacks. This is because it requires no sophisticated setup. An attacker must only be near a user to observe the device's screen. Considering the ease of execution of shoulder surfing, we investigated shoulder surfing more in-depth through two studies, which are this thesis's second and third contributions. First, we conducted a one-month diary study to understand how shoulder surfing happens in the real world. We found that shoulder surfing can happen anywhere, anytime, without the users realising it. Further, our results showed that content such as text and photos are shoulder surfed more frequently than authentication credentials. Second, to examine the impact and importance of addressing shoulder surfing, we conducted an online survey asking participants how it impacted their social lives, perceptions of privacy, and interactions with their mobile devices. We discovered that shoulder surfing is a deep concern among users, affecting their perception of privacy. It was seen as the gateway to threats like identity or device theft. Based on the empirical discoveries around how shoulder surfing happens and impacts users' privacy perceptions, the fourth contribution of this thesis looks into uncovering a user-centred approach to designing protection mechanisms. For this, we designed and validated a scientific instrument, the Out-of-Device Privacy Scale (ODPS), to measure users' privacy regarding threats in the physical world. ODPS fills the gap between protection mechanisms and users' perceptions of privacy. The fifth contribution presents an exploratory study to explore correlations between personal attributes such as ODPS and user preferences for privacy mechanisms extracted from the literature. The results proved that user preferences for protection mechanisms highly correlate with ODPS. Overall, the results help understand the relationship between a user's perception of privacy against device-external threats and the design of protection mechanisms. We conclude by discussing design recommendations to assist in developing novel protection mechanisms. Based on a series of empirical investigations, this thesis presents a user-tailored privacy investigation of shoulder surfing and informs the design of protection mechanisms.

Contents

Abstract	i
Acknowledgements	xiv
1 Introduction	2
1.1 Motivation	2
1.2 Shoulder Surfing: Threat Model	3
1.3 Thesis Walk-through & Research Questions	4
1.4 Key Contributions	6
1.5 Thesis Statement	7
1.6 Research Methods	8
1.6.1 Systematic Literature Review	8
1.6.2 Diary Studies	8
1.6.3 Qualitative Surveys	8
1.6.4 Scale Development	8
1.6.5 Descriptive Research	9
1.7 Publications & Declaration of Co-Authorship	9
1.8 Further Relevant Publications by the Thesis Author	11
2 A Systematic Deconstruction of Human-Centric Privacy & Security Threats on Mobile Phones	14
2.1 Introduction	15
2.2 Related Work	16
2.3 Methodology	18
2.4 Requirements of Human Centred Attacks on Mobile Phones	20
2.5 Glossary of Attacks	21
2.6 Level 1: Novice Attacks	21
2.6.1 Human Capabilities	23
2.6.2 Human Capabilities & Manual Tools	24
2.6.3 Human Capabilities & Hardware Tools	24
2.7 Level 2: Intermediate Attacks	25

2.7.1	Mobile Apps	25
2.7.2	Mobile Apps & User Phone Permissions	25
2.7.3	Mobile Apps, Hardware Tools & Phone Permissions	26
2.8	Level 3: Proficient Attacks	26
2.8.1	Software Tools & Human Capabilities	26
2.8.2	Software & Hardware Tools	27
2.8.3	Software, Hardware & Manual Tools	27
2.8.4	Software Tools & Mobile Apps	27
2.8.5	Software Tools, Hardware Tools & User Phone Permissions	28
2.8.6	Software Tools, Mobile Apps & User Phone Permissions	28
2.8.7	Software & Hardware Tools, Mobile Apps, Permissions & Human Capabilities	29
2.9	Level 4: Expert Attacks	29
2.9.1	Advanced Programming	29
2.9.2	Advanced Programming & Mobile Apps	30
2.9.3	Advanced Programming, Hardware Tools & Human Capabilities	30
2.9.4	Advanced Programming, Mobile Apps & Hardware Tools	30
2.9.5	Advanced Programming & Software Tools	31
2.9.6	Advanced Programming, Software Tools & Hardware Tools	31
2.9.7	Advanced Programming, Software Tools, Hardware Tools & Human Capabilities	32
2.9.8	Advanced Programming, Software Tools & Mobile App	32
2.9.9	Advanced Programming, Software Tools & Permissions	33
2.9.10	Advanced Programming, Software Tools, Hardware Tools & Mobile Apps	33
2.9.11	Advanced Programming, Software Tools, Hardware Tools, & Permissions	34
2.9.12	Advanced Programming, Software Tools, Mobile Apps & Permissions	34
2.9.13	Advanced Programming, Software & Hardware Tools, Mobile App, & Human Capabilities	38
2.9.14	Advanced Programming, Software Tools, Mobile App, Hardware Tools & Permissions	38
2.9.15	Advanced Programming, Software Tools, Mobile Application, Hardware Tools, Permissions, Human Capabilities	39
2.10	Discussion	40
2.10.1	Using the categorisation	40
2.10.2	Key Takeaways & Future Research Directions	42
2.11	Conclusion	44

3	Shoulder Surfing through the Social Lens: A Longitudinal Investigation & Insights from an Exploratory Diary Study	46
3.1	Introduction	48
3.2	Background & Related Work	49
3.2.1	Shoulder Surfing Stories	49
3.2.2	Shoulder Surfing Mitigation Methods	50
3.3	Methodology	51
3.3.1	Study Design	51
3.3.2	Recruitment & Participants	52
3.3.3	Procedure	52
3.3.4	Data Analysis	52
3.4	Limitations & Future Work	53
3.5	Findings	53
3.5.1	The Observer's Side of the Story	54
3.5.2	The User's Side of the Story	55
3.5.3	Stories from 3rd Persons	57
3.6	Discussion	58
3.6.1	Shoulder Surfing in Everyday Life - An Overview	58
3.6.2	The Prevalence of Content-Based Shoulder Surfing	58
3.6.3	Principal Lesson Learned	59
3.6.4	Single or Multiple Mechanisms for Content-Based Shoulder Surfing?	60
3.6.5	Context-Aware & Configurable Shoulder Surfing Protection Mechanisms	61
3.6.6	Detecting Shoulder Surfing	61
3.7	Conclusion	62
4	<i>"What you think is private is no longer"</i> - Investigating the Aftermath of Shoulder Surfing on Smartphones in Everyday Life through the Eyes of the Victims	64
4.1	Introduction	65
4.2	Background	67
4.2.1	The Prevalence of Shoulder Surfing	67
4.2.2	Users Responses to Privacy Violations & Shoulder Surfing	69
4.2.3	Existing Software-based Mitigations to Shoulder Surfing	70
4.3	Methodology	70
4.3.1	Questionnaire Design	71
4.3.2	Study Procedure	71
4.3.3	Pilot Testing	72
4.3.4	Ethical Considerations	72
4.3.5	Recruitment & Participants	72
4.3.6	Limitations	73

4.3.7	Data Analysis	73
4.4	Results	74
4.4.1	Setting the Narrative of Shoulder Surfing:	74
4.4.2	Privacy Perceptions	76
4.4.3	Device Usage After Shoulder Surfing	79
4.4.4	User Concerns around Shoulder Surfing	84
4.4.5	Training & Education on Shoulder Surfing	86
4.5	Discussion & Directions for Future Work	87
4.5.1	Shoulder Surfing as the Stepping Stone to Other Serious Threats	87
4.5.2	Shoulder Surfing by Children Puts Them at Risk	89
4.5.3	Self-Equipping Users for Protection Against Shoulder Surfing	90
4.5.4	User Awareness Alone Won't Prevent Shoulder Surfing Risks	90
4.6	Conclusion	91
5	Out-of-Device Privacy Unveiled: Designing and Validating the <u>Out-of-Device Privacy Scale (ODPS)</u>	93
5.1	Introduction	94
5.2	Background	95
5.2.1	Measures of Privacy	95
5.2.2	Out-of-Device Privacy in the Literature	96
5.3	Stage 1: Item Development	97
5.3.1	Identification of Construct	98
5.3.2	Initial Item Pool Generation	98
5.3.3	Refining Items & Assessing Content Validity	99
5.4	Stage 2: Towards Developing the Scale	101
5.4.1	Initial Data Analysis	101
5.4.2	Exploratory Factor Analysis	102
5.5	Stage 3: Final Scale Validation	103
5.5.1	Study Design	103
5.5.2	Participants	104
5.5.3	Initial Data Analysis	104
5.5.4	Confirmatory Factor Analysis	105
5.5.5	Tests of Reliability	105
5.5.6	Construct Validity	105
5.6	Discussion	106
5.6.1	Obstructions in Scale Development Studies	106
5.6.2	Using ODPS to Measure Out-of-Device Privacy	107
5.6.3	Using ODPS to design Protection Mechanisms	107
5.6.4	Using ODPS to measure Privacy Culture	107

5.6.5	Using ODPS in Combination with Other Privacy Scales	108
5.6.6	Instructions for Scoring	108
5.6.7	Limitations & Future Work	108
5.7	Conclusion	109
5.8	Acknowledgements	109
6	SoK: Privacy Personalised - Mapping Personal Attributes & Preferences of Privacy Mechanisms for Shoulder Surfing	111
6.1	Introduction	113
6.2	Background & Related Work	115
6.2.1	User-Level & Device-Level Protection Mechanisms	115
6.2.2	Personal Attributes & Privacy Preferences	116
6.2.3	Research Gap	116
6.3	Stage 1: Collecting Content-Based Protection Mechanisms against Shoulder Surfing	117
6.4	Stage 2: Categorisation of Mechanisms	119
6.4.1	Categorisation Strategy	119
6.5	Stage 3: Data Collection	119
6.5.1	Questionnaire Design	119
6.5.2	Pilot Study	121
6.5.3	Ethical Considerations	121
6.5.4	Data Quality Checks	122
6.6	Results	122
6.6.1	Recruitment & Participants	123
6.6.2	Experience with Shoulder Surfing	123
6.6.3	Perceptions of Protection Mechanisms	123
6.6.4	Ranking of Mechanisms	124
6.6.5	General Perception of Mechanisms	126
6.6.6	Correlation between Personal Attributes & Perception of Protection Mechanisms	128
6.7	Discussion	130
6.7.1	Privacy Mechanisms for General Population	130
6.7.2	Key Takeaways	131
6.7.3	Future Work	132
6.8	Conclusion	132
7	Final Reflections	135
7.1	Reflecting on the Findings	136
7.2	Contributions	137

7.2.1	Conceptual Contributions:	137
7.2.2	Empirical Contributions:	137
7.2.3	Theoretical Contributions:	137
7.2.4	Methodological Contributions:	138
7.2.5	Design Guidelines Contributions:	138
7.3	Pathways for Continued Exploration	138
7.3.1	Beyond W.E.I.R.D. Populations	139
7.3.2	Inclusive Security & Privacy Practices	139
7.3.3	Evaluation of Protection Mechanisms & Need for Vigilance	140
7.3.4	Unconcerned Users or Vulnerable Users?	141
7.3.5	Roleplay of Privacy Paradox	141
7.3.6	Creating Contextual Privacy Settings	141
7.3.7	Remote vs In-Person Data Collection	142
8	Conclusion	144
A		145
A.1	Papers Included in the Systematic Literature Review	145
A.2	Codebook Used for Coding the Attack Requirements	148
B		150
B.1	Diary Study Format	150
B.2	Codebook for the Diary Study	153
C		156
C.1	Survey Format for the Impact Study	156
C.2	Codebook for the Impact Study	160
D		162
D.1	Item Generation Phase	162
D.1.1	Items Created Using Literature-Based Approach	162
D.1.2	Items Constructed Through Deductive Approach - Researchers Devel- oped Items	163
D.1.3	Items Constructed Through Deductive Approach - Items by Larger Pool of Researchers	164
D.2	Items Used in the Pre-Testing Phase	166
D.3	Items Explored in the Exploratory Factor Analysis	167
D.4	Final Set of Items & The Respective Sources	169
D.5	Exploring Multi-Factor Solutions - Additional Analysis	170

E	173
E.1 Questionnaire Format	173

List of Tables

5.1	The Table shows the results of Exploratory Factor Analysis. The items marked in red (last three items) were removed from further analysis as they did not load sufficiently high. IN = Item Number; FL = Factor Loading.	104
5.2	The Table shows (1) the correlation (Kendall's Tau) between ODPS and IUIPC & CFIP and (2) the reliability score of each of the subscales in our dataset of the second study.	106
5.3	The table shows the final look of the 18-item <u>Out-of-Device Privacy Scale</u> (ODPS)	108
6.1	The Table shows the results of the systematic literature review conducted on the top 10 venues in HCI and Computer Security according to Google Scholar (accessed: July 2024).	118
6.2	The Table shows an overview of the ten mechanism categories derived from literature.	120
6.3	The Table shows the overall perception of protection mechanisms (general) . .	127
6.4	Distances between Mechanisms indicating similarities and differences	127
6.5	The Table shows the result of the Principle Component Analysis representing components structure. The statement highlighted in red was removed as it did not load sufficiently high (> 0.30).	129
6.6	The Table shows Participants' perception of general privacy mechanisms in relation to their gender.	130
7.1	An Overview of Research Questions answered individually in each chapter. . .	136
A.1	The Table shows the list of papers extracted from the selected publication venues which are included in the systematic literature review.	146
A.2	The Table shows the list of papers extracted by performing Backward Search which are included in the systematic literature review.	146
A.3	The Table shows the list of papers extracted by performing Forward Search which are included in the systematic literature review.	147
A.4	The Table shows the codebook for Attack Infrastructure Requirement Categories	149

B.1	Codebook used to analyze the Diary Study (1/2)	154
B.2	Codebook used to analyze the Diary Study (2/2).	155
C.1	Codebook Used to Analyse Questionnaire Responses	161
D.1	The Table shows the list of items included in the final version of the ODPS and the corresponding sources.	169
D.2	The table shows the results of a 4-factor solution using a loading cut-off value of 0.4.	171
D.3	The Table shows the 3-factor solution using a loading cut-off value of 0.4. . . .	171
D.4	The Table shows the 2-factor solution using a loading cut-off value of 0.4 . . .	172

List of Figures

1.1	An Overview of Thesis. (This figure was created using CANVA under a free content license [43].	6
2.1	The figure shows the step-wise systematic literature review methodology we followed to develop the categorisation of Social Engineering and Side-Channel Attacks on Mobile Phones.	17
2.2	The figure shows the categorisation of Human Centred Social Engineering and Side Channel Attacks on Mobile Phones from the Perspective of an Attacker. We developed this categorisation based on the resources extracted from the papers resulting from the systematic literature review.	21
2.3	The figure shows the categorisation of attacks in four levels from an attacker's perspective. The expertise required to perform an attacker increases as we progress in categorisation levels.	22
2.4	The figure shows a thermal image of smartphone authentication captured using a thermal camera, i.e. a Flir camera. The authentication information can be easily observed by observing the heat traces. This is a typical scenario of Thermal Attacks that belongs to the category of Novice Attacks.	23
2.5	The figure showcases one of the common scenarios of shoulder surfing - a type of Novice Attack - in the daily lives of users where the bystander uses direct observation to make observations of the screen and is able to retrieve personal information about the user.	24

3.1	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 [43] under Free Content License.)	48
3.2	Location (left) and time (right) of shoulder surfing incidents experienced by participants of diary study either as observer, observee, or as third person. . . .	54
3.3	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.	57
4.1	Shoulder surfing can happen anywhere at any time by anyone. In this paper, we investigate the impact of shoulder surfing on user's social lives and interaction with their devices. For this, we surveyed N=91 participants from the UK and inquired about their privacy perception, device interaction, and awareness and training around shoulder surfing. (The image uses figures by Deivid Saenz and Sofia Salazar [250,251].	65
4.2	The Figure shows the overview of the qualifiers and respective frequencies of codes throughout our results. All occurrences of the respective qualifiers always refer to the same portion of the number of times codes.	74
4.3	The Figure shows the boxplots for the responses of participants to the questions centred around the impact of shoulder surfing.	75
4.4	High-level summary of the key findings of the impact of shoulder surfing. (The image uses figures by Deivid Saenz and Sofia Salazar [250,251]. The overall figure was created using CANVA under free license [43]).	88
5.1	The figure shows daily life scenarios when out-of-device privacy threats in the physical world, such as shoulder surfing, take advantage of the user's physical surroundings to invade data privacy without the user realizing it. (The image was created using Canva under free license [43].)	94

5.2	We followed three high-level stages to develop the scale: 1) item development, 2) scale development, and 3) scale validation. At each stage, we followed the recommendations from the literature to refine and develop the scale iteratively. The figure shows the breakdown of the high-level phases carried out in the development of Out-of-Device Privacy Scale (ODPS) along with the sample sizes in each phase.	98
5.3	The figure shows the scree plot produced using the data for Exploratory Factor Analysis to determine the appropriate number of factors.	103
6.1	The Figure shows participants' feedback on each protection mechanism category. Participants could select from a 7-point Likert scale ranging from strongly disagree (1) to strongly agree (7).	125
6.2	The figure shows the ranking of protection mechanism categories.	126
B.1	(The image was taken from the work by Eiband et.al. [85] on shoulder surfing to better illustrate the meaning of shoulder surfing.)	151
B.2	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	152
E.1	The figure shows an example of everyday life shoulder surfing	173

Acknowledgements

This PhD travelogue holds twin chapters, written in parallel,
Love and support reads one, wisdom and knowledge reads the other,
Complementing each other, the two chapters hold hand in hand,
Making this travelogue incomplete without each other,
To my beloved father - the epitome of limitless love and support,
The man who taught me to be strong, brave, and independent,
Who's voice always echoed in my ears, giving me strength and hope,
Whose memories kept me moving forward through the gravel roads of life,
To my beloved mother - the embodiment of unconditional love and eternal hope,
Always reminding to plant seeds of hope and watch them blossom in the dark,
I carry their words like fireflies in the dark, illuminating the pathways ahead,
With love and gratitude forever, I step ahead, knowing they are always with me.
To my amazing supervisors; Mohamed Khamis, Karola Marky & Stephen Brewster,
This PhD journey is indebted to your unlimited wisdom and knowledge,
You have been the compass in the lost world of my PhD,
Guiding me, paving the way through your insightful supervision,
For every question, every pause, every uncertainty,
You have directed every path I walked on,
This journey ends with a suitcase full of memories and hopeful dreams,
Setting out the next journey in the golden light of dawn.

I

Chapter 1

Introduction

"The real voyage of discovery consists not in seeking new landscapes, but in having new eyes."

— Marcel Proust

1.1 Motivation

The rising ubiquity of smartphones has increased privacy violations. Everyday life scenarios – such as checking emails on a smartphone while having coffee at a cafe, making online payments at a workplace, or commuting on a bus and using a smartphone to navigate the way – are all susceptible to privacy and security attacks such as shoulder surfing.

Shoulder surfing refers to observing someone's device screen without consent. To make successful observations, an attacker needs to be in close vicinity of the user, which is the only requirement for this kind of attack [85, 89]. The threat of shoulder surfing escalates with the rising ubiquity of technological devices. With devices being used anywhere and anytime, the threat of shoulder surfing is always present. It exists in high and as well as in low-socioeconomic countries [85, 252] and is globally recognised [131]. Prior work has provided evidence that shoulder surfing is experienced in public and private environments and is reported by known and unknown observers [85]. Shoulder surfing can leak authentication and personal information such as text messages or photos [85].

Acknowledging the threat of shoulder surfing, researchers have investigated occurrences of shoulder surfing through various methods such as surveys [85, 93], interviews [91] or Virtual Reality studies [5, 248]. Yet, the studies presented in the literature have the following limitations: they were done retrospectively or were limited to a specific location. Second, to address shoulder surfing, researchers have proposed several mitigation strategies, such as lowering the screen brightness [187, 316, 320] or replacing the content displayed on the screen with randomly generated content [156, 211]. Researchers have also explored haptic-based mechanisms such as device vibrations to alert the user for shoulder surfing [246]. Alert icons or a live camera feed indicating bystanders have also been explored to alert the user about being shoulder surfed [246].

Related work pins down several similar mechanisms that offer content-specific protection, such as for photos or text [292] or full-screen protection regardless of content [156]. While these works present interesting insights into occurrences of shoulder surfing and novel and promising protection against shoulder surfing, there are several gaps in this research, which we present below:

1. **Retrospect Gap:** Prior work lists user stories of shoulder surfing in a one-time survey or at a location-specific investigation. This makes it hard to understand if shoulder surfing is a repeated experience or a one-time experience. The frequency of shoulder surfing would determine the severity of the issue. Shoulder surfing can happen anywhere; it is not location-specific and, therefore, requires comprehensive investigation.
2. **Impact Gap:** While literature presents evidence on the occurrence of shoulder surfing, it minimally highlights what happens after the shoulder surfing incident, i.e., the impact of shoulder surfing. Furthermore, it does not distinguish between the perspectives of users and observers, which makes it challenging to see shoulder surfing from the victim's lens. Understanding the impact of shoulder surfing on the victims is important as it establishes the motivation and urgency to address shoulder surfing.
3. **Protection Gap:** There is a lack of understanding of what protection mechanisms users will prefer, e.g., if users prefer alerting mechanisms only or mitigation mechanisms that hide the screen's content in some way. Exploring user preferences assists in providing personalised privacy protection to users against shoulder surfing.

This thesis bridges the above-mentioned gaps by conducting (i) an in-depth study into the anatomy and occurrences of shoulder surfing (chapter 2 and 3), (ii) the impact of shoulder surfing on victim users (chapter 4), and (iii) presenting a user-centred method for assigning privacy protection mechanisms to users based on their privacy profiles (chapter 5 and 6).

1.2 Shoulder Surfing: Threat Model

Privacy refers to an individual's right to protect their personal information's access and use, while security refers to safeguarding against unauthorized access [224]. While privacy emphasises the control of information, security refers to the mechanisms implemented to practice this control. Shoulder surfing refers to the act of observing someone's device screen without permission. Shoulder surfing can be recognized as a privacy and security attack. It's a violation of privacy that uncovers personal information such as text messages or photos, and its security bypasses reveal authentication credentials such as PINs or passwords. While shoulder surfing has the dual characteristics of being a privacy and security attack, in this thesis, we focus on the privacy aspect of shoulder surfing.

A threat model explains the exploitation points of a system and how an attack is performed [45]. In this thesis, we follow the threat model frequently used in existing research on shoulder surfing [86, 162, 174]. The threat model is as follows: we assume that a user is accessing personal information, such as text or photos, on a mobile device in a public or private setting; another person, known or unknown to the user, is sitting or standing close to the first user and has the device in line with his sight; there are no reflections or shadows, so the screen observation perfectly aligns with the second user's sight.

1.3 Thesis Walk-through & Research Questions

This thesis uses a range of methodologies to address the five RQs by collecting data from 2632 participants. Methodologies ranged from conducting a systematic literature review, longitudinal diary study, exploratory surveys and psychometric scale development. This thesis is organised in the following way:

- **Chapter 2** Systematic Literature Review: This thesis presents a review of related work in Chapter 2. Additionally, each chapter presents its own related work section that synthesizes the literature from the lens of the paper topic. Finally, a recent review of literature is included as part of Chapter 6.

A review of existing literature on social engineering and side channel attacks was the starting point of this thesis. A critical review of existing knowledge covering the top 10 venues in HCI and Computer Security provided an in-depth awareness of research challenges, gaps, and future work research directions. By systematically categorising the information gained from a sample of 65 scientific papers, we discovered that shoulder surfing is one of the "Novice Attacks" that do not require a sophisticated setup or expertise of an attacker but only require making observations in the close vicinity of the user. This property of shoulder surfing makes it easier to perform.

This work package assisted in answering **RQ 1**:

RQ 1: Where does shoulder surfing fit in the ecosystem of social engineering and side channel attacks?

- **Chapter 3** Holistic Diary Study: After discovering that shoulder surfing is one of the Novice Attacks that does not require a sophisticated setup, our next step looked into investigating the occurrences of shoulder surfing in the daily life of users, specifically focusing on how, when, and where it happens. For this, we conducted a longitudinal diary study with 23 participants and found out that shoulder surfing happens frequently in users' daily lives. Users reported experiencing it in public and private environments by known and

unknown people. Interestingly, content-based shoulder surfing (such as text messages and photos) was more frequently shoulder surfed than authentication-based shoulder surfing (such as PINs and passwords). This study helped in answering **RQ 2**:

RQ 2: How is a user's privacy violated through shoulder surfing in the real world?

- **Chapter 4** Assessment of Impact of Shoulder Surfing through the Eyes of the Victims: In the previous stage, we learned that content-based shoulder surfing is more prevalent and can happen anywhere at any time. In this chapter, we look into how this impacts victims of shoulder surfing in their daily social and device interactions. We also assess how experiencing shoulder surfing impacts users' perceptions of privacy. To uncover this information, we conducted an online survey with 91 users in the UK. We learned that the impact of shoulder surfing is highly individual and was seen as unavoidable and frequently occurring. Shoulder surfing led to perceived increased time for task completion, made participants rethink accessing data and made users concerned about their privacy and other people's privacy. It was further perceived as a privacy threat, leading to more serious threats like identity or device theft. This chapter answered **RQ 3**:

RQ 3: How does shoulder surfing impact victims' social and device interaction?

- **Chapter 5** Psychometric Scale Instrument: Categorising users based on their privacy profiles has been a conventional method for clustering users and has been proven useful for understanding the needs of specific user groups. In this chapter, we propose and develop a scientific instrument - a psychometric scale - to measure the importance users attribute towards protecting their data from out-of-device threats such as shoulder surfing. The scale assists in designing user-centred protection mechanisms offering personalized and holistic protection. This chapter answers **RQ 4**:

RQ 4: How can we measure users' privacy perceptions in the context of shoulder surfing?

- **Chapter 6** Exploring Correlations: We next explore how different user groups, based on their privacy profiles, have different (or the same) preferences for protection mechanisms. To answer this, we conducted an online survey with 192 participants in the UK and discovered that user preferences for protection mechanisms highly correlate with their Out-of-Device Privacy Scale. Based on the results, we derive design recommendations to assist the design of novel mechanisms. This chapter answered **RQ 5**:

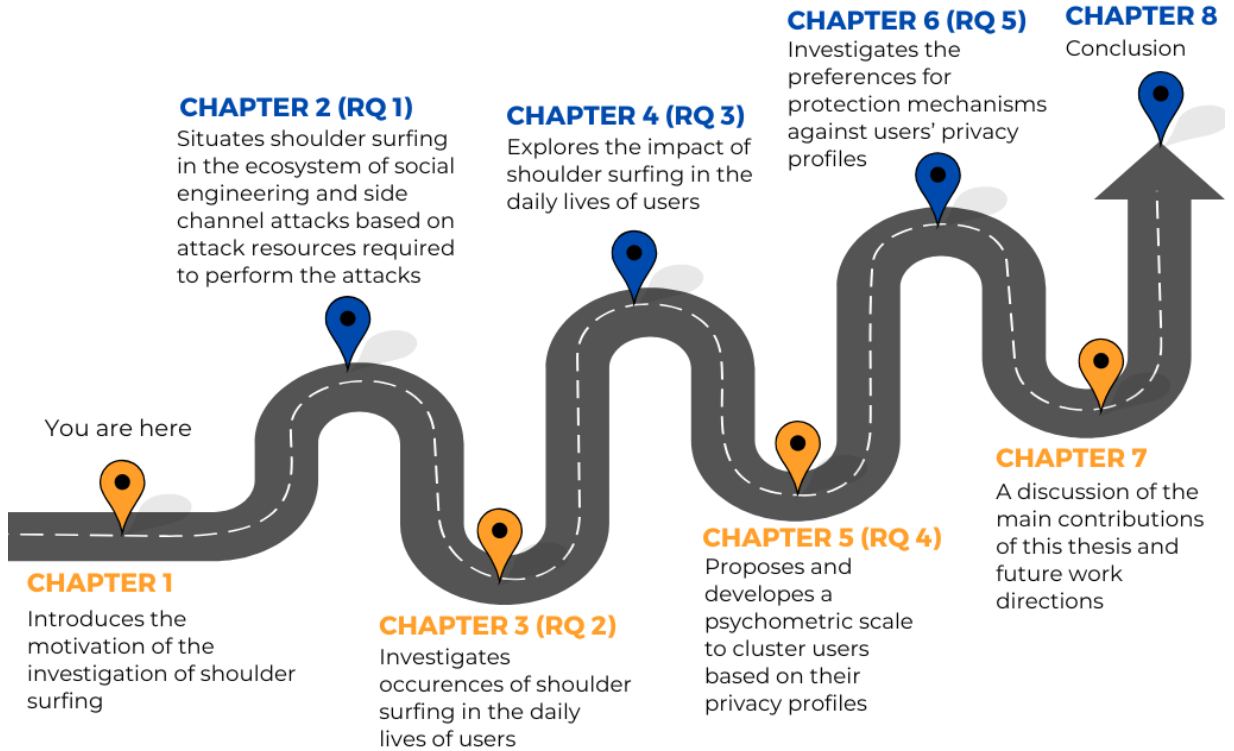


Figure 1.1: An Overview of Thesis. (This figure was created using CANVA under a free content license [43].

RQ 5: How can the design of technical protections against shoulder surfing be informed to reflect users' privacy profiles?

1.4 Key Contributions

This thesis investigates and mitigates privacy issues in users' daily lives. We address the RQs in five stages: a systematic literature review, a holistic diary study, an assessment of the impact of privacy violations, psychometric scale development, and lastly, exploring correlations between personal attributes and preferences for protection mechanisms to inform the design of protection mechanisms. We make the following primary contributions.

1. **Categorisation of Attacks on Mobile Devices:** This thesis proposes a novel categorisation of social engineering and side-channel attacks on mobile devices based on the required resources for performing these attacks. The categorisation consists of four levels:

- (1) Novice Attacks, (2) Intermediate Attacks, (3) Proficient Attacks, and (4) Expert Attacks. Each level indicates resource complexity defined by ISO/IEC metrics. The categorisation assists in the assessment of attacks and in determining accessibility vs scalability. This contribution provides a micro-view of attacks, and especially shoulder surfing, from the lens of existing knowledge. (Chapter 2)
2. **Occurrences & Impact of Shoulder Surfing:** This thesis provides empirical evidence and confirms prior work findings around the occurrences of shoulder surfing. Then, this thesis presents the first exploration of the impact of shoulder surfing on the daily lives of users. The results highlight that shoulder surfing is independent of location, time and relationship with the observer. Its impact varies from user to user. This contribution bridges the "*retrospect and impact gap*". (Chapter 3 and 4)
3. **Psychometric Scale Instrument:** We next present a validated and reliable psychometric scale instrument to measure users' importance of privacy towards threats in the physical world, such as shoulder surfing. The scale is a novel user profiler method to help group users based on their privacy profiles. This contribution helps to cover "*protection gap*". (Chapter 5)
4. **Preferences for Protection Mechanisms:** Lastly, this thesis puts forward the first evidence of the relationship between personal attributes and preferences for protection methods against shoulder surfing. It introduces novel design guidelines considering personal attributes of users. This contribution assists in covering "*protection gap*". (Chapter 6)

1.5 Thesis Statement

This thesis develops an understanding of shoulder surfing - an everyday life privacy violation and presents a user-centred approach to safeguard users' privacy from shoulder surfing. Categorising users to offer personalised experiences while understanding the needs of specific user groups is a well-established approach in literature. This thesis presents a novel psychometric scale instrument to cluster users based on their privacy profiles and the importance of protection against out-of-device threats. It first categorises social engineering and side channel attacks on mobile devices based on attack resources. Using the categorisation, it identifies shoulder surfing as a novice attack that exclusively relies on human capabilities, manual tools, and basic hardware tools. Then, an exploration study of shoulder surfing in users' daily lives is conducted. It then highlights the need to address shoulder surfing by conducting an assessment of the impact of shoulder surfing through the eyes of the victims. This thesis proposes and develops a scientific instrument based on empirical investigations to cluster users based on their privacy profiles.

This thesis concludes with investigations on exploring correlations between users' personal attributes and preferences for privacy protections against shoulder surfing, exploring correlations to inform the design of protection mechanisms.

1.6 Research Methods

This thesis makes use of five research methods from the domain of Human-Computer Interaction: (1) systematic literature review, (2) diary studies, (3) qualitative surveys, (4) psychometric scale development, and (5) descriptive research.

1.6.1 Systematic Literature Review

Systematic literature review refers to conducting literature reviews using a keyword-focused search query followed by inclusion and exclusion criteria. A systematic literature review assists in getting an overview of the latest research published. This thesis performed a systematic literature review to identify existing social engineering and side channel attacks on mobile devices and categorised them based on attack resources for attack assessments. [Chapter 2](#)

1.6.2 Diary Studies

A diary study is a qualitative and longitudinal research method that captures participants' experiences over time [32, 245]. They fill the gaps between one-time survey responses and observations in a naturalistic and controlled environment [140]. One of the categories of diary studies is feedback-styled diary studies [44]. They are based on prompt questions that participants respond to when they experience something. Due to this quality of responding to questions as soon as participants experience something, diary studies do not suffer from recall biases or memory decay [244]. In this thesis, we used diary studies to explore occurrences of shoulder surfing in users' daily lives. [Chapter 3](#)

1.6.3 Qualitative Surveys

Qualitative surveys with open-ended questions assist in capturing data from a large and diverse sample. They help mitigate the impact of the researcher's presence when asking questions on sensitive topics such as personal experiences. In this thesis, we deployed qualitative surveys to elicit the impact of shoulder surfing from the eyes of the victims. [Chapter 4](#)

1.6.4 Scale Development

Psychometric scale development is a process of developing a scientific instrument that captures granular concepts such as privacy attitude or behaviour by asking a series of questions. The

captured construct is then used as a user profiling method. The scale development process follows rigorous dimensionality, reliability, and validity tests. In this thesis, we developed a psychometric scale instrument to capture users' importance for out-of-device privacy.

Chapter 5

1.6.5 Descriptive Research

Descriptive research refers to research that provides information on a population sample [79, 279]. This thesis uses descriptive research to uncover user preferences for privacy protection mechanisms against shoulder surfing based on their privacy profiles. Chapter 6

1.7 Publications & Declaration of Co-Authorship

This thesis presents five papers; three out of five are published at top peer-reviewed security and HCI venues, while two are currently under review at IEEE Security & Privacy.

Chapter 2 constitutes the following paper and represents the background chapter of the thesis:


Habiba Farzand, Melvin Abraham, Stephen Brewster, Mohamed Khamis, & Karola Marky. A Systematic Deconstruction of Human-Centric Privacy & Security Threats on Mobile Phones. *International Journal Human-Computer Interaction* (2024): 1-24. [89]

The idea was initiated by my supervisor, Karola Marky. I conducted the systematic review under the guidance of my supervisors, Karola Marky and Mohamed Khamis. My colleague, Melvin Abraham, assisted in the extraction of information about the resources of attacks from a subset of papers that I selected and reviewed selected sections of the paper. The work was regularly discussed with my supervisors, Karola Marky and Mohamed Khamis. I wrote the initial draft of the paper and made the subsequent corrections after receiving feedback from my supervisors: Stephen Brewster, Karola Marky, and Mohamed Khamis.

Chapter 3 constitutes of the following paper:

Habiba Farzand, Karola Marky, and Mohamed Khamis. "Shoulder surfing through the social lens: A longitudinal investigation & insights from an exploratory diary study." In *Proceedings of the 2022 European Symposium on Usable Security*, pp. 85-97. 2022. [94]

I initiated, designed, and ran the study. I conducted the data analysis with assistance from my supervisor, Karola Marky, who assisted in resolving coding disagreements. I reported and interpreted the data. The work was regularly discussed with my supervisors, Karola Marky

and Mohamed Khamis. I wrote the initial draft of the paper and made the subsequent corrections after receiving feedback from my supervisors, Karola Marky and Mohamed Khamis. This work has also been published at SOUPS 2023 as a poster and received  "Distinguished Poster Award" [95].

Chapter 4 constitutes of the following paper:

Habiba Farzand, Shaun Macdonald, Karola Marky, & Mohamed Khamis (2025, May). *"What you think is private is no longer"* - Investigating the Aftermath of Shoulder Surfing on Smartphones in Everyday Life through the Eyes of the Victims. Under review at IEEE Security & Privacy 2025 [92].

I initiated, designed, and ran the study. I conducted the data analysis with assistance from my colleague, Shaun Macdonald, who assisted in resolving coding disagreements and helped generate Figure 4.3. I reported and interpreted the data. The work was regularly discussed with my supervisors, Karola Marky and Mohamed Khamis. I wrote the initial draft of the paper and made the subsequent corrections after receiving feedback from my colleagues, Shaun Macdonald, and supervisors Karola Marky and Mohamed Khamis.

Chapter 5 constitutes of the following paper:

Habiba Farzand, Karola Marky, & Mohamed Khamis (2024, May). Out-of-Device Privacy Unveiled: Designing and validating the out-of-device privacy scale (ODPS). In Proceedings of the CHI Conference on Human Factors in Computing Systems, pp. 1-15. 2024. [96]

I initiated, designed, and ran the study. I conducted the data analysis, reporting and interpretation of the data. The work was regularly discussed with my supervisors, Karola Marky and Mohamed Khamis. I wrote the initial draft of the paper and made the subsequent corrections after receiving feedback from my supervisors, Karola Marky and Mohamed Khamis.

Chapter 6 constitutes of the following paper:

Habiba Farzand, Karola Marky, & Mohamed Khamis (2025, May). SoK: Privacy Personalised - Mapping Personal Attributes & Preferences of Privacy Mechanisms for Shoulder Surfing. Under review at IEEE Security & Privacy 2025 [97].

I initiated, designed, and ran the study. I conducted the data analysis, reporting and interpretation of the data. The work was regularly discussed with my supervisors, Karola Marky and Mohamed

Khamis. I wrote the initial draft of the paper and made the subsequent corrections after receiving feedback from my supervisors, Karola Marky and Mohamed Khamis.

1.8 Further Relevant Publications by the Thesis Author

The author of this thesis contributed to further research that informed or inspired the work presented in this thesis. Below is a selective list of publications where the author led or collaborated with other researchers. For a full list of publications, please visit Google Scholar Profile.

- Mohamed Khamis, Rebecca Panskus, **Habiba Farzand**, Marija Mumm, Shaun Macdonald, and Karola Marky. "Perspectives on DeepFakes for Privacy: Comparing Perceptions of Photo Owners and Obfuscated Individuals towards DeepFake Versus Traditional Privacy-Enhancing Obfuscation." In Proceedings of International Conference on Mobile and Ubiquitous Multimedia (MUM 2024). [160]
- **Habiba Farzand**, David Suarez, Thomas Goodge, Shaun Macdonald, Karola Marky, & Mohamed Khamis, Paul Cairns. "Beyond Aesthetics: Evaluating Response Widgets for Reliability & Construct Validity of Scale Questionnaires" In Extended Abstracts of the Proceedings of CHI Conference on Human Factors in Computing Systems (CHI 2024). [90]
- Vito Gentile, **Habiba Farzand**, Simona Bonaccorso, Davide Rocchesso, Alessio Malizia, Mohamed Khamis, & Salvatore Sorce (2023). User-Centered Evaluation of Different Configurations of a Touchless Gestural Interface for Interactive Displays In IFIP Conference on Human-Computer Interaction (pp. 501-520). Cham: Springer Nature Switzerland (INTERACT 2023). [108]
- **Habiba Farzand**, Karola Marky, & 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. As a Poster in the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022). [93]
- Mohamed Khamis, **Habiba Farzand**, Marija Mumm, & Karola Marky (2022, June). 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 (pp. 1-5). [157]
- **Habiba Farzand**, Florian Mathis, Karola Marky & Mohamed Khamis (2022, January). Trust & privacy expectations during perilous times of contact tracing. In Usable Security & Privacy Symposium (USEC 2022) in conjunction with NDSS. [98]

- **Habiba Farzand**, Kinshuk Bhardwaj, Karola Marky, & Mohamed Khamis (2021). The interplay between personal relationships & shoulder surfing mitigation. In Proceedings of Mensch und Computer 2021 (pp. 338-343). 🏆 "Honourable Mention Award" [91]

II

Chapter 2

A Systematic Deconstruction of Human-Centric Privacy & Security Threats on Mobile Phones

Abstract: Mobile phones are most likely the subject of targeted attacks, such as software exploits. The resources needed to carry out such attacks are becoming increasingly available and, hence, easily executable, putting users' privacy at risk. We conducted a systematic literature analysis to understand the relationship between resources and attack feasibility and present a categorisation of social engineering and side-channel attacks on mobile phones focusing on the resources attackers require. Our proposed categorisation levels facilitate an in-depth understanding of how mobile phone attacks can be executed using different combinations of partly simple resources. The analysis reveals that discrete protection mechanisms are insufficient to provide all-inclusive protection. The proposed categorisation assists in building novel solutions for safeguarding users' privacy from diverse attacks by carefully considering the potential misuse of resources. We conclude by outlining future research directions highlighting the urgent need for a holistic user defense.

Publication 1



Farzand, H., Abraham, M., Brewster, S., Khamis, M., & Marky, K. (2024). A Systematic Deconstruction of Human-Centric Privacy & Security Threats on Mobile Phones. *International Journal of Human-Computer Interaction*, 1-24.

2.1 Introduction

Social engineering and side-channel attacks are two commonly explored attack categories [10, 76, 144, 149, 173, 273]. Social engineering attacks refers to manipulating humans into revealing information or carrying out the attacks by influencing them [141]. Whereas, side-channel attacks exploit the leakage of devices to reveal information such as power consumption or electromagnetic emanation [258]. While any technological device could be a target of such attacks, handheld mobile devices are an attractive target for attackers, due to the rich data they can collect or data entered by users which could include personal information [135], health-related data [132], voice interactions [15, 20, 114] or emotional states [117, 188].

Methods to attack mobile devices are manifold [60, 178]. Yet, attackers mostly require specific resources to attack mobile users, such as a malicious app installed on the user's device or external requisites, like a video recording device, to capture the user's input. Prior work has proposed several taxonomies around social engineering or side-channel attacks [10, 144, 148]. Yet, the ease of attack execution based on required resources has not received in-depth attention from the research community. For this, we investigate the following research question:

RQ1: What resources are required to perform privacy and security attacks on mobile devices, such as social engineering and side channel attacks?

This paper addresses this gap by investigating the resources attackers need for successful attacks. To achieve this, we performed a systematic literature review on social engineering and side-channel attacks by selecting the top 10 publication venues in “Human Computer Interaction” and the top 10 publication venues in “Computers Security & Cryptography” according to the Google Scholar ranking system. Additionally, we checked papers published at SOUPS (i.e., the Symposium on Usable Security and Privacy, co-located with the USENIX Security Symposium) since it covers the intersection research of HCI and security. We extracted attack requirements from the systematic literature review, including resources (e.g., specific hardware, software or knowledge) from the resulting papers from the systematic literature review.

The resources required to perform a specific attack are quite versatile, making it challenging to compare different attacks to assess their likelihood or severity. Without categorisation, it is difficult to understand which attack is easier to perform than another. This directs us towards our second research question:

RQ2: How can privacy and security attacks be methodically categorized to reflect the ease of execution?

Using the extracted list of resources, we developed a categorisation that establishes a hierarchy of security and privacy attacks on mobile devices based on their required resources, indicating their ease of execution. Our proposed categorisation is four-layered: (1) Novice Attacks, (2) Intermediate Attacks, (3) Proficient Attacks, and (4) Expert Attacks.

Our investigation shows that possible attacks on mobile devices have become quite ubiquitous. They are no longer limited to the physical location of users. Furthermore, the barriers for laypeople without specific knowledge to becoming attackers are low due to recent advances in attack tools. Based on that, we can conclude that one does not even have to be a so-called "*script kiddie*" anymore because human capabilities (e.g., observation by looking at a device) and manual tools (e.g., paper and pen) are already sufficient to invade the privacy of mobile users. Our proposed categorisation assists researchers and practitioners in classifying (existing and future) attacks based on attack requirements. This knowledge helps estimate the scalability and frequency of privacy attacks and provides new perspectives in designing novel and comprehensive privacy-preserving mechanisms. Our categorisation further enhances the development of social engineering and side channel attack mitigation mechanisms and measures.

Research Contribution. The contribution of this paper is manifold:

- 1) **In-depth literature review:** We present an in-depth literature review about resources that attackers need to carry out attacks on handheld mobile devices.
- 2) **Categorisation based on requirements:** We systematically investigate the resources and organize them into a four-layered categorisation of (1) Novice Attacks, (2) Intermediate Attacks, (3) Proficient Attacks, and (4) Expert Attacks. Our categorisation provides an in-depth overview of attack resources.
- 3) **Highlighting the ease of attacks:** Our work shows that any individual can easily become an attacker, for example, by using human capabilities and manual tools. More sophisticated attacks can become more accessible for individuals due to the easily available resources such as malware. Finally, our research highlights the urgent need for a better defence of users on a more holistic level rather than placing an additional burden on users to opt for individual countermeasures for individual attacks or overloading them with the need to be aware of attacks 24-7.

2.2 Related Work

The first group of taxonomies focuses on one particular *category* of social engineering attacks. Among them, the taxonomy from Heartfield and Loukas specifically considers semantic social engineering attacks [130]. Semantic attacks are a category of social engineering attacks that perform an attack by manipulating object characteristics, such as system applications, with the purpose of deceiving as opposed to directly attacking the user. Heartfield and Loukas propose a baseline for classifying semantic attacks by breaking them down into their components and surveying the applicable defences. However, related work has shown that other categories of social engineering attacks can be carried out without interfering with the user-computer interface,

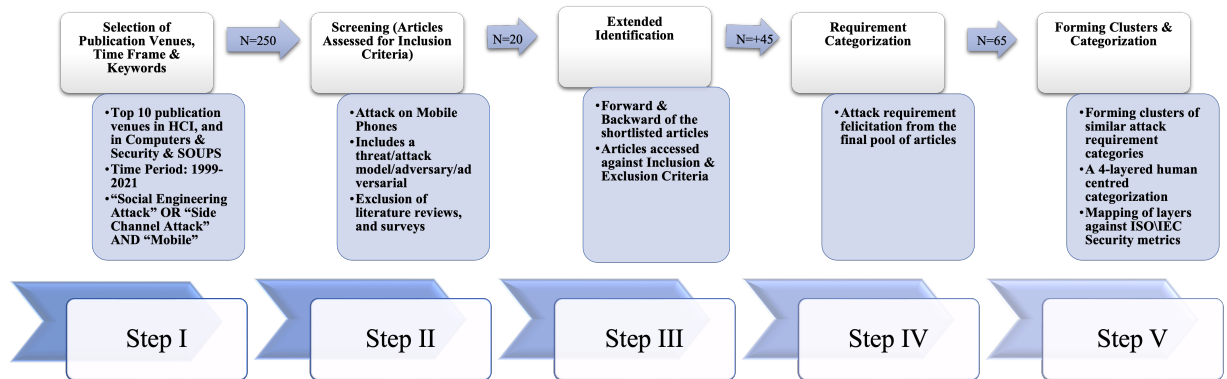


Figure 2.1: The figure shows the step-wise systematic literature review methodology we followed to develop the categorisation of Social Engineering and Side-Channel Attacks on Mobile Phones.

such as thermal attacks [12]. Other work focuses on hardware-based side-channel attacks and analyses the types, mitigation methods, targets, techniques, and methods [148].

The second group of prior work consists of surveys focusing on one particular *type* of social engineering attack, such as phishing [124]. In this context, Gupta et al. [124] discuss various methods to perform phishing attacks, their prevention, detection, and their role in the daily lives of people [124]. Gupta et al. reported that phishing is typically carried out on email spoofing or instant messaging and targets users with little or no knowledge of social engineering attacks or internet security. Gupta et al. further discuss various types of phishing attacks and prevention techniques. Prior work also presented surveys on side-channel attacks in the Internet of Things (IoT) and discussed several significant areas for research and improvement in security [76] while other researchers have also investigated side-channel attacks on critical infrastructures and relevant systems [289]. Recent work on security attacks on graphical passwords has explored various attacks for graphical passwords and their countermeasures through literature investigation [233].

While all these taxonomies and categorisations deliver valuable insights, they either consider one particular category of social engineering attacks or one specific attack type. This paper bridges this gap by presenting the first comprehensive evaluation of social engineering and side-channel attacks considering the resource-oriented nature of attacks from an attacker’s perspective. In doing so, different attack types can be compared to each other and evaluated for their ubiquity, frequency, and feasibility, which is important for designing adequate and comprehensive countermeasures.

2.3 Methodology

This section describes the steps of our systematic literature review on human-centred social engineering and side channel attacks on handheld mobile devices. The adopted methodology is illustrated in Figure 2.1.

Step 1: Key Words & Search Space: First, we identified keywords iteratively through discussions among three experts from the field. Our search query reflects our research focus on side-channel and social engineering attacks on mobile devices: (*social engineering attack** OR *side channel attack**) AND (*mobile** OR *mobile device** OR *mobile phone** OR *phone** OR *smartphone** OR *personal device** OR *handheld device**). We carefully tested the keywords the experts discussed to overcome the keyword selection bias and made a pre-search to ensure our keywords were not too limited in the search space.

As search space, we selected the top 10 publication venues in “Human-Computer Interaction” and the top 10 in “Computers Security & Cryptography” according to the Google Scholar ranking system (date accessed: May 06, 2021) and set the time of publication from 1999–May 2021 as 1999 is the year when one of the most influential human-centred security papers was published that strongly advocated considering human factors in the design of security mechanisms [6]. Since this paper marked the beginning of usable security and privacy research, we selected papers published after this year. We also checked papers published at SOUPS since this is a top venue for usable security and privacy research [79].

Step 2: Screening: The search results from Step 1 were then manually inspected for the location of the keywords within the full text. We further screened the papers, based on our inclusion criteria of having a threat, adversary or adversarial model. A threat model explains the vulnerabilities of a system [111] and details how an attack is performed against a target and which resources are needed by the attacker [243] from the perspective of an attacker or a defender [193, 215]. Threat models differ from adversary models because adversary models refer to goals, assumptions, and capabilities [262] representing a general approach to executing attacks. However, as noted by other researchers [80], threat and adversary models have been used interchangeably in the literature. To provide maximum coverage of relevant papers, we additionally included papers that provided an adversary model, an adversarial model, an attack model, or an attack overview. Each paper had to provide an attack overview, including a threat model, so that we can extract a complete list of resources the attacker needs without making any assumptions.

Step 3: Backward & Forward Search: For each paper identified in Step 2, we performed a backward and forward search using the same keywords to include any relevant papers published elsewhere other than the selected publication venues. We re-applied the exclusion and inclusion

criteria to the papers resulting from Step 3. The complete list of included papers included in the categorisation can be found in Appendix A.1.

Exclusion Criteria: Papers that included the keywords in references, paper classification, or author’s biography were removed from the analysis. We excluded papers that focused on devices other than mobile phones. Further, we excluded papers that were not peer-reviewed, such as papers on ArXiv, bachelor/master’s theses, and doctoral theses. For the doctoral theses, we checked the list of references for the same set of keywords and exclusion and inclusion criteria. A paper was excluded if the model description was incomplete and required subjective interpretation. We only included papers written in English. Lastly, we excluded papers with a model that just relied on coercing the victim, e.g., by using physical violence [49], because our research focuses on the resources and skills of attackers rather than coercion.

Step 4: Extraction of Resources: For each paper, one researcher extracted a list of requirements by copying the information given in the paper. Another researcher verified the resulting list. Next, we followed an inductive categorisation approach to cluster the requirements into groups until categorisation was no longer meaningful [208]. This resulted in seven clusters. Two researchers validated the clusters. We refer to the clusters of resources as *requirements*. The coding sheet for requirements can be found in Appendix A.2.

Step 5: Building the Categorisation: We used the seven clusters of requirements from the previous step to describe each attack identified in the papers. During this analysis, four levels of requirements that build our categorisation emerged: (1) Novice, (2) Intermediate, (3) Proficient, and (4) Expert.

To estimate the resource complexity of an attack in each category, we considered the *security levels* defined by the ISO/IEC Security metrics [1, 11, 63]. The ISO/IEC Security metrics are international standards that address cybersecurity used in many research papers such as [207]. The *security levels* in particular describe the *measure of confidence that the System Under Consideration, Zone, or Conduit is free from vulnerabilities and functions in an intended manner*” [11, p.8]. More specifically, the ISO/IEC Security metrics describe the level of protection from the system view, considering different types of attackers based on the resources needed to attack a system. These levels are quite generic yet provide a way to protect a system. By mapping the resulting categories of attack resources, we show how easy or difficult an attacker can attack a mobile device. The ISO/IEC 62443 security levels [1, 11, 63] are as follows¹:

SL0 “No special requirement or protection required”

SL1 “Protection against unintentional or accidental misuse”

¹Please note, that we only consider the attack perspective in terms of requirements and not the protection of the attacked system.

SL2 “Protection against intentional misuse by simple means with few resources, general skills and low motivation”

SL3 “Protection against intentional misuse by sophisticated means with moderate resources, (IACS-specific) knowledge and moderate motivation”

SL4 “Protection against intentional misuse using sophisticated means with extensive resources, (IACS-specific) knowledge and high motivation”

Limitations: Like most literature reviews, our work has several limitations. First, our literature review was conducted in May 2021. Papers published after this time are not considered. We selected “social engineering attacks” and “side channel attacks” as search keywords based on an expert discussion and keywords from relevant papers to focus our search. However, there might be further papers published on these topics that do not include our selected keywords in the full text. Papers that did not match the screening criteria were excluded from the analysis. While this might have shrunk the space of outcome, it produced a final list of papers focused on the criteria mentioned above. Papers that provided fuzzy information about attacks left too much room for subjective interpretation, which would have threatened the validity and reproducibility of our work. Lastly, some of the publication venues did not offer a search function, such as the USENIX Security Symposium. For this, we used Google Scholar to elicit relevant papers. Some papers may have been dropped due to the limitations of Google Scholar as the search engine.

2.4 Requirements of Human Centred Attacks on Mobile Phones

In this section, we detail the requirement categories that we extracted from the literature. From the final set of papers, we extracted seven categories of requirements. We detail them below with explanations and examples that an attacker may utilise to perform social engineering or side-channel attacks.

1) *Software Tools*: Refers to benign programs that make use of sophisticated algorithms but are not specifically designed for malicious use. Examples include a remote server, software that implements an n-gram Markov Model, or software that collects fine-grained accelerometer data.

2) *Mobile Phone App*: A specific app that needs to be installed on the victim’s device that is specifically designed for malicious use. Examples include spyware and phishing apps.

3) *Advanced Programming*: Advanced programming expertise from specialized fields of programming. Examples include knowledge of implementing and executing deep learning, or image processing algorithms.

4) *User Phone Permissions*: Access to specific sensors and resources that are guided by permissions on the victim’s device is required to execute the attack, such as access to WiFi.

5) *Hardware Tools*: External electronic hardware tools are required in the attack setup. Examples include charging cables and wireless routers.

Expert Attacks	Advanced Programming	Software Tools	Mobile Application	User Phone Permissions	Hardware Tools	Human Capabilities
	Advanced Programming	Software Tools	Mobile Application	User Phone Permissions	Hardware Tools	
	Advanced Programming	Software Tools	Mobile Application	Hardware Tools	Human Capabilities	
	Advanced Programming	Software Tools	Mobile Application	User Phone Permissions		
	Advanced Programming	Software Tools	Hardware Tools	User Phone Permissions		
	Advanced Programming	Software Tools	Hardware Tools	Mobile Application		
	Advanced Programming	Software Tools	User Phone Permissions			
	Advanced Programming	Software Tools	Mobile Application			
	Advanced Programming	Software Tools	Hardware Tools	Human Capabilities		
	Advanced Programming	Software Tools	Hardware Tools			
	Advanced Programming	Software Tools				
	Advanced Programming	Mobile Application	Hardware Tools			
	Advanced Programming	Mobile Application	Human Capabilities			
	Advanced Programming	Mobile Application				
Proficient Attacks	Software Tools	Mobile Application	User Phone Permissions	Hardware Tools	Human Capabilities	
	Software Tools	Mobile Application	User Phone Permissions			
	Software Tools	Hardware Tools	User Phone Permissions			
	Software Tools	Mobile Application				
	Software Tools	Hardware Tools	Manual Tools			
	Software Tools	Hardware Tools				
Intermediate Attacks	Software Tools	Human Capabilities				
	Mobile Application	Hardware Tools	User Phone Permissions			
	Mobile Application	User Phone Permissions				
Novice Attacks	Human Capabilities	Hardware Tools				
	Human Capabilities	Manual Tools				
	Human Capabilities					

Figure 2.2: The figure shows the categorisation of Human Centred Social Engineering and Side Channel Attacks on Mobile Phones from the Perspective of an Attacker. We developed this categorisation based on the resources extracted from the papers resulting from the systematic literature review.

6) *Human Capabilities*: Resources that fall within the physical and personal abilities of humans, such as physical access to the device, close proximity in distance, knowledge about the victim, and target observation.

7) *Manual Tools*: Refers to non-electronic/non-powered devices or tools. Examples include pens and pencils.

A visual representation of the categorisation can be found in Figure 2.3.

2.5 Glossary of Attacks

We propose four categories: (1) Novice, (2) Advanced Beginner, (3) Proficient and (4) Expert (see also Figure 2.3). When detailing each layer, we also map it to the ISO/IEC Security metrics [1, 63] and present options to counter specific attacks. The following sections detail each of the categories and respective subcategories. Figure 2.3 shows the visual representation of the categorisation.

2.6 Level 1: Novice Attacks

All attacks at this level exclusively rely on human capabilities, manual tools, and basic hardware tools. Human capabilities, such as making observations through human sight, do not require the attacker to acquire special expertise in using specific equipment since the requirements needed to perform the attack are within the capabilities of a human. Manual tools like pens and pencils are



Figure 2.3: The figure shows the categorisation of attacks in four levels from an attacker's perspective. The expertise required to perform an attacker increases as we progress in categorisation levels.

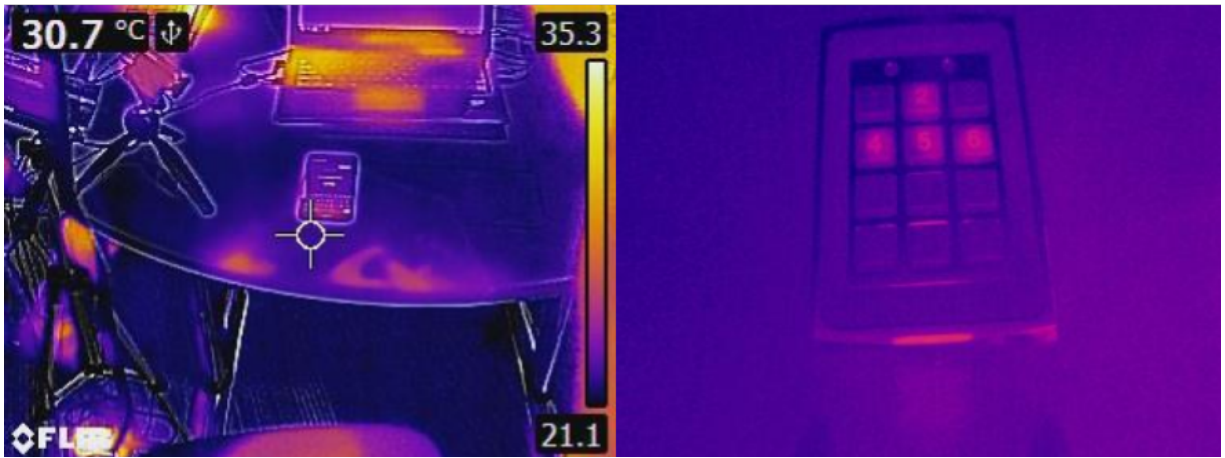


Figure 2.4: The figure shows a thermal image of smartphone authentication captured using a thermal camera, i.e. a Flir camera. The authentication information can be easily observed by observing the heat traces. This is a typical scenario of Thermal Attacks that belongs to the category of Novice Attacks.

readily available and accessible. Basic hardware tools, such as specific cameras, are easy to buy and use. It does not require training or a special setup to use. Given this, the attacks with such requirements can be labelled as “novice attacks”. Considering ISO-IEC Security standards [63], this attack category corresponds to **SL0** and **SL1** because no special requirements are needed. The following clusters of requirement categories fall under Novice Attacks.

2.6.1 Human Capabilities

By utilizing the human capability of making observations through sight or using personal information about the victim, an attacker can uncover the victim’s mobile device content, replay the gained knowledge to gain unauthorized access to the user’s device or transfer SIM contract details to another SIM card number. Attacks such as zero effort, replay, and mimicry [306] can only be efficiently performed using human capabilities. No external resources are required. Similarly, a SIM swap attack [183] can be performed by convincing the carrier to update the SIM card linked to the victim’s phone. For this, the attacker only needs to know the victim’s name and phone number and have access to auto-refill interfaces. Shoulder surfing (traditional) [82,211] - also referred to as one of the out-of-device threats [96], is another attack that can be performed by making observations of the victim’s device screen. The attacker can uncover confidential and private information by observing the screen as the victim interacts with the device. Though shoulder surfing is mostly reported on smartphones [85,94], its evidence is found in interaction with multiple tech devices such as Virtual Reality, and researchers have proposed numerous mechanisms to combat it [139,298].

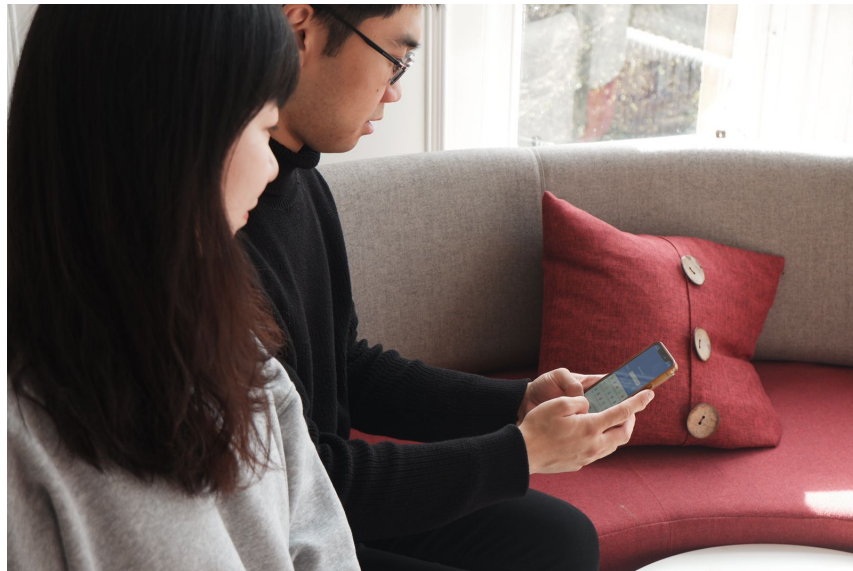


Figure 2.5: The figure showcases one of the common scenarios of shoulder surfing - a type of Novice Attack - in the daily lives of users where the bystander uses direct observation to make observations of the screen and is able to retrieve personal information about the user.

2.6.2 Human Capabilities & Manual Tools

By utilizing the human capability of making observations through sight with some manual tools, an attacker can uncover the victim's mobile device content with which the victim interacts. Adding manual tools to human capabilities contributes to the attack's success. An example of such an attack is shoulder surfing (advanced). The traditional shoulder surfing attack is advanced by adding manual tools for note-taking, such as a pen or pencil. The attacker aims to capture the victim's device authentication pattern (such as Pass sketches [311]) by observing their input.

2.6.3 Human Capabilities & Hardware Tools

Utilising human capabilities and some basic hardware tools, such as a recording device, can assist an attacker in performing several attacks, especially authentication-based attacks. Examples of such attacks include pattern lock attacks [175], smudge attacks (traditional) [18], microscope attacks [18], and thermal attacks [18]. In the case of a pattern lock attack, the attacker is close to the victim and uses a recording device (for example, a smartphone's camera) to record authentication steps, including input patterns and gestures. Then, the attacker gets physical access to the victim's device to unlock it. Similarly, to perform smudge attacks, an attacker inspects smudge residue left by the victim's fingers on the device to reconstruct credentials. For this, the attackers need physical access to the device and some hardware tools, such as a compact camera to capture the smudges on the screen and a hard light source to get the edged shadows. By manually inspecting the image, the attacker can reconstruct the credential.

Authentication information a user enters can be uncovered by utilizing a microscope attack.

For this, the attacker has to be in close proximity to the target device and then use a high-definition camera to capture an image of authentication while it is being performed. The attacker can then utilise a microscopic device, such as a USB microscope with 400x magnification, to deduce the entered information. Like a microscope attack, authentication information can be uncovered using a thermal camera. When using a thermal camera, the attacker needs a thermal camera and should be close to the user or have physical access to the device. The attacker can then capture a thermal image of the screen right after the authentication information has been entered, and then, by manual inspection, the attacker can unveil the entered information. Figure 2.4 and 2.5 shows an exemplary scenario of thermal attacks and shoulder surfing.

2.7 Level 2: Intermediate Attacks

Attacks belonging to this category require limited effort for practical implementation, namely, a combination of mobile apps, hardware, and manual tools, as well as human capabilities. Hardware tools are easily accessible and offered at cheap prices by various vendors. Hence, access to hardware tools is no longer a difficult task to accomplish. Manual tools and human capabilities also come at a minimal price and effort. Hence, the only arrangement the attacker needs to make is to prepare a mobile application. With a combination of a mobile app with hardware tools, human capabilities, and manual tools, various attacks could be performed. Considering ISO-IEC standards [1, 11, 63], this attack corresponds to **SL2**. The following lists the combinations of requirements that attackers can utilise to compromise a victim user's privacy and security.

2.7.1 Mobile Apps

A mobile app can be used in a malicious way to learn sensitive information about users. A classic example is clickjacking [234], where by clicking on an overlay created over the victim app, an attacker tricks the user to, e.g., grant permission. The overlay is created by a malicious app, which is opaque in the foreground. While thinking about performing a legitimate action, the user only visually sees the victim app while running in the background while interacting with the malicious app. This way, only through developing a mobile app and tricking the user into installing it on his device the attacker learns the sensitive information. Indistinguishably, a cache-based timing attack [315] also requires only a mobile app. The mobile app is used to extract sensitive information by exploiting the cache contention between the normal world and the secure world.

2.7.2 Mobile Apps & User Phone Permissions

A mobile app with few permissions can perform a resource race attack [38]. The race between mobile apps to access resources can be exploited to steal sensitive information. For example, a

malicious app can steal sensitive information from a legitimate app that captures it, e.g., photos.

2.7.3 Mobile Apps, Hardware Tools & Phone Permissions

With the addition of hardware tools to a mobile app with access to some target phone permissions, an attacker can perform an activity interface inference attack [308]. The goal of this attack is to uncover the user's app activity. The attacker makes use of the shared memory side-channel information. The attacker develops a malicious app with access to the Internet as well as the device storage and installs it on the victim's device. The app continuously collects information about the foreground application processes and uses it in a training data phase to build an activity signature database. Then, in the attack phase, the malicious app sends the collected characteristic data to a server for calculations. It then uses the signature database to uncover the activity.

2.8 Level 3: Proficient Attacks

The attacks falling in this category require increased effort, resources, and capabilities. The development of a mobile app along with software tools is necessary to perform the attacks. Phone permissions are not difficult to access. Most attacks require Internet permission only, which is marked as a "PROTECTION_NORMAL" by Android [103,259]. Moreover, it has been observed that users do not pay attention to the permissions being granted to apps [99]. Hence, it has become easy for an app to get access to permissions. The complex part of this category is that the attacker must have software skills and must know how to develop malicious apps. There are multiple ways to manipulate the user to install malicious apps without realizing the malicious intent behind them (cf. [112]). Considering ISO-IEC standards, this attack category corresponds to **SL3**.

2.8.1 Software Tools & Human Capabilities

Pattern-based authentication systems could be attacked and leaked while using software tools along with human capabilities. Dictionary-based pattern guessing attacks [58] are a blueprint of such attack categories. A Pattern Dictionary-Based attack requires physical access to the target device and trying the most probable unlock patterns to access the phone. The goal is to unlock the phone in less than 20 trials because mobile OSes lock the phone and require their users to log in through their mobile OS account after 20 failed attempts. To unlock the phone in 20 attempts or less, the attacker uses a probabilistic password model, such as the n-gram Markov model [196]. This model could be trained using real-world data of unlock patterns. While this attack is easy to carry out, this attack methodology cannot be applied to every mobile OS.

2.8.2 Software & Hardware Tools

Adding hardware tools to software tools can assist an attacker in performing channel state information-based attacks [313]. In such an attack scenario, the adversary aims to access sensitive information entered on the victim's device. To make this attack possible, at least one or two wireless devices, such as a wireless router, a laptop, or a smartphone, must be placed within 0.5-5 meters distance from the target device in a static setting. The wireless devices must support ICMP protocol and communicate CSI readings.

2.8.3 Software, Hardware & Manual Tools

A new kind of charging attack called juice filming attacks [147, 210] can be performed using software tools with the assistance of hardware and manual tools. In a typical juice filming attack, the attacker records user inputs, e.g., by a VGA/USB interface that is connected to the smartphone via a malicious charger [210]. The VGA/USB interface is concealed in the user's environment. No app needs to be installed on the target smartphone, and no user permission is required.

2.8.4 Software Tools & Mobile Apps

GUI-based [29, 101], memory footprint [145] and cross-app side-channel attacks [317] can be executed when software tools are combined with a mobile app.

With the goal of performing a GUI-based attack, which is sometimes also referred to as Pixel Perfect Phishing Attack [101], the attacker makes use of a malicious app installed on the victim's phone. The app has the ability to merge multiple attack vectors, such as UI-intercepting draw-overs [100, 220], toast messages [220], non-UI-intercepting draw-overs [100, 194, 220] and enhancing techniques, such as app repackaging [126, 321, 322], accessing the proc file system [145] to perform attacks. The malicious app presents itself as a benign app, e.g., as a utility. When the malicious app is launched, it monitors other apps on the victim's phone and waits until a target app is launched. The malicious app can be a look-alike version of the target app that discloses any information entered into a remote server.

Similarly, in a memory footprint attack, again, a mobile app with some software tools is sufficient to bypass user privacy. In a memory footprint attack, two processes (victim and attack process) running in parallel on the same host can learn the secrets of web browser processes by tracking the changes in the app's memory footprint. As a first step, the attacker profiles the target program and creates an attack signature database through a malicious app. Next, the attack process measures the memory footprint of the victim process. The attacker can download the activity signature database or send the attack memory footprints to a remote server for matching.

Using the same set of resources as required to perform a memory footprint attack, an attacker is capable of performing cross-app side-channel attacks. This attack exploits side-channel infor-

mation leakage on the OS level. A malicious app is installed on the victim's device, runs in the background and collects traces for each event of interest. For each time series, the difference between two consecutive points is noted, and then SAX transformation and BOP construction are performed. Next, the attacker converts BOP into LibSVM and uses LibSVM to perform classification. RBF kernel could be used for SVM classification and a probability model to perform cross-validation.

2.8.5 Software Tools, Hardware Tools & User Phone Permissions

When user phone permissions are complemented by software tools with the addition of some hardware tools, attacks like keystroke inference can be easily implemented. CSI-based keystroke inference attack [185] is a classic example of such attack resources. Users who use public WiFi can be victims of CSI-based keystroke inference attacks. To perform this attack, the attacker requires the victim's device to be connected to public WiFi. This is commonly seen in public spaces such as restaurants, shopping malls, airports and alike. The WiFi hotspot usually has an application layer security (HTTPS) that helps in gaining user trust that the connection is safe. Upon getting the device connected, the WiFi hotspot collects CSI from the victim's device through ICMP protocol/ Further, through a directional antenna, the noise in CSI is eliminated. Li [185] proposed an algorithm for keystroke recognition. They adopted a low pass filter to remove high-frequency noises and Principal Component Analysis to reduce the dimensionality of the feature vectors. They also proposed a context-oriented CSI-collected method to recognize the PIN input.

2.8.6 Software Tools, Mobile Apps & User Phone Permissions

A combination of software tools and mobile applications with access to permissions can assist in performing fingerprinting and performance degradation attacks such as Quality of Service (QoS) attack [142] and sensitive apps fingerprinting attack [231]. To perform a QoS attack, a malicious app on the victim's device creates a sticky background service. The malicious app only requires permission to use stats from the user. A cache profiling tool is then run to obtain spanning addresses to perform the exotic atomic operations. Upon detecting the victim app, the Exotic Atomic operations start and degrade the QoS of the victim's app. This loop keeps on running until the app is not in the foreground. Then, the QoS degradation attack is stopped, and the system bottleneck is released as soon as the user quits the victim app. This procedure keeps on repeating until the app is removed from the phone. Sensitive app fingerprinting attack [231] also works in a similar fashion to QoS attacks. In a sensitive app fingerprinting attack, There are multiple ways in which a malicious app, depending on its permissions and privileges, can uncover what other app installed on a victim's device. For example, a malicious app can easily check if a specific target app is installed on the victim's device by using specific API calls,

access to the device storage or a VPN service. With some special permissions, a malicious app can get the list of running processes or infer the UI states. With debugging privilege, the app can retrieve the list of package names and learn the path to the installation file of a specific target app. Further, a curious app can also achieve this by using multiple API calls.

2.8.7 Software & Hardware Tools, Mobile Apps, Permissions & Human Capabilities

Interfaces, e.g., for financial transactions, can be maliciously targeted when software tools are used in addition to a mobile app with access to permissions and hardware tools and human capabilities such as UPI-based attacks [176]. Multiple attacks could be performed on payment interfaces, such as unauthorized registration by using a user's phone number, unauthorized bank transactions using the victim's phone number, and partial debit card number, and unauthorized transactions without the debit card number. To perform these attacks, the attacker uses a rooted phone and reverse engineers the payment apps. Debug statements are then added and repackaged with signature statements from the attacker. The attacker then releases the repackaged version as a malicious app that requests Internet access and access to SMSes and the phone state. The victim downloads the app and grants the permissions. Then, by following the standard procedure of signing up and granting permissions, the attacker reveals sensitive information and is able to perform malicious activities.

2.9 Level 4: Expert Attacks

The attacker in this category is a resource-rich adversary that makes use of various combinations of resources, such as mobile phone apps, software tools, advanced programming, hardware tools, and access to phone permissions. In some cases, manual tools and human capabilities are also required. The requirements make the attacks sophisticated and require expert knowledge to implement them. Hence, such attacks can be labelled as "Expert Attacks". Considering ISO-IEC standards, this attack corresponds to **SL4**.

2.9.1 Advanced Programming

Only through advanced programming expertise, an attacker is well-equipped to perform an attribute inference attack [146]. To perform an attribute inference attack, the attacker uses public data (such as review data) and a machine learning classifier to get a victim user's private attributes, such as location. The machine learning classifier is a multi-class classifier that takes review data as input, and by using a training dataset gets the city lives of the victim. The public data is easy to collect and can be found on public profiles, such as social network profiles.

2.9.2 Advanced Programming & Mobile Apps

Equipping a mobile application with advanced programming can result in inference attacks and microarchitectural attacks [106]. In an inference attack [276,277], there are two phases; training and attack. In a training phase, the attacker builds templates for information leaks, e.g., by collecting API calls and dynamic time warping. In the attack phase, the attacker distributes a malicious app that does not require any permission. The app observes identified information leaks and infers corresponding events. This type of attack is similar to the activity interface inference attack [308] detailed above, yet requires different resources and reveals other kinds of information. Likewise, microarchitectural attacks [106] steal data using a diverse range of side channels or corrupt data using hardware vulnerabilities. The attacker has access to an integrated GPU either by deploying a malicious app or directly through malicious scripts when a user visits a website. The attacker only makes use of primitives of the GPU.

2.9.3 Advanced Programming, Hardware Tools & Human Capabilities

Reflections of a virtual keyboard can be compromised to leak sensitive information with the aid of advanced programming, hardware tools, and human capabilities. Such attacks are referred to as reflection-based attacks [240]. In this attack, not just capturing a video of the virtual keyboard of the victim's phone but also the reflection of the virtual keyboard on reflective screens, such as the victim's sunglasses, could reveal what the victim typed. This attack requires the attacker to be somewhere near the victim and video-record the user interaction through a video recording device either by directly observing the screen or by observing the reflections of the screen in nearby objects. The attacker can also install a video recording device in the victim's environment to minimize the attacker's noticeability. After the video recording, the attacker works on acquiring stable frames of the video sequence which are then used for stabilizing image transformations. Next, the video frames are aligned against a reference image of the victim's phone. The attacker then trains the classifiers to detect the keypresses made by the victim. The output is refined by building a language model that also serves the purpose of filling in the missed detections.

2.9.4 Advanced Programming, Mobile Apps & Hardware Tools

The timing of sensitive user interfaces can be leaked to perform a power analysis attack. To perform such an attack, the attacker requires advanced programming, a mobile app, and hardware tools. An example of such an attack is the power analysis attack [122]. A power analysis attack requires a malicious app to be installed in the OS environment in which the victim's app is running. The goal of the attack is to know the timing of the sensitive UIs as they appear on the smartphone screen. The attacker then performs the next steps to disclose the confidential information. When the malicious app is in the process of misusing the power side channel, it

functions in the background and records the power data while the target app is running in the foreground. The malicious app tries to infer the sensitive UI of the victim app based on the collected power traces. After the identification of the target UI, further attacks can be carried out.

2.9.5 Advanced Programming & Software Tools

A combination of advanced programming and software tools can be used to perform severe attacks such as a memory disclosure attack [118]. Unlike most attacks, this attack does not require the installation of a malicious app on the victim's device. All it requires is for the victim user to visit a website that contains the attacker's malicious code. Through this, the attacker can uncover which apps run on the victim's device, user activities, and the specific web pages open on the victim's device. This attack has one condition to be successful, i.e. page deduplication should be enabled on the smartphone. It then exploits page deduplication to perform a memory disclosure attack. This attack has 3 steps: 1) filling a page with expected data to be found on the victim system through malloc implementation, 2) waiting for the operating system or hypervisor to deduplicate the attack arrays, 3) and lastly measuring the write-access time to know whether a page has been deduplicated.

2.9.6 Advanced Programming, Software Tools & Hardware Tools

An amalgamation of software and hardware tools with advanced programming can be leveraged by an attacker to perform attacks like a remote screen attack [186] or mobile social network attack [225]. Through a remote screen attack, it is possible to exploit the screen display. The victim merely needs to have a website containing a malicious script. This attack works by exploiting the display mechanism using liquid crystal (LC) elements that act as a passive signal modulator and LCS response that contains screen information. An RF signal processing scheme, including a deep learning model, assists in the wavelet analysis, which is then followed by the spectrogram feature augmentation. Based on this concept, Li et al. [186] modelled a proof-of-concept by developing "WaveSpy" - a remote screen inference system that uses mmWave-based LCS response to get real-time sensitive information without any knowledge of the screen and that too through the wall.

Along the same lines, a mobile social network attack aims to get user traces from a smartphone with the use of an external sound card. To perform this attack, devices such as Alcatel POP3 are needed. In the training phase, a clean run utilizing sandbox proposed by [225] is executed. Then, the traces are analysed. The next step involves raw data pre-processing and is done for the subsequent neural network analysis. Following this, trace synchronization is achieved. The attackers are then able to detect crypto computation signals.

2.9.7 Advanced Programming, Software Tools, Hardware Tools & Human Capabilities

When advanced programming, software and hardware tools are merged together with human capabilities, attacks like advanced smudge attacks [47, 263], and website fingerprinting [275] or video-based attacks [264, 309, 309, 312] can be easily done to invade users' privacy and bypass security.

Advanced smudge attack requires examination of smudges left on the device screen after it has been used by the victim. This requires physical access to the victim's device. To analyze the smudges, attackers can use (1) image processing to infer possible patterns from the smudges by pre-processing [42, 205], e.g., by OpenCV [227], and (2) sorting patterns based on the occurrence probabilities computed using n-gram Markov model which is built using real-world pattern data-sets or using deep learning. Similarly, website fingerprinting attacks could be performed with the help of a malicious app running in unprivileged mode and monitoring incoming and outgoing traffic statistics from `tcp_rcv` and `tcp_snd` of a target app. This data acts as training data. After collecting the data, the malicious app looks for relaunching of the target app. It then gathers traffic data from `tcp_rcv` and `tcp_snd` again and matches the collected data with previous training data to infer the sensitive information. The collected data could also be sent to a remote server for analysis and for matching the device name of the attacked device with the training devices available

Another way to steal authentication credentials using the same set of resources is to observe and video capture the hand movements of the victim when they are typing the password [264] or unlock pattern [309]. The video could be captured using any video recording device, such as a smartphone, a camcorder, or through surveillance camera footage. The resulting footage can be analyzed by different means, including TLD Tracking Tool [151] for tracking the anchor hand point and the anchor point on the apparent side of the mobile device, edge detection [293], and further computer vision tools, to reconstruct the user input. For example, the attacker can build a probability-based password model using two large data sets: 1) UNIQPASS v15 Password Data set [260], and 2) Video data set for computer vision analysis.

2.9.8 Advanced Programming, Software Tools & Mobile App

Treacherous attacks such as cross-cache [191] or flush-reload side-channel attacks [318] can be performed by combining advanced programming with software tools and a mobile app. Cross-cache attacks require a malicious app that does not prompt any permission. This attack can monitor the activity of the GPS sensor, camera or Bluetooth. This information leak can help the attacker to know details about the victim. In a learning phase, a template matrix is computed to see how many cache hits occur on a specific address. Then, in the attack phase, this matrix is used to infer events from the cache hits. The events could be stimulated via the android-debug

bridge (adb shell).

Using the same resources as required by cross-cache, flush-reload side-channel attacks make use of a malicious app packaged together with a native component that is compiled with Android NDK. The attacker is equipped with the knowledge of C and C++ programming languages.

2.9.9 Advanced Programming, Software Tools & Permissions

The inviolability of user's privacy can be bypassed by exploiting AdSDKs attack [272], which is a fusion of advanced programming, software tools and phone permissions. Not just malicious apps but also malicious ads displayed can infer sensitive information about users by accessing external storage. The most important asset in this attack is an ad-supported app that runs on the target user's device and shows malicious ads in a confined WebView instance. For instance, the attacker can trick the victim into downloading an HTML page that holds a malicious payload. After the payload page is presented to the user, the attacker's ad calls the payload by opening this page within the same WebView where the ad is running.

2.9.10 Advanced Programming, Software Tools, Hardware Tools & Mobile Apps

Combining advanced programming with software and hardware tools and mobile apps can enable complex attacks, such as power analysis or inference attacks on processors.

An inference attack [121] on the processor requires a permission-less malicious app to be installed on the victim's device. The attacker can acquire knowledge of running apps, launching websites, and streaming videos. In the training phase, the attacker builds a machine learning/deep learning model on a training device similar to the victim device by recording the raw LLC profiles of target apps, websites, and videos. The trained models are then integrated into the app and published on the app store. In the second phase, the malicious app prepares eviction sets for profiling the LLC on the target device, followed by extracting vector features. They are then classified with already trained models to infer sensitive content, including opened applications, websites, and streaming videos.

Parallel to inference attack on the processor, power analysis side-channel attack [307] uses the unprivileged power consumption traces, to infer sensitive UIs, guess password lengths, and also estimate geolocations. A malicious app running in the background collects power traces continuously. The power patterns can be collected either through hardware-based methods (e.g., a Monson Power Monitor) attached to the target smartphone or through software-based methods (e.g., directly polling voltage and current readings within the mobile system). The collected power traces can then be analysed to infer confidential data. A malicious app's key role in this scenario of exploiting PSCs is to achieve automatic detection of pre-learned power patterns. This can be achieved by pattern matching or machine learning algorithms, e.g., dynamic time

warping (DTW).

2.9.11 Advanced Programming, Software Tools, Hardware Tools, & Permissions

Signal reflection information can be targeted with the help of advanced programming, software and hardware tools, and permissions. A wireless transmitter-based attack [314] collects signal reflection information before the user starts to unlock a device until the user ends up unlocking the device. In [314], researchers proposed an approach to performing this attack called; WiPass. They collected CSI data and used discrete wavelet decomposition to remove noise from obtained signals. (1) WiPass removes the noise from collected signals using a two-level Symlet filter, (2) uses the DCASW to extract the features to build the finger motion profiles and finally as the last step, (3) uses a hierarchical dynamic time warping (DTW) approach to recognize the unlock passwords.

2.9.12 Advanced Programming, Software Tools, Mobile Apps & Permissions

Attacks similar to GUI squatting [55], gesture typing [266], and keystroke attacks [230] are feasible to perform if a mobile app and permissions are complemented with advanced programming and software tools.

In a gesture typing inference attack [266], gesture typing keyboards are the target. It involves a malicious app running with Internet access. The malicious app observes and records publicly available events from the system while the user enters text in the victim app. The malicious app can only record the signals, i.e. the counters, but not the words themselves. For each word entered by the user, a series of events is observed in the system that can be used as a fingerprint to recognize the word entered. Supervised machine learning (Recurrent Neural Network (RNN)) is used to remove noise from the data. The fingerprint is constructed from the training data and is used to infer sentences entered later in the victim app. The RNN outputs for each word signal in a sentence signal a probability that the word signal corresponds to a particular word in the dictionary. The data is sent to remote attackers.

GUI squatting attack [55] refers to automatically generating phishing apps using image processing and deep learning techniques. The automatically generated phishing apps have the ability to steal sensitive information by taking screenshots of login screens. The generated apps require Internet permission to upload the collected sensitive information to a remote server. To generate phishing apps, image processing techniques, such as canny edge detection [228] and edge dilation [226] are used. The GUI components are classified with a deep learning algorithm, i.e. a CNN. Then, these components are arranged to generate layout code matching the XML file for the imitation of the original apps. Then, the deception code is designed for the interactive

components, and a response is assigned to each interactive component. Chen et al [55] implemented this approach using Python and several open-source libraries, such as OPENCV [227] and OCR techniques [223].

Keystroke attacks through accelerometer readings [230] involve a malicious app running in the background collecting accelerometer readings. By using machine learning (e.g., Random Forest Algorithm [134]), the text entered on a device is extracted from accelerometer readings. The app requires network access for uploading the collected data and access to fine-grained accelerometer data. This attack involves keypress segmentation, probabilistic keypress classification and sorting keystroke sequences by maximum likelihood. A probabilistic error model is constructed for sorting keystroke sequences by maximum likelihood.

In a Pin Skimmer attack [265], the user installs a malicious app and has root access to the device. This attack requires access to the camera and microphone. A smartphone with two operating systems (e.g., Android and TrustZone OS) that operate in parallel are required to perform this attack. The malicious app cannot access sensitive information available on the TrustZone OS, even with root access on Android OS. The sensitive information apps are launched in the Trusted OS. The rootkit retains access to certain shared resources like an accelerometer, camera, GPS, microphone, and like. Using the front video camera and the microphone, the Pin Skimmer attack collects all user-pressed events entered into the sensitive app and records them using the front camera in a video file with audio. It saves the image to disk, and the attacker then uploads the collected data to a remote server where, through image processing skills, the exact PIN is retrieved. Support Vector Machine (SVM) [323] was implemented as a learning algorithm with open source libraries LibSVM [50] and Weka [21].

A user's metro location can be inferred through a malicious app that reads accelerometer and orientation sensor data and uploads the readings to a remote server [138]. This location inference attack aims to reveal what a target user's metro ride trace is. It accomplishes its mission by noting the differences between distinct station interims leading to distinct macro motion characteristics that are captured by the motion sensors of the victim's smartphone. The readings are then analysed, and machine learning algorithms are used to identify the victim's ride intervals.

Recording tap sounds and vibrations while an application is running from the stereo-microphones and gyroscopes of a smartphone, can be maliciously used to perform a keystroke inference attack [216]. To perform this attack, a malicious application like a custom keyboard is presented to the user to collect typing behaviour for the purpose of training a model. The microphone requires permission during installation, but this permission can be justified with the aid of any feature offered by the malicious application. After monitoring the victim's behaviour, the malicious application uploads the collected data to a remote server. After training, it listens to the keypresses in the background from the sensitive Android applications. Then the application detects the point of interest location of the victim using GPS or cellular or wireless networks,

then the malicious application collects gyroscope and microphone data. A fast Fourier transform filter could be used to detect frequencies corresponding to the sample tap values.

Ambient light sensors could also be exploited to perform attacks on user input such as PINs [274]. They can be accessed via the Android Sensor API. To perform such an attack, a malicious application is used to collect the light-sensor information while the user is interacting with the device. The malicious application tricks the user into the application in a manner similar to inputting PINs. It then uses this data as the training data. Malicious applications also require an internet connection to have powerful servers for machine learning algorithms. After collecting sufficient samples, the malicious application again tricks the victim user into restarting the device or the victim application. This is done to capture the ambient-light sensor information during PIN input of the victim application. Then by means of machine learning, the PIN input is retrieved. Matlab statistics toolbox can be used to determine the PIN entered.

App fingerprint attacks [206] could be performed by exploiting magnetic sensor measurements to infer current activities on the smartphone. Therefore, fingerprint browsing and app activity are possible. For this, a malicious app with Internet access and access to zero-permission sensor information is required. To fingerprint the browser, the victim opens a webpage that is controlled by the attacker. The webpage has at least some malicious component belonging to the attacker, such as ads. Magnetometer readings are collected continuously and the attacker attempts to identify the launched apps or websites with the help of a supervised learning approach. The malicious app gathers the labelled traces for all websites and apps. The learning could be performed on numerous devices that the attacker holds or accessed using cloud testing platforms. In the case of website fingerprinting, the learning phase could also be done on the victim's phone. Principal component analysis is performed on the magnetometer data, and random forest is used to classify the traces.

An inference attack through interrupt timing attack aims to discover the unlock pattern or sensitive information entered by the target user [77]. Diao et al. [77] proposed a novel way of doing this by tricking the target user into installing a malicious app. The malicious app requires no permission from the user as it works by reading interrupt statistics which are public to any process and contain information about all running devices. This information is used to infer sensitive information passing through the running devices. This attack can collect two types of sensitive information, unlock pattern and UI information. After collecting the unlock pattern information, it could be uploaded to a remote server for which INTERNET permission will be required. The UI information could be used for further malicious attacks such as phishing. In Diao et al.'s implementation of the attack, they used native C and Java with Android NDK [19] to write the interrupt modules for the malicious app. They then trained a Gaussian model using data from 5 participants to infer the sequence.

Textual content can be easily leaked through a malicious application [17]. The malicious application can compromise the OS and achieve root or kernel privileges. A malicious application

such as malware can use various methods to achieve root privilege, such as a rowhammer attack. For kernel privileges, malicious applications can make use of code injection or return-oriented programming. The malicious applications can then use ADB capability to store screenshots. Wei et al. [17] presented SchrodinText as a solution to protect specific textual content decided by the application developer.

User input inference attack [290] requires a malicious app that runs in the background and records all hover inputs of all apps. The malicious app has access to `SYSTEM_ALERT_WINDOW` and the Internet. The data collected is uploaded to a remote server for analysing the data.

A UI state inference attack requires an app running in the background and access to the Internet [53]. The attack first detects the activity transition event, which is known by the shared-memory side channel. After the detection, the identity of the new activity is achieved using the Activity signature and Activity transition graph. In a training phase, an automated tool is built to generate Activity transitions in an app and collect feature data to build the activity signature and the activity transition graph. In the attack phase, the app collects feature data during activity transitions. It then leverages the activity signature and a transition model based on the activity transition graph to execute the attack.

Train routes can be identified by exploiting device sensors, such as accelerometer, magnetometer, and gyroscope. Such attacks can be classified as sensor-based positioning attacks [299]. As a first step, a machine learning algorithm is applied to the sensor data, and then the activity of the user is detected. Next, the departure and arrival times of vehicles from the sequence of human activities are detected. Finally, by correlating the detected departure and arrival time of the train with the aid of timetables and route maps, the potential route of the journey is identified. This whole process primarily requires a malicious app with internet access on the victim's device. The malicious app continuously collects sensor data and sends them to the adversary who then estimates the route of travel by analysing the sequences. The attacker holds information on the list of public transport systems that are likely to be used by the victim. Machine learning, specifically random forest, is used to process the sensor information.

A digital password inference attack [284] leverages an accelerometer to reveal passwords on smartphones by exploiting the user-independent features of the movement of tapping buttons. Angle features are extracted to reflect changing trends and a multcategory classifier by combining the dynamic time-warping algorithm to get the probability of each movement. Then, by using a Markov model, the unlock process is modelled, and the sequences with the highest probability are used as the attack candidates. The data is sent to a server, which cleans it from noise and segment movements. Then, the data is used to train a classifier. It is then combined with the dynamic time-warping (DTW) algorithm to reveal the possibility and probability of each movement of a password sequence. The Markov model is then used in the unlocking process with multiple movements.

User-typed text can be extracted by recording the sound of the in-built microphones of a

smartphone through an acoustic emanation attack [123]. Signal processing techniques assist in extracting a probable set of characters per tap, and then by using natural language processing algorithms, most probable words and sentences are constructed. From the recorded audio signals, the first step is to detect tap instants which can be done by using the Detect Peak Intervals algorithm. It takes audio as input and returns a set of time intervals as the output. A malicious application installed on the victim's device can easily record the audio and later send it to a remote server for processing. The malicious application only needs permission to access the internet and a microphone.

2.9.13 Advanced Programming, Software & Hardware Tools, Mobile App, & Human Capabilities

An attacker can learn about the victim's path using advanced programming with software tools, a mobile application, hardware tools, and human capabilities. In a user path identification attack [179], the attacker identifies the walking path of a user by connecting the real-world identity to the network identity of the devices. To practically implement this attack, the attacker uses a low-cost software-defined radio device, such as USRP [88] with open-source cellular projects, such as srs LTE [278]. This attack requires two mandatory steps: (1) the attacker has to be located within 0.4-2 kilometres of the victim, and (2) the user must carry out a mobile downlink activity while walking, e.g., streaming a video. The adversary must have some basic knowledge about when the victim is walking, and that is when the attacker performs the path identification. As the victim accesses mobile downlink activity, the attacker captures the number of secondary cells at each location.

2.9.14 Advanced Programming, Software Tools, Mobile App, Hardware Tools & Permissions

A fusion of advanced programming, software, hardware tools, and phone permissions can lead to keystroke inference [232], a smartphone speech inference [116], and sensor-based location tracking attacks [217].

A keystroke inference attack [232] considers short inputs by the users, such as PINs or passwords and long inputs, such as emails or text messages. To perform this attack, a malicious app must be installed on the target user's device. Data from acceleration and gyroscopes are collected and used as training data. All collected data is temporarily stored on the SD card of the mobile device and is transferred to a remote server as soon as the phone is connected to the WiFi. The app only requires access to four user permissions: `INTERNET`, `READ_PHONE_STATE` permission, `WRITE_EXTERNAL_STORAGE`, and `GET_TASKS` permission. This attack assumes that the target user is using the standard QWERTY soft keyboard in a vertical orientation on his device.

The smartphone speech inference attack [116] is performed during a phone conversation by a malicious app having access to the motion sensor with the aim of making inferences on the voice content of the phone conversation. To conduct classifier training for speech inference attacks, the attacker can use a target-agnostic (TAG) or target-aware (TAW) approach. In TAG, the attacker collects training data from the accomplice who speaks words of interest on the phone while collecting the accelerometer and gyroscope data. In TAW, the training set would include data collected from the target. To discover the hardware used by the victim, the attacker may use surveillance in person or use recorded video that reveals how the victim holds the phone. This information trains the deep neural network for the speech inference attack.

Sensor-based location tracking attack [217] is performed when a victim user is driving a car with a smartphone. This attack uses smartphone sensors and tracks the victim user's location. To perform this attack, an app must be installed on the user's device that collects sensor data: accelerometer, gyroscope, and magnetometer. The recorded sensor data is uploaded to a remote server and processed. Turn angles, route curvatures, accelerations, headings and timestamps data are combined with public geographic area information to infer the user's route. This process is facilitated by graph construction and a search algorithm.

2.9.15 Advanced Programming, Software Tools, Mobile Application, Hardware Tools, Permissions, Human Capabilities

Not just outdoor location but the indoor location could also be inferred when advanced programming and software tools are added to a mobile application along with permissions, hardware tools, and human capabilities. An indoor location inference attack [319] includes a malicious app that secretly collects sensory data, including accelerometer, gyroscope, and magnetic field sensors and, in return, eavesdrops on the location. The app requires access to a network, either WiFi or cellular, to upload the location information to the attacker's remote server. In a training stage, the attacker walks through the targeted indoor location while carrying a number of mobile devices. This way, they collect the sensor readings as they pass through the targeted location track. To improve the accuracy, Bluetooth Low Energy (BLE) beacons are used in each sensitive location to activate sensor readings automatically as the attacker passes through it. Then, segmentation is performed on the large length of the data stream to get the desired specific part of the data stream, known as the exemplar. Further, noise reduction is performed. After the exemplars are ready, a robust supervised learning scheme using an anomaly calibration technique is used to construct a classifier to recognize the sensor pattern for each sensitive location. In the attack phase, the attacker adds the classifier to a malicious app, which then collects the sensor readings in the background and sensitive indoor locations.

2.10 Discussion

In this paper, we propose categorising social engineering and side channel attacks based on the resource-oriented nature of attacks. While several vectors could indicate the feasibility of an attack, such as the cost of resources, this is easily overcome due to the availability of multiple vendors where an attacker can get access at a low or cheaper price. For example, a thermal camera can be brought from Amazon at a price like £155 [16] but can also be bought cheaper from places like eBay or Facebook Marketplace. This makes the cost of resources slightly less attention grabber, and access to resources is the top priority for the investigation to determine the feasibility of attacks.

2.10.1 Using the categorisation

The proposed categorisation presented in this paper can be used in multiple ways. Below, we discuss a few usage directions and research questions that the categorisation can assist in answering.

1) Attack Assessment: Our categorisation can be used as an assessment method to ease the carrying out of specific attacks. In doing so, we can estimate the share of the population capable of executing a particular attack, which would indicate the ubiquity of the attack. For example, carrying out a novice attack, such as a traditional shoulder surfing attack, would only require the attacker to be in close proximity to the victim and make close observations. In contrast, performing an expert attack, such as a GUI squatting attack, requires more sophisticated tools and skills, such as image processing and deep learning. Comparing the resources required for these two attacks shows that anyone, regardless of background and expertise, could be a shoulder surfer as seen in prior work as well [85, 94], but to make an expert attack such as a GUI squatting attack, one has to be well-equipped with tech and security knowledge and tools. In sum, the low barriers to invading someone's privacy make it possible for a more significant proportion of the population to become attackers with little to no training. This also points out that similar attacks could occur anywhere at any time, heightening the need for adequate mitigation. Our categorisation would help organizations and individuals to set defence priorities and make informed decisions when using smartphones in different environments, such as private or public. Furthermore, the proposed categorisation can also assist organizations in making informed decisions about resource allocation when developing policies and methods to mitigate specific attacks. It can also be used to classify the severity of new emerging attacks. First, a list of requirements is required to carry out the attack. Based on the requirements, the attack can be linked to one of the four categorisation layers (see Section 2.4). We now present an exemplary thought to showcase how the categorisation can assist individuals, researchers, and organizations in conducting attack assessments using the proposed categorisation.

Example 1: Utilising Individual of Categorisation Novice attacks are at the centre of attention as they require minimal resources that anyone can easily acquire. Using categorisation to understand the attack requirements sets the focus on limiting access to resources or prohibiting their use in unavoidable circumstances. For example, shoulder surfing is a type of novice attack that only requires one to be in close proximity to the user and make careful observations. This property of shoulder surfing attacks makes them practical at any place around anyone. From the perspective of an individual, the individual knows that the attack is performed through direct observation of the screen, so the individual will be careful when accessing personal information in the vicinity of others in public and private environments. This behaviour could vary among users as they vary in their perception of the importance of privacy [96]. From the perspective of researchers, they can investigate the core requirement of the practicality of the attack, i.e., screen observation. For example, the details on the angle or duration of observation and distance between attacker and victim could assist in designing adequate countermeasures [5, 248]. Furthermore, organizations could propose policies that prohibit access to sensitive information in public environments or set conditions for access.

Example 2: Utilising Layers of the Categorisation Focusing on specific layers of the categorisation could help researchers in designing holistic protection methods. By inspecting the common requirements in each layer of the categorisation, common resources can be extracted, and then countermeasures specifically targeting the availability and use of those resources could be limited or prohibited as per the scenario. This would help in providing holistic protection against a group of attacks.

2) Accessibility versus Scalability: As we move horizontally across the categorisation levels, the feasibility of an attack decreases as the complexity of resources required increases. For example, to perform Expert Attacks, attackers must have advanced programming knowledge, software tools, mobile applications, access to user phone permissions, and hardware tools. However, the attacks at the Novice Level require human capabilities and easily available hardware tools, which can be performed more easily. This introduces interesting scalability aspects: the more difficult it is to execute an attack, which makes it less accessible, the more potential victims can be targeted.

While Novice Attacks that don't require technical skills or special equipment or setup, are easily accessible to anyone, executing the attack does not scale well because one attacker can only target a small number of victims at a given instance, mostly only one. For example, in the case of a shoulder surfing attack that requires observing someone's device screen without permission, an observer can only observe one screen at a time. Similarly, thermal attacks, which are another example of Novice Attacks, can be done on one user's device at a given instance. On

the other hand, more sophisticated attacks scale better since one attacker can target many users. For example, juice filming attacks, which are examples of proficient attacks, require a one-time setup, and then multiple users could be the target. One might argue that this is an advantage because there are hurdles to overcome in order to become a large-scale attacker. Yet, research also hints at another issue: easily available attacks might not be well-known by potential victims, and hence, they may be more susceptible to suffering the attack's consequences. For example, in a study by Jiang et al., [147] 74.5% of participants did not know about charging attacks, but only 14.1% of participants did *not* know about malware-based threats. Therefore, charging attacks might become more prevalent than malware-based attacks because of 1) the easy setup and 2) the lack of user awareness. This might be similar to other attacks that can be easily executed.

2.10.2 Key Takeaways & Future Research Directions

1) Anyone can easily become an attacker. Our categorisation has four different layers on how difficult it is for attackers to execute the attacks, which indicates the attack's scalability. Attacks in the "expert" layer require sophisticated knowledge and resources. Even though these attacks can scale well, they are unlikely to become ubiquitous because the hurdle for attackers is too high. "Proficient" attacks are on the verge of being script kiddies by using malware available online and programming skills. What is more concerning, though, are the lower two layers, "novice" and "intermediate." Attacks in the layer "intermediate attacks" require less expertise, some hardware tools that can be bought easily, and a mobile application that can be available online. Each requirement is benign and, hence, easy to get (e.g., video editing software). Consequently, this level can be reached by individuals with low knowledge, drastically reducing the hurdle to becoming an attacker. Finally, "novice" attacks like shoulder surfing do not require technical expertise and setup. Anyone can become a shoulder surfer spontaneously, and probably most individuals have already shoulder-surfing someone even without intention [85,91,94]. Consequently, carrying out "Novice" attacks is no longer restricted to highly motivated criminals with specific resources, *anyone can now become an attacker*.

2) Individual mechanisms are insufficient. Many attacks exist to target various attributes of mobile user privacy and security; the literature also underpins numerous mitigation or protection methods. For example, for protection against shoulder surfing attacks, a user can utilise mitigation methods, such as EyeSpot [156]. Similarly, for protection against thermal attacks [12,200], mechanisms such as PIN scrambler [166] can be used. The problem with using such individual mechanisms is that they require extra effort from the users and more time, rendering them ineffective [?, 120, 127, 154, 174]. Individual mechanisms also need memory allocation on the devices and have specific device model requirements to fulfil for the user to use the mechanism. In such a situation, what matters the most is how non-expert users can protect themselves and minimize the possibility of being attacked without additional protection mechanisms that require

much effort. This demands a more holistic understanding of user protection focused on an entire attack ecosystem rather than patching devices to resist single attacks. Further, mobile devices combine more and more functions ranging from shopping to banking that users want to perform on the go. As these devices can be attacked more and more easily, they result in a single point of failure that is not well enough protected.

Future Research Direction #1

Q1: How can users be ubiquitously defended against groups of attacks rather than patching against individual attacks?

Future Research Direction #2

Q2: How can we improve security and privacy mechanisms on mobile devices to safeguard them better?

3) User awareness alone is insufficient. Attacks can happen anywhere in the physical and digital world without time constraints. Awareness of the user's surroundings has repeatedly been proposed as a possible solution to protect users against multiple attacks without the need to have an additional mechanism in practice [47, 85, 210, 240, 311, 313]. While this might be a viable solution in some situations, (e.g., using a public WiFi), we cannot expect users to be aware of all possible attacks whenever they use a mobile device. Further, monitoring surroundings requires much too much effort from the user and could result in a waste of interaction time with the device. Furthermore, much of the surrounding awareness goes unnoticed because of the cognitive load caused by the task the user is performing on the device, for example, in the case of shoulder surfing [115]. Because of that, we need viable alternatives to defend users who do not rely on users to pay attention and defend themselves.

Future Research Direction #3

Q3: How can we effectively defend mobile users in their daily lives without relying on their awareness of their surroundings?

4) Rethinking the app developer's role in providing protection. While the non-expert and expert users play their part in protecting the privacy and security of their mobile phones, app developers can contribute by making app-level improvements. For example, changing the grid pattern location can assist against smudge attacks [47]. Adding body noise while using public WiFi can help with location-based attacks [313], restricting access to certain proc files can safeguard against UI state inference attacks [53], forcing apps to declare the purpose for accessing mobile phone sensors and adding noise to the sensor data can protect against sensor-based

attacks. However, most attacks require access to the Internet only to implement an attack successfully. The INTERNET permission is marked as safe permission by Android [103, 259] and is granted to apps without asking the user. Attackers can exploit this privilege to upload the collected sensitive information to a remote server for processing using advanced programming skills, such as machine learning. Second, most attacks target user location. While the location is extremely important information that enables users to accomplish various tasks, it is most compromised. Location data can be preserved by anonymization, but attacks on anonymization have also been witnessed [113]. The security incidents of location leakage might be one reason users are reluctant to adopt COVID-19 Contact Tracing Apps [98].

Future Research Direction #4

Q4: How can the developers be helped to configure Internet access to make it hard to exploit for performing attacks?

Future Research Direction #5

Q5: How can location privacy be better preserved?

2.11 Conclusion

With the increasing ease of access to resources to perform attacks, the security and privacy of mobile phone users are at risk. This paper explores the resources required for an attacker to carry out an attack. Based on the latest literature and a sample of 65 papers, we present a multi-layered categorisation of social engineering and side-channel attacks on mobile phones. The categorisation provides evidence for how user privacy can be violated with as little effort as direct observation through using human capabilities and as enormous effort as combining installing a malicious app with advanced programming skills, hardware tools, and much more. By analysing the work surveyed, we conclude with future research directions to better protect the privacy and security of mobile phone users.

III

Chapter 3

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

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.

Publication 2 (Full Paper Publication)



Farzand, H., Marky, K., & Khamis, M. (2022, September). Shoulder surfing through the social lens: A longitudinal investigation & insights from an exploratory diary study. In Proceedings of the 2022 European Symposium on Usable Security (pp. 85-97).



Figure 3.1: 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 [43] under Free Content License.)

3.1 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 [173]. While shoulder surfing can also be done using cameras, binoculars, or mirrors, direct observation is the most frequently used method [127, 311]. 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 [85, 203, 214]. 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 [85, 214, 248].

Related work proposed several mitigation methods aiming to protect users from shoulder surfing [239, 248, 295]. While such mechanisms deliver effectiveness, when and what mechanism is perceived suitable with respect to shoulder surfing incidents is not explored. Thus, in-

forming 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?

3.2 Background & Related Work

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

3.2.1 Shoulder Surfing Stories

Muslukhov et al. [214] 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. [85] 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

surfing 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. [248] 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 [22]. In a study by Aviv et al. [22], 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.

3.2.2 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 [91].

Examples of mitigation mechanisms offering protection from shoulder surfing of personal photos can be based on graphic filters that distort the pictures in galleries [295]. To protect textual content, researchers proposed using customized fonts to copy users' handwriting to make the text more difficult to read for observers [86]. Following a similar direction, EyeSpot [156]

and PrivateReader [239] track the user's eyes to hide content that is not being looked at. Further methods for safeguarding include selective showing [320], selective hiding [320], fake text filters [156], grayscale filter [320], lowering brightness [246], showing alert icon [246, 320], crystallize filters [156], dimming filters [156], showing a front camera preview [246], flashing the front LED [246], flashing borders [35], showing the shoulder surfer's silhouette [35], showing the shoulder surfer's gaze direction with a silhouette [35], and hiding content using a white screen [136]. 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 [91]. It is also crucial because low social acceptability also poses an effect on the user's self and external image [163] with further impact on the user experience as well [302].

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.

3.3 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 [8]. They complete the missing pieces in the research methods between observation in a naturalistic environment, observation in a fixed lab, and surveys [140]. Moreover, diaries are increasingly gaining attention in HCI research [59, 87, 270] and are frequently used by social researchers [245]. 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.

3.3.1 Study Design

Diary Design: We used the survey provider Qualtrics [237] 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 [85]. We asked partici-

pants 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 B.1.

Relationship Classification: Personal relationships and shoulder surfing share a two-sided connection [91]. 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 [78].

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 B.1.

3.3.2 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 [87, 270]. 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.

3.3.3 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 [287]. 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.

3.3.4 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 [208].

To determine whether further data collection is required, we calculated information saturation using the method proposed by Guest et al. [119] that sets the information threshold at $\leq 5\%$. 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 $\leq 5\%$ 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 [209]. This resulted in the refinement of the codebook. The codebook that denotes the categories can be found in the Appendix B.2.

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.

3.4 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 [252]. 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.

3.5 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 3.2 showcases

the time and location reported in the diary log of shoulder surfing incidents.

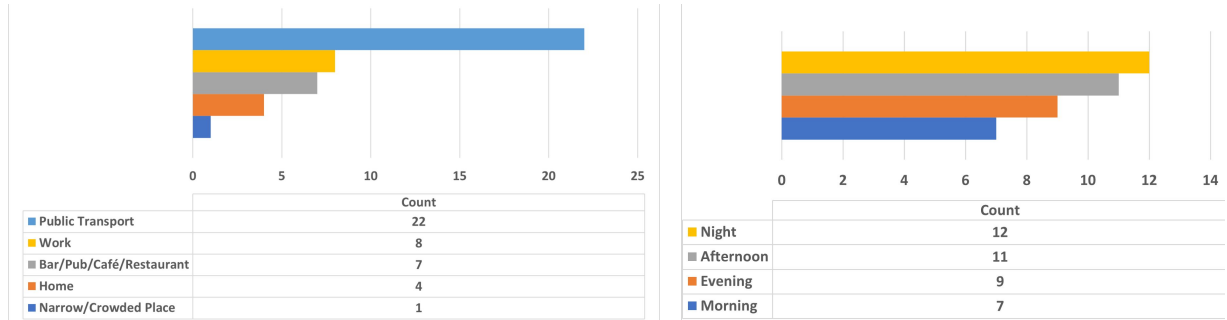


Figure 3.2: Location (left) and time (right) of shoulder surfing incidents experienced by participants of diary study either as observer, observee, or as third person.

3.5.1 The Observer's Side of the Story

Out of the $N=42$ stories logged, $N=23$ stories 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 [155]. These findings assist in answering **RQ 3.1**.

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.

3.5.2 The User's Side of the Story

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 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 [135], 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 3.1**.

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 [246] 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 [157, 180] and reduced notifications.

Using a mechanism may impact the relationship between the user and the observer [91]. 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 3.3 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 [78] 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 [78] 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 [157]. 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 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

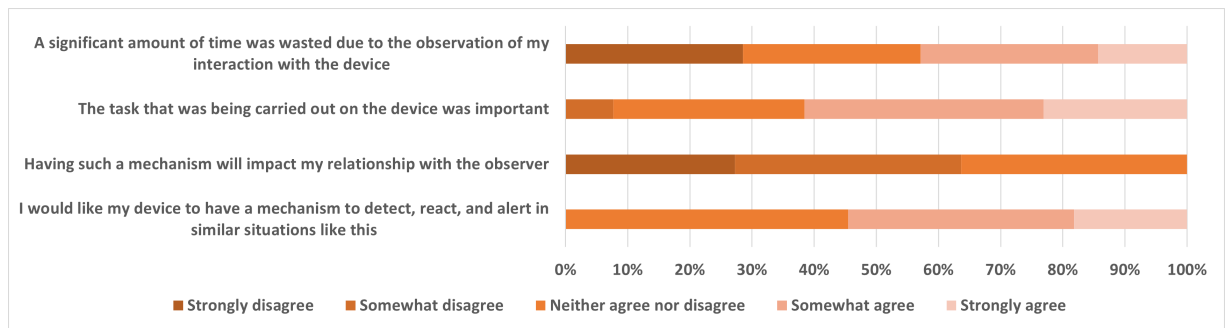


Figure 3.3: The responses received on a 5-point Likert scale for the impact of shoulder surfing on interaction time wastage, the importance of the task, preference for mechanisms, the impact of mechanism on relationship perceived by observees of the diary study.

different levels of the closeness of the relationship with the observer. Hence, one protection mechanism cannot offer a "one-size-fits-all" solution.

3.5.3 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 3.1**.

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.

3.6 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.

3.6.1 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 have? 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.

3.6.2 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 [159, 238, 239], privacy attacks resulting from shoulder surfing are less investigated but more frequently experienced by users [85, 91]. The security aspects of shoulder surfing look into protecting authentication information such as PINs and passwords [22]. With the advancement in technology, we have biometric systems such as fingerprint authentication [28] or EOG-based authentication [238] 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 surf-

ing 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 [85]. 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 [68, 301]. Privacy provides a personal space that is vital for human growth [61]. 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?

3.6.3 Principal Lesson Learned

Shoulder surfing is not only limited to public environments [85, 248] but its evidence is also found in private environments as seen in the results of the diary study and prior literature [127]. 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 [85]. 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 [91]. 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 [85]. 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 [155]. 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 [85]. Goucher et al. [115] 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?

3.6.4 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 [182] and system usability [34]. Farzand et al. [93] developed a typology of perceived privacy sensitive content in shoulder surfing sce-

narios 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?

3.6.5 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 [85,91]. 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?

3.6.6 Detecting Shoulder Surfing

Mitigating shoulder surfing requires successful detection of shoulder surfing as the first step. Bâce et al. [23] 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 [75] and through gaze estimation [247]. 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 [247] but brings along the challenge of bystander gaze privacy issues [152]. 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?

3.7 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 preferences 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.

IV

Chapter 4

***"What you think is private is no longer"* - Investigating the Aftermath of Shoulder Surfing on Smartphones in Everyday Life through the Eyes of the Victims**

Abstract: Shoulder surfing has been studied extensively; however, it remains unexplored whether and how it impacts users. Understanding this is important as it determines whether shoulder surfing poses a significant concern and, if so, how best to address it. By surveying smartphone users in the UK, we explore how shoulder surfing impacts a) the privacy perceptions of victim users and b) their interaction with smartphones. We found that the impact of being shoulder-surfed is highly individual. It is perceived as unavoidable and frequently occurring, leading to increased time for task completion. Individuals are concerned for their own and other people's privacy, seeing shoulder surfing as a gateway to more serious threats like identity or device theft. Participants expressed a willingness to alter their behaviour and use software-based protective measures to prevent shoulder surfing; yet, this comes with a set of user-defined criteria, such as effectiveness, affordability, reliability, and availability. We discuss future work directions for user-centred shoulder surfing mitigation.

Publication 3

"What you think is private is no longer" - Investigating the Aftermath of Shoulder Surfing on Smartphones in Everyday Life through the Eyes of the Victims

Farzand, H., Macdonald, S., Marky, K., & Khamis, M. (2025, May). "What you think is private is no longer" - Investigating the Impact of Shoulder Surfing on Smartphones in Everyday Life through the Eyes of the Victims. Under review at IEEE Security and Privacy 2025. <https://arxiv.org/abs/2411.18265>

Farzand, H., Macdonald, S., Marky, K., & Khamis, M. (2025, May). *"What you think is private is no longer"* - Investigating the Impact of Shoulder Surfing on Smartphones in Everyday Life through the Eyes of the Victims. Under review at IEEE Security and Privacy 2025. <https://arxiv.org/abs/2411.18265>



Figure 4.1: Shoulder surfing can happen anywhere at any time by anyone. In this paper, we investigate the impact of shoulder surfing on user’s social lives and interaction with their devices. For this, we surveyed N=91 participants from the UK and inquired about their privacy perception, device interaction, and awareness and training around shoulder surfing. (The image uses figures by Deivid Saenz and Sofia Salazar [250, 251].)

4.1 Introduction

Everyday life scenarios – such as using a smartphone on a bus to navigate or to respond to messages while enjoying a cup of coffee in a cafe – are susceptible to shoulder surfing (cf. [85, 89, 93–95]). In such scenarios, the observer takes advantage of the user’s unawareness to observe and uncover information displayed on the smartphone. Anyone surrounding the user could shoulder surf without being noticed by the user. Consequently, such scenarios can invoke the user’s privacy, potentially resulting in uncomfortable feelings between the user and the observer [85]. Even worse, they could even impact them personally or professionally [104]. For example, a senior UK civil servant lost their position because someone photographed their laptop screen [69]. Further, the confidential details of US customers of a Bank of America branch office in downtown St. Petersburg were visible to people on the street outside the office [104]. In the law firm Ernst & Young (EY), a call centre provided screenshots of internal systems to fraudsters [104]. Shoulder surfing does not need to be done only through direct observation; it can also be done by other means, such as a camera. The examples above clearly highlight the consequences shoulder surfing can lead to.

Research on shoulder surfing has provided in-depth insights into the anatomy of shoulder surfing, revealing how, when, and where it happens using multiple methods such as sur-

veys [85, 93, 127, 203], diary studies [94], interviews [91], focus groups [253] and even virtual reality [4, 5]. Users also physically manipulate their devices, e.g., by tilting [162], switching it off [85], or using a privacy screen [235] when they realized being shoulder surfed. Similarly, privacy and HCI researchers have proposed numerous software-based mechanisms to combat the risk of shoulder surfing through alerting the user using icons [246] or by mitigating the risk using overlay filters [156], greyscaling [320], lowering screen brightness [246] or gaze-based mechanisms that limit the observer's view [35]. This paper continues this line of research by exploring the impact of shoulder surfing on the daily lives of victims of shoulder surfing and their interactions with smartphones, specifically investigating the following research questions:

“RQ 1: How does shoulder surfing impact the perception of victims of shoulder surfing towards protecting their device information?”

“RQ 2: How does shoulder surfing impact victims' willingness to use smartphones and their social interaction?”

To address these research questions, we surveyed 91 victims of smartphone shoulder surfing in the UK. We gathered their experiences around how their encounters with shoulder surfing have impacted their social and device interaction. We asked participants about their past experiences, present knowledge, and future willingness to use protection measures against shoulder surfing. We also asked participants if they had received any training or education on protecting their privacy against shoulder surfing.

To answer **RQ1**, participants held diverse perspectives on the impact of shoulder surfing. On the one hand, we collected evidence that shoulder surfing multiplied the situational awareness of participants, making them pay continuous attention to the changes in their surroundings. On the other hand, shoulder surfing by anyone was a concern for almost all participants; a few participants were even concerned about being shoulder surfed by children, as the participants felt that the potential harm was greater for the child, as the observer, rather than for themselves as the victim. Shoulder surfing was seen as unavoidable, frequent, and always prevalent. The privacy concerns led participants to adopt available privacy tools such as privacy screens - screen protectors that prevent viewing from certain angles. Additional mechanisms were seen as giving participants a sense of safety and security. However, their adoption depended on factors including effectiveness, ease of use, level of interruption during the device interaction, and financial cost of the mechanism. Overall, the main concern around shoulder surfing was privacy. Shoulder surfing was seen as giving rise to more serious concerns, such as the risk of a potential stalker, unauthorized access, identity theft, device theft, and blackmail. Participants were also concerned about other people's privacy, such as those whose data was seen while being shoulder surfed.

To answer **RQ2**, participants could not always avoid using their smartphones in the setting in which they were previously shoulder surfed. This was so because the setting was essential

to their daily life, such as public transport or workspaces. However, they took actions like restricting access to sensitive information in public or waiting for a private environment to access information to avoid potential loss of privacy due to shoulder surfing. Others made adjustments in their physical settings, such as selecting a seat on the bus which was not lower than the seat behind it or switching to non-sensitive apps when under the threat of shoulder surfing. Shoulder surfing distracted participants and slowed down the participants from interacting with their devices. Participants had to pay increased attention, which resulted in increased time to complete what they were doing on their phones. Due to the threat of shoulder surfing, participants reduced their usage of their phones. Our participants held no training or education on protecting their privacy from shoulder surfing but shared user-level measures that they have been practising for protection such as repositioning themselves, lowering screen brightness, and alike.

While shoulder surfing was seen as impacting the privacy perception of victims of shoulder surfing, another perspective of shoulder surfing included not perceiving it as a threat. Some participants considered shoulder surfing as harmless, so additional mechanisms to protect privacy were seen as unneeded. This perception was mainly held by a set of participants who had fewer shoulder surfing incidents and generally avoided accessing sensitive information in public.

Research Contribution.

1. We present in-depth insights into the impact of everyday life shoulder surfing on the social and device interactions of victims of shoulder surfing, explaining *why* and *how* shoulder surfing impacts users,
2. Our research bridges the gap between investigations of episodes of shoulder surfing in the wild and the need for privacy protection methods. We discuss and provide recommendations to address the challenges in mitigating the negative impact of shoulder surfing on diverse users, including vulnerable user groups such as children.

4.2 Background

4.2.1 The Prevalence of Shoulder Surfing

In 2016, at least 4640 publications were indexed on Google Scholar that were linked to shoulder surfing [85]. Eight years later today, in 2024, the research on shoulder surfing has increased to more than double, counting to at least 10,700 publications [257]. The massive increase in the research on shoulder surfing shows the prevalence of shoulder surfing. One of the underlying reasons for the intensive and continued research on understanding and mitigation of shoulder surfing is the widespread usage of smartphones. Due to their ubiquity, they are the devices that are most shoulder-surfed [85, 93]. It is forecasted that by the next five years, the smartphone user base will reach 9.72 million in the UK with a 4.92% increase [282]. A study by Marques et

al. [204] presents evidence that people who own a smartphone are more likely to shoulder surf others. This shows that as the number of smartphone users is increasing, the threat of shoulder surfing is also increasing. Shoulder surfing, sometimes also referred to as "snooping on other people's phones", has been reported to be done by 1 in every 5 adults in the US and is most prevalent among young users [204].

Shoulder surfing requires only being in close proximity to make observations, meaning anyone can become a shoulder surfer [89]. Shoulder surfing can reveal two categories of information: (1) security-critical information (such as PINs and passwords) and (2) content information (such as text and photos). Most research focused on security-critical information leaked through shoulder surfing [14, 37, 72, 120, 294] and has proposed multiple mechanisms that overcome the risk of shoulder surfing. Some examples include fingerprint authentication [28] or EOG-based authentication [238]. Addressing security-critical shoulder surfing is important as it could lead to unauthorized device access; however, protecting from content shoulder surfing is also critical as it violates user privacy, leaks personal information and can lead to serious consequences such as potential stalking [85]. In contrast, content shoulder surfing is more frequently experienced and reported in comparison to security-critical shoulder surfing further motivating the investigation of content shoulder surfing [85, 94].

Among the plethora of shoulder-surfed content, text, photos, and games form the most shoulder-surfed content [85]. Within the text category, messages were mostly reported, followed by social media, email, and news. Similar findings were also reported in a diary study [94] where victim users reported using messengers, email apps, and video calling apps when being shoulder-surfed and observers reported having observed messaging, games, social media, and emails. In a study by Saad et al. [249], four apps of varied content types, including Facebook, WhatsApp, games, and photo galleries, were compared and reported that following authentication, WhatsApp was the most observed app while photo gallery remained the second most observed. In the same line of research, Abdrabou et al. [5] reported that games and videos are more often shoulder-surfed in comparison to text. Considering the work around the content being shoulder surfed, every content type appears susceptible to shoulder surfing.

Shoulder surfing is not only done by outsiders (such as strangers); it can be done by anyone. Prior work presents a list of user-observer relationships that have either shoulder-surfed someone or were observed while interacting with their devices. The user-observer relationship spectrum includes strangers, acquaintances, friends, colleagues, family members, and partners [85, 91, 94]. Similar to the variety in user-observer relationships, shoulder surfing can happen anywhere, including in public (e.g., workspace, educational institutes, restaurants) and private environments (e.g., at home) [85, 91, 94, 127]. Despite the broad list of locations, public transport is one of the most shoulder-surfed locations and strangers are the most common user-observer relationship [85].

Overviewing the continued line of research on shoulder surfing, alongside the diversity of

content, location, and user-observer relationships involved, highlights that the risk of shoulder surfing can occur in a wide range of contexts. Further, the threat of shoulder surfing is globally recognized [131]. This broadly highlights the need to investigate how shoulder surfing impacts users' social interactions and device use, motivating the focus of our study.

4.2.2 Users Responses to Privacy Violations & Shoulder Surfing

One of the main risks of privacy violations is the leakage of personal data, especially Personally Identifiable Information (PII), a significant concern among users [195]. To keep personal items and identities containing PII safe, users hold their belongings close to them or restrict access, especially for electronic devices by using various authentication systems, such as biometrics or pattern locks [28, 195]. Users have even reported using outdated mobile phones to protect their devices from threats, such as device theft, making them less appealing to thieves [195]. Furthermore, users have reported not storing any financial information, such as credit card information, on their devices to prevent any misuse of information [195].

Similar to protecting the information from threats (e.g., device theft), users adopt several measures to protect their information from shoulder surfing. These include putting the device down, turning it off, or hiding the screen using hands [85, 91, 94]. Alongside the physical responses to shoulder surfing, users have also voiced emotional reactions to shoulder surfing, such as causing an angry look or initiating a conversation with the observer with a negative intent [85]. Users also reported using a privacy screen that hides content from certain angles as a way to protect from unconsented observations [91]. Tilting of the device to hide content has also been reported as a measure to protect privacy [162].

Shoulder surfing has led to negative feelings between users and observers, such as uneasiness, embarrassment, harassment, anger, and spying [85]. Cross-cultural examinations have provided evidence that shoulder surfing can have more serious negative consequences for low socio-economic groups in comparison to high socio-economic groups due to the exaggerated fears of one's own privacy and fragile trust among users [252]. To sum up, shoulder surfing is a concern among users, as are other privacy violations. Prior work has touched upon users' response to shoulder surfing by capturing real-world stories [85, 94]; they provide limited insight into how the users' response affects users' perception of protecting their information from shoulder surfing and how it impacts their device and social interaction. As evident from related work, users employ various strategies to mitigate and combat shoulder surfing. However, the emotional and behavioural responses reveal deeper concerns about its impact on daily device interactions. Thus, understanding how these emotional and behavioural responses affect user behaviour is important for developing effective mitigation strategies.

4.2.3 Existing Software-based Mitigations to Shoulder Surfing

In response to shoulder surfing, researchers have developed several software-based mechanisms to offer privacy protection to users. For instance, Zhou et al. presented four screen filter-like mechanisms that included grayscale, dim, selective viewing and selective hiding [320]. The mechanisms provided users with awareness of shoulder surfer through glyph notifications and response through visual protections. Zezschwitz et al. resented three image distortion techniques that included crystallisation, pixelation, and oil painting [295]. These mechanisms were specifically tested for the privacy of photos, and the results showed high usability for all filters. Following a similar approach, Tang et al. presented a combination of blurry and pixelation techniques, "EyeShield", for protection against shoulder surfing [285]. The proposed system would blur out text and mobile UIs while the images would be protected through pixelation. Blurring was also studied by Li et al. in combination with blocking to obfuscate faces in photos [292]. Zhang et al. proposed a coarse-grained and fine-grained masking technique that adjusted the spatial frequency and luminance contrast of coloured visualizations to protect data visualizations on mobile devices from shoulder surfing [316]. Similar to these works, many other research works have also focused on proposing solutions for mitigating shoulder surfing [187, 246, 283]. In reviewing these mechanisms, it's clear that many focus on technical solutions without fully considering how shoulder surfing affects users' interactions with their devices, their social behaviour, or their perceptions of privacy. Understanding these broader impacts is essential for designing more effective and user-friendly mitigation strategies. Our research addresses this gap by exploring how users experience and respond to shoulder surfing in everyday contexts, informing the development of more holistic protection methods.

Research Gap

Despite the growing body of research on understanding shoulder surfing and users' response to it, there is a notable gap in the understanding of the impact of shoulder surfing on the victim users' interaction with devices and their general social interactions. Understanding the impact is crucial as it lays the foundation for the need to mitigate shoulder surfing. Our research aims to fill this gap by exploring how and when victim users are impacted by shoulder surfing. Furthermore, we explore the situation around training and education of users on protection against shoulder surfing.

4.3 Methodology

To investigate the device and social impact on users caused by shoulder surfing, we conducted an online survey study with N=91 participants from the UK via Prolific [236].

4.3.1 Questionnaire Design

Our goal was to formulate questions that focused on the impact of shoulder surfing. We wanted to capture data from a diverse pool of users in terms of gender and professional status, and therefore, opted to design an online questionnaire. Questions were formulated about what and how shoulder surfing impacts device usage and users' social interaction. Along with open-ended questions, Likert items capturing the users' agreement or disagreement were also included. The questions were trialed by two researchers with expertise in human aspects of social engineering and side-channel attacks to ensure broad and accurate coverage of the goal. The questionnaire was improved based on the researchers' feedback. We used Qualtrics - an online survey builder platform, to build the survey questionnaire [237].

4.3.2 Study Procedure

Our study procedure was divided into two stages:

Stage 1: Screening Victims of Shoulder Surfing: In this study part, we recruited participants who have experienced shoulder surfing on a smartphone as victims. For this, we first ran a short-listing study on Prolific (N=180) and asked participants if they had experienced shoulder surfing on smartphones as a victim. Participants were presented with the definition of shoulder surfing to help them understand the term and respond accordingly. Participants who responded as being victims of shoulder surfing were invited for Stage 2 of the study. At this stage, participants were not informed about the invite to the second study. All participants from both stages were compensated as per Prolific's compensation policy.

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

1. **Step 1: Information & Consent Signing:** Participants were welcomed to the study and were explained the aim of the study, i.e. to capture their experiences and concerns about shoulder surfing on smartphones. Participants were then presented with the consent form and asked to accept it if they wished to proceed with the study.
2. **Step 2: Setting the Scene:** Next, we presented participants with the definition of shoulder surfing and then asked them to recall their most recent experience of shoulder surfing on a smartphone as a victim. This question served multiple purposes, such as checking the understanding and attention of participants and setting up the context.
3. **Step 3: Eliciting Details:** In this part, we asked participants about the impact of shoulder surfing. We focused the questions on how shoulder surfing has (or has not) impacted them socially or their interaction with the device. To avoid biasing the participants, we

presented them with a series of Likert items, and each one was followed by a question that asked for an explanation of their choice.

4. **Step 4: Demographics:** We concluded the survey by asking demographic questions on age, gender, and employment status and redirecting participants back to the recruitment platform for reimbursement.

4.3.3 Pilot Testing

We pilot-tested our questionnaire internally with two Usable Security and Privacy researchers at our institute, and based on their feedback, we refined the wording of the questions. Researchers also gave us feedback on the overall goal of the questionnaire and the questions asked. This helped ensure that the formulated questions adequately answered the research questions.

4.3.4 Ethical Considerations

The Ethics Committee at our institute approved the study. The study presented in this paper was conducted in line with the ethics guidelines provided by our institute. Before beginning the study, the participants were presented with an information sheet and a consent form detailing the goal of the survey, the tasks required to complete the study, and how the survey results will be used. Data collection and storage were aligned with the GDPR guidelines.

4.3.5 Recruitment & Participants

The sample consisted of $N=100$ participants residing in the UK. We recruited participants via Prolific and reimbursed them via Prolific set standards for participant compensation. Participants took 11.34 minutes on average to complete the questionnaire ($\text{std}=7.39$). Checking completion time is a well-established strategy to check for participants' attentiveness and has been used in multiple research papers such as [73]. For our analysis, we excluded 8 participants' data as they filled the questionnaire in less than half the average time to complete the questionnaire. To check the participants' attentiveness and understanding of the goal of the study, we asked them to describe their latest experience of shoulder surfing. We further removed the data of one participant as they had responded from the perspective of observers and not victims. The final sample included $N=91$ participants. Out of $N=91$ participants, 47.25% self-identified as a man, and 52.74% self-identified as a woman. Participants aged between 22 and 73 years ($\mu=38.23$, $\sigma=10.15$). A majority of the participants (65.93%) were employed full-time, 24.17% employed part-time, 3.30% students, 3.30% homemakers, 2.20% unemployed and 1.10% retired.

4.3.6 Limitations

In this section, we acknowledge the study's limitations. The participants were located in the UK - a Western country - where shoulder surfing is reported to have less severe consequences than Eastern countries [252]. This might have impacted participants' responses and opinions on shoulder surfing. However, our study serves as the first step towards investigating the impact of shoulder surfing. Since shoulder surfing is a global threat that exists regardless of culture, we suggest future work to replicate the study in different cultures to capture a holistic view of the impact of shoulder surfing. In our study, participants relied on their memory to report how their shoulder surfing experiences have impacted them. This may have introduced recall bias as participants may not accurately remember the details [288]. Accordingly, more ecological studies focusing on in-the-wild investigations should look into verifying the results reported in the paper. Lastly, we recruited participants from an online platform where users self-nominate themselves to take part; we found our sample to be balanced in terms of gender and diversity in employment status, with a majority being employed full-time and a few with student status. This distribution of demographics addresses the limitations of many studies where the sample mainly consisted of students such as [39, 85].

4.3.7 Data Analysis

As a first step, one researcher familiarised themselves with the data and applied open coding to the data. To increase the reliability of the coding, another researcher verified the coding by independently coding a subset of the data (25%). Both researchers then discussed the codes, and any coding disagreements were resolved during a meeting session. After this, the codes were grouped into main themes until no meaningful grouping was possible [208]. Following the guidelines of previous work, we refrain from reporting inter-rater reliability [33, 209, 300] to support a qualitative coding approach based on discussion and merging of results. We present the results based on the themes derived. We report the number of times a code occurred using the guidelines presented in Figure 4.2 to offer an improved readability experience and to give an impression of how often a particular code appeared in the respective category. However, we do not quantify the frequency of the category reported, and hence, it should not be considered a quantitative analysis. Where necessary, we use participants' quotes to provide better context and explanation.

Prior research has provided evidence that shoulder surfing impacts victim users differently based on their cultural ecosystem [252]. In line with this research, we specifically focus on the users in the UK. Drawing comparisons based on gender, age, education or geographical location is out of the scope of this paper.

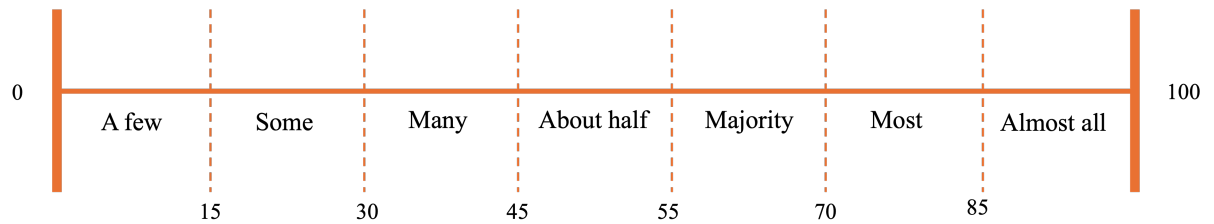


Figure 4.2: The Figure shows the overview of the qualifiers and respective frequencies of codes throughout our results. All occurrences of the respective qualifiers always refer to the same portion of the number of times codes.

4.4 Results

4.4.1 Setting the Narrative of Shoulder Surfing:

To set the focus of the study, we asked participants to describe their latest shoulder surfing experience. 17.58% experienced it “a few months ago”, 40.66% of participants recalled experiencing the latest shoulder surfing incident “less than a month ago”, 37.36% “a few days ago”, and 4.40% of participants experienced shoulder surfing either “the day before” or “on the day” of participating in the study. Participants were then asked if they experience shoulder surfing daily on a 5-point Likert scale (1=strongly disagree; 5=strongly agree), to which 20.88% somewhat agreed or strongly agreed, while 68.13% somewhat disagreed or strongly disagreed (Median=2, Mean=2.36, SD=1.12).

Further, participants were asked to describe their shoulder surfing experience in an open-ended question. Participants mentioned their most recent shoulder surfing experience, including details like relationship with the observer, shoulder-surfed content, and feelings associated with it.

About half of the participants mentioned being shoulder-surfed by “strangers”, and a few mentioned being shoulder-surfed by “partners”, “colleagues”, “parents”, “friends”, “family members”, and “children”. A few participants specifically mentioned being shoulder-surfed “at the office”. Participants expressed feelings of “*privacy invasion*” and being “*paranoid*” to be linked with their experience of shoulder surfing. Some participants mentioned “messages” as shoulder-surfed content, while a few participants mentioned “videos”, “social media”, “news”, “music players”, and “internet browsers”.

P41: *I have a young child. I was reading work email and I observed that my child is reading the message. They have also been caught doing this with WhatsApp.*

P44: *My child was reading my messages over my shoulder as I was typing them to a friend. I told him it's rude to and he pretended to look away but I could see he was still watching me.*

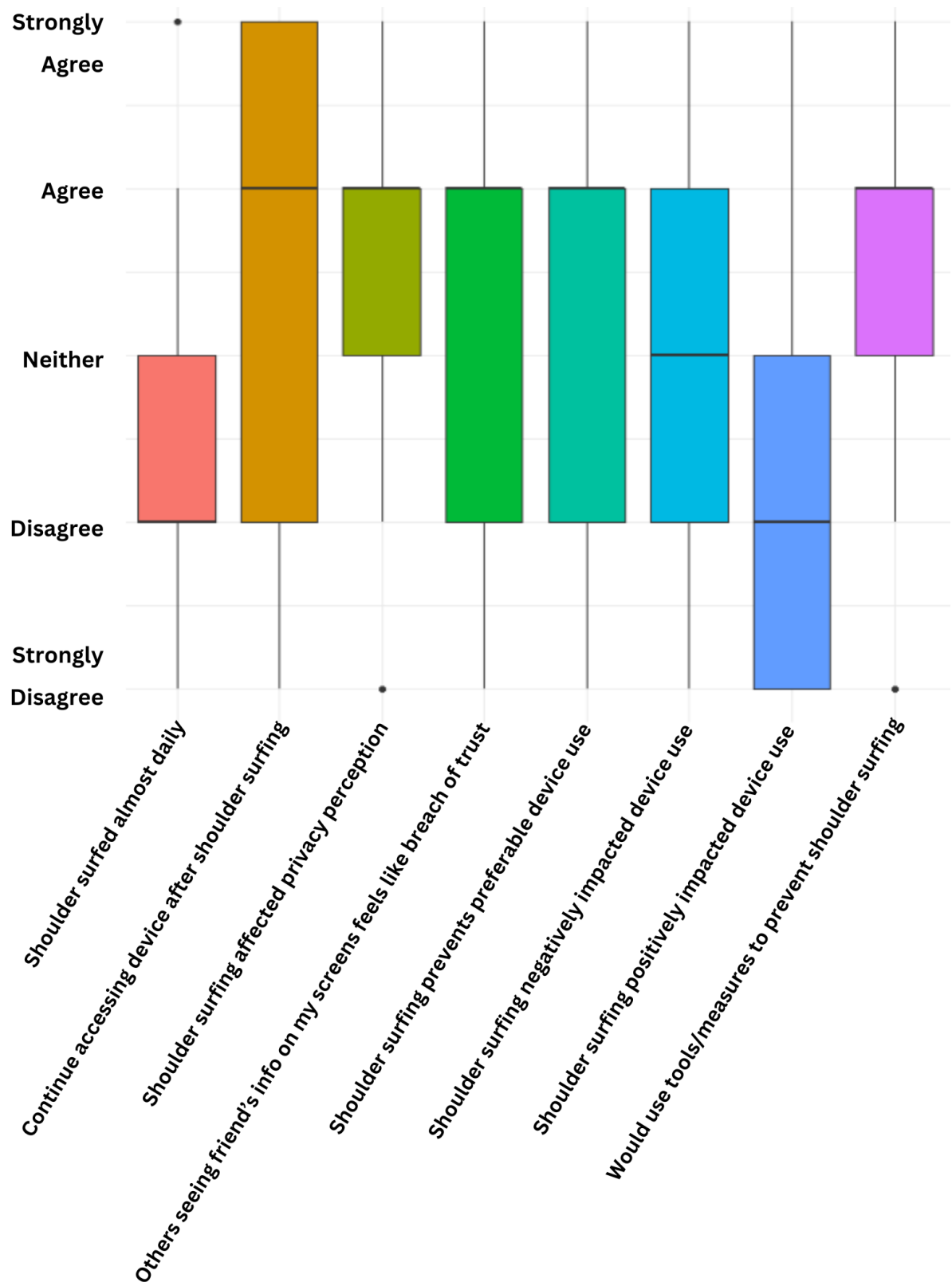


Figure 4.3: The Figure shows the boxplots for the responses of participants to the questions centred around the impact of shoulder surfing.

4.4.2 Privacy Perceptions

In this section, we present the results of the impact of shoulder surfing on the privacy perceptions of users and the openness towards using additional mechanisms in the future to protect personal information from shoulder surfing.

Personal Privacy Perceptions

When asked if shoulder surfing affected their perceptions of privacy; more than half of the participants (58.24%) somewhat or strongly agreed, while only 16.49% somewhat or strongly disagreed (mean=3.58, SD=1.05, median=4). Shoulder surfing was perceived to be affecting the perception of privacy of participants in multiple ways, which we detail below:

Situational Awareness: A few participants mentioned that experiencing shoulder surfing raised their awareness about their surroundings. They had to check their surroundings before engaging in a task that required accessing sensitive information so that no sensitive information could be leaked. They were more aware of “who” was around them while they accessed information on their devices. Shoulder surfing made a few participants rethink about accessing sensitive information around others, such as banking information.

Privacy Concerns: Shoulder surfing was seen as a privacy invasion by some participants, and a few felt that it gave rise to negative feelings, such as “discomfort”, “disrespect”, “un-trustworthiness”, and “annoyance”. A few participants felt that privacy was needed and voiced location-specific protection, such as in public locations, especially public transport. Context-specific concerns were also mentioned by a few participants; for example, what they do on the phone and who they are with, and similar factors would determine if participants are concerned about being shoulder surfed. Concerns about shoulder surfing by “children” were also raised, with a few participants reporting they had to stop interacting with their devices to prevent it. A few participants were inclined to use protective measures to protect their privacy, such as a privacy screen. The following quotes from participants reflect their privacy concerns:

P100: *"...it did shock me a bit that someone could be so blatant in staring at someone's potentially private information."*

P41: *"I thought I was reading something on my own. In this case it was not age appropriate. I stopped to educate my child."*

P69: *"What I do on my phone is my business and my business alone. I should be the one to decide who sees what's on my phone screen."*

Prevalence of Shoulder Surfing Some participants voiced that shoulder surfing is unavoidable and shoulder surfers will always be there. The participants believed they were aware of

shoulder surfing, which has happened multiple times. Participants also commented that they, being the victims in our case, had overlooked other people's screens and were surprised to find the specific content. The following quote from the participant shows the perspective on the prevalence of shoulder surfing.

P14: *"What you think is private is no longer"*

P22: *"I was already pretty aware that we now live in a society with significantly less privacy that we used to enjoy"*

On the contrary, a few participants reported that shoulder surfing did not affect them. This was usually the case because participants perceived shoulder surfing as harmless and were casually interacting with the device while being shoulder-surfed, such as playing a game or watching a sports match. In such cases, they did not mind being shoulder-surfed.

Openness to Using Protection Measures

We asked participants if they would like to use additional measures or tools to prevent shoulder surfing. More than half of them (61.96%) somewhat or strongly agreed. Participants voiced existing measures that were practised to safeguard against shoulder surfing and favoured continuing to use them. A few participants mentioned that they either already had a privacy screen or considered having one in the future. In the case of the need for privacy, a few participants considered repositioning themselves or their phones or looking for a less busy place. Locking the screen upon realising shoulder surfing was also mentioned by a few participants as a way to protect their information.

A few participants mentioned having a sense of security through additional protection mechanisms. The use of additional measures was favoured by a few participants as they assisted in the prevention of shoulder surfing. Some participants believed extra measures would offer them privacy and protect their data. While other participants acknowledged the security and privacy brought about by the additional measures, they also voiced several preconditions to be considered before adopting any protection measure. We detail the preconditions below:

Conditions for Use: Easy availability of the protection measure, awareness of such measures, and context-dependence (for example, who the participants are with during the shoulder surfing event and alike) were among the other preconditions mentioned by a few participants. A few participants preferred additional protection measures for application-specific use only, such as online banking apps.

Design of Tools: When it comes to the design of tools, a few participants mentioned specific attributes of protection measures that are to be considered when using them in the future, such

as ease of use, level of interruption while interacting with the device, and the financial cost of the measure. A few participants also mentioned that using additional measures will depend on the tool, for example, whether it has been proven effective, how it works, and its reliability. These aspects would determine whether the participants will use the specific tool. The following quotes further highlight the perspectives of participants on using protection mechanisms in the future.

P31: *"If something was proven effective"*

P35: *"I would need to feel confident they help"*

P39: *"I value my privacy very highly it would depend on what those measures were and if they cost/how much they cost"*

P94: *"Not aware or thought of any additional privacy methods other than putting a shield around my head"*

P33: *"Whether or not I use additional privacy measures or tools may depend on the burden it might cause (e.g. bloatware, additional costs, installing dodgy software on devices). "*

P67: *"It has definitely made me more conscious of my privacy, and made me wary of the person who shoulder surfed me."*

Perceived Redundancy of Privacy Protection Measures: Participants mentioned existing privacy-preserving tools that were used, such as privacy screens, While participants expressed willingness to use additional protection measures in future, some marked it as unnecessary. This was due to multiple reasons; for example, people did not see shoulder surfing as an issue, generally avoided accessing sensitive information in public spaces, such as public transport, had infrequent incidents of shoulder surfing or were not much concerned about it.



Summary: As seen in prior work, shoulder surfing was perceived as violating privacy and evoked negative feelings [85]. Conversely, a few participants were not impacted by shoulder surfing [127] as they had experienced it a few times only, did not access sensitive information in public and perceived it to be harmless. Participants expressed willingness to use additional measures against shoulder surfing as shown previously [91]. Novel findings included that shoulder surfing gave rise to situational awareness, and participants were actively checking their surroundings when interacting with their devices. Participants viewed shoulder surfing as unavoidable and acknowledged that it had happened multiple times. One of the major concerns around shoulder surfing was shoulder surfing by children. While participants were willing to use mechanisms to protect their privacy, it was seen as depending on a range of factors like availability, effectiveness, reliability, financial cost, and the design of tools.

4.4.3 Device Usage After Shoulder Surfing

We assessed the device usage by asking questions about using the device in the same setting as the one they were shoulder-surfed in, general device usage after shoulder surfing, and task completion.

Using the Device in the Same Setting as the Previously Shoulder Surfed Setting

Using the device in the same setting as the shoulder surfed setting can be challenging for users, as it can result in another shoulder surfing incident. A large majority of participants (67.39%) voiced that they continue using the device in the same setting in which they were shoulder-surfed for a number of reasons; for example, a few participants mentioned that the setting of shoulder surfing is unavoidable for them (like public transport, office or one's home), which they have to use for various purposes.

However, they are more aware of the people around them. Participants could not avoid using smartphones in the shoulder-surfed settings, but they took action to protect their privacy. For example, they would not access sensitive information when around people and wait for a more private environment to access sensitive information. Since the participants avoided accessing sensitive information in the same setting as the one previously shoulder surfed in, they no longer minded others taking a look over their screen. Therefore, there was no need to change or avoid the setting. A few participants mentioned using quick scrolling, tilting the device, or switching off the device in the shoulder surfing setting to protect their screen from being observed. Relationship dynamics also played a role in determining if the participant felt the need to change the setting. For example, a few participants were also not much concerned about changing their setting as they were shoulder-surfed by their partner, which they did not perceive as concerning. The following quotes from participants represent their perspectives on using smartphones in the shoulder surfing setting:

P42: *"...for the most part if its not urgent I refrain until I am out of that setting."*

P8: *"I have to be there regularly and I use my phone during my waiting time. I make sure I don't access any sensitive information"*

P55: *"As I said, I ended up putting my phone away as I didn't like the feeling of being watched at all. It made me feel paranoid and wondering whether anyone else had been looking at my phone beforehand. It really affected me in that regard."*

Participants who disagreed with the statement on continuing to access smartphones in the same setting also held similar perspectives. Participants adjusted their behaviour in the setting where they were shoulder surfed to prevent shoulder surfing. For example, they changed their seating location on the bus and preferred a seat that was not lower than the one behind it. Furthermore, they also restricted access to applications that contain sensitive information in three

ways: (1) shifted to using non-sensitive apps such as a music player, (2) put the phone away, or (3) waited to get out of that setting and then accessed their phones. Participants also used other activities to avoid using the phone, such as reading a book. Overall, participants perceived shoulder surfing as an invasion of privacy, making them uncomfortable and worried about what other people could see on their smartphones.

Impact on Task Completion

More than half of the participants (62.63%) somewhat or strongly agreed that experiencing shoulder surfing prevented or slowed them down from completing the task. It took longer for participants to complete the task they were doing because of the (1) changes in the way they interacted with their devices, (2) concerns about bystanders, and (3) changes participants had to make in the physical settings.

Device Interaction: Participants had to stop the task they were doing or turn off their devices to stop being shoulder-surfed. A few participants mentioned interacting and performing tasks with their devices more discreetly and scrolling through quickly, which they would have spent more time on otherwise. Participants had to change apps to protect information from being leaked through shoulder surfing. The selective use of apps resulted in the prevention of accessing information and also slowed down the participants while interacting and completing their tasks with their devices, which in turn slowed the rate at which they were completing their tasks. For a few participants, realising being shoulder surfing distracted them from interacting with their devices.

Concern about Bystanders: Shoulder surfing evoked negative feelings like discomfort, annoyance and frustration in a few participants. Participants kept thinking about the bystander, which prevented them from completing the task they were doing on their smartphones. Shoulder surfing made a few participants think twice before accessing information, and a few participants specifically avoided accessing sensitive information apps such as banking apps. Precisely, they would avoid accessing any information that they do not prefer others to see.

Physical Setting: A few participants mentioned that they had to look for a more private or less busy space to continue using their phone: for example, waiting until they got off public transport or using the phone in the bathroom to avoid shoulder surfing at workspace. Since the participants did not access their phones while under the threat of shoulder surfing, they experienced boredom as a result. In cases where waiting for a private space was not an option, participants had to look around to ensure no one was looking at their screen or cover the screen from observations in parallel to completing the task on devices. Interacting with the device while looking out for bystanders and protecting the screen from observations resulted in increased time to complete

their tasks. Shoulder surfing raised awareness of the surroundings among a few participants and, as a result, were more cautious about accessing their devices. The following quotes from participants narrate their experiences of completing the task in the presence of shoulder surfing.

P39: "I will use my phone in the bathroom so nobody can see my screen"

P51: "When I notice I stop doing what I'm doing and become very annoyed and frustrated"

P57: "Yeah because that is an invasion of your privacy & things that you need to be could be confidential"

On the contrary, some participants were unaffected by shoulder surfing, not preventing or slowing them down from accomplishing the tasks they were performing on their devices. This was due to multiple reasons, such as the participants were not doing anything sensitive on their smartphones, like watching videos, so they continued doing it without letting shoulder surfing impact their interaction with the device. Other reasons included that participants accessed private information in private settings only and not in public settings when others surrounded them and therefore shoulder surfing did not affect what they were doing on their smartphones. A few participants just moved their smartphones away from the bystander and continued using their devices. In a few cases, the shoulder surfer was someone known to the participant, and this was a reason for the participant to be less concerned about it. Participants also shared that the shoulder surfing stopped when they caught the shoulder surfer and that helped them to continue back their task without interruption. The impact on task completion was also seen as dependent on the general perception of shoulder surfing by participants, for example, a few participants were seen as not concerned about shoulder surfing in general and therefore continued doing what they were doing. Shoulder surfing made a few participants complete their tasks quickly, forcing them to complete their tasks in less time.

Impact on Device Usage

The impact of shoulder surfing on device usage was perceived from multiple perspectives. Shoulder surfing negatively impacted many participants and raised situational awareness. Some participants were concerned and took protective measures to protect their privacy. For a few participants, shoulder surfing made them reduce their usage, consider the setting of device use, change the physical settings, or avoid using the devices due to privacy and security reasons. It was also dependent on the context of how much shoulder surfing impacted a few participants, such as location. On the contrary, it did not impact many participants. We detail the reasoning for both perspectives below:

For the statement, "experiencing shoulder surfing negatively impacted the way I use my device", 39.56% somewhat or strongly agreed. Shoulder surfing had a negative impact on how users used their devices due to (1) concerns around privacy, (2) taking measures to protect pri-

vacy, and (3) restricted access to information and devices.

Triggering of thoughts on Privacy Concerns before the Reuse of the Device: Before using the device again after experiencing shoulder surfing, participants had a series of thoughts and reflections on privacy concerns. Participants felt their privacy was not respected and the information on their smartphones should be personal to them only. Participants were also concerned that someone could steal their sensitive information. Shoulder surfing made them aware of the potential risks of using the phone in public. Some participants were more aware and cautious of their surroundings and felt unsafe due to who was around them and who possibly was watching them. They had to check their surroundings constantly to avoid being spied on. Participants expressed the realisation that nothing is private anymore. Participants mentioned being care-free in using their devices earlier when they did not have any experience with shoulder surfing; however, now they constantly worry about shoulder surfing. Shoulder surfing made participants self-conscious, apprehensive, and cautious of how they used their device and raised the negative feeling of being embarrassed due to being shoulder surfed. It was considered an invasion of privacy, a rude and intrusive act that made them feel awkward. Participants felt disrespected and distracted and were concerned about being targeted for other threats due to shoulder surfing.

Restricted Access to Device & Information: A few participants voiced that shoulder surfing made them avoid using the device, which negatively impacted the quality of their time, such as commuting time. Participants also voiced that they avoid accessing sensitive information until they are in a private environment, such as one's home. Shoulder surfing made participants hesitant to access data in public. They also believed that they could use their phones in limited spaces only. Shoulder surfing slowed the participants from interacting with the devices and distracted them, making them concentrate less on their tasks. A few participants had to pay increased attention to what they were doing on their phones. Due to the threat of shoulder surfing, participants reduced their usage of their phones.

Protecting Privacy: The negative impact of shoulder surfing on the device resulted in participants trying to adopt measures to protect their privacy. For example, participants tried to keep their screens angled away to hide them from unconsented observations. Participants had to move their positions, shift their whole body to a different angle or lower the brightness of their devices. They had to be more discreet in how they used their devices. One participant got a private screen, making it harder for surrounding people to observe the screen content. A few participants mentioned that the negative impact was due to security reasons.

P72: *"It has made me think a bit more negatively about using my device. I used to be very carefree using my phone, now I always have a worry about being shoulder surfed."*

P97: *"It does make me more aware of strangers and the environment such as a pub after being shoulder surfed in this way. The experience was a negative one and I felt almost embarrassed."*

Perceived Positive Impact A small percentage of participants (12.09%) somewhat or strongly agreed that shoulder surfing positively impacted their device usage. Participants mentioned that they had learnt their lesson and, therefore, the impact of shoulder surfing was perceived to be positive. The lessons shoulder surfing taught them were about awareness of their surroundings and device use, i.e., who was watching them, what they could be sharing unintentionally, and what notifications they wanted to appear on their phones. The experience of shoulder surfing nudged participants to stay more alert and safe and quickly complete their tasks. It made them cautious and careful, and a few acted to protect their privacy, such as repositioning themselves, readjusting the phone at their workplaces or discontinuing using the phone. The threat of shoulder surfing made them thoughtful about accessing specific apps that could contain sensitive information. These actions helped them to stop their information from being further leaked. One of the participants got a privacy screen to help against shoulder surfing. Participants also mentioned that they avoided using smartphones, especially in public transport, opted for restricted use, and only accessed sensitive information in private spaces. These measures helped them to avoid potential shoulder surfing. A few participants were slightly annoyed because of the overall situation, but they were able to get over it quickly. Participants mentioned that the negative impact was a short-lived experience and was forgotten easily and quickly. The experience of being shoulder surfed was also looked at as a positive one as due to shoulder surfing, participants had to put their phones down, but this was good as they should not be constantly looking at their phones. The following quotes from participants reflect the positive perspective on the impact of shoulder surfing on device usage:

P93: *"I have learnt my lesson"*

P94: *"It makes me work quicker to avoid a 'shoulder surfing' "*

P44: *"I need to use my phone less around my children so it was a good thing I stopped and also it meant my messages to my friend stayed private."*

Neutral Responses to Shoulder Surfing Participants who were found to be neutral on the negative impact of shoulder surfing on device usage felt that they were now just more aware of where to sit in public transport or to be more careful about the general surroundings, which could be perceived as positive or negative. Shoulder surfing did not change how they use their devices; it was a frustrating experience, but participants made arrangements such as being more cautious about accessing private information in public, avoiding accessing private information (such as banking information or messages) or not using the device in the same setting until later

to avoid the side effects of accessing them in public. More than the experience itself, participants were focused on the bystander. One of the participants communicated with the bystander on the content being observed, which in this case was the score of a sports match, and everything went smoothly. A few participants referred to themselves as generally complacent and lackadaisical; thus, shoulder surfing did not affect their device use.



Summary: Participants perceived shoulder surfing negatively and positively impacting their device usage for similar reasons, such as taking measures to protect privacy and restricting access to information and devices. However, the difference lies in the perception of users. While some participants felt that shoulder surfing made them aware of their surroundings and, because of this, they knew how to avoid similar situations, some participants reported being constantly worried about potential shoulder surfing. For some participants, the negative impact was long-lived, making them concerned about their privacy and information leakage, while for some, the negative impact was short-lived and forgotten quickly.

4.4.4 User Concerns around Shoulder Surfing

We assessed user concerns around shoulder surfing by asking participants to express their top three concerns around shoulder surfing and their concern for other people's privacy.

Top User Concerns around Shoulder Surfing

When asked about the top three concerns around shoulder surfing, about half of the participants explicitly mentioned privacy, and many mentioned personal information, as well as content-specific concerns (such as banking, biological information, and photos). The remainder gave explanations about privacy-related aspects. For example, some mentioned shoulder surfing being unethical, and a few mentioned misuse of information and perception of self in the eyes of others. Furthermore, a few also mentioned identity theft, data insecurity, information theft, other people's privacy, revealing of inappropriate content, invasion of personal space, risk of a potential stalker, unauthorized access and blackmailing. The following quotes from participants reflect the concerns. The following quotes from participants narrate the concerns of participants:

P66: *"Violation of privacy which is not a personable thing to do."*

P72: *"I worry about my friends/relatives privacy."*

P22: *"loss of data that could lead to theft/hacking/identity theft etc"*

Other People's Privacy

When asked how participants felt about breaches of trust in keeping other people's information safe, they held diverse perspectives on violating trust in other people's privacy. About half of the participants were concerned about other people's privacy, especially for content like photos or messages. It was seen as letting the other person down as the sent message was for only the intended person and not for anyone else. The observed information could be a private inside joke or personal advice for the participant and the sender; however, it may look inappropriate for any other person. Participants voiced that they hold expectations from their friends to keep their content safe with them, which also applies to the participants. If they cannot do so, it breaches privacy and trust. Invasion of other people's privacy was seen as worse than the invasion of personal privacy as it was their responsibility, and they failed to keep the content private. Though the observer and the friend did not know each other, it was still perceived as worrying. Participants also mentioned accessing content in a setting where no one could see it apart from themselves. They also said that they would try not to let similar incidents happen. The following quotes from participants reflect on their perspective on other people's privacy:

P9: *"I feel that I have let that person down."*

P13: *"It would be a breach of trust for their information to be shared unbeknownst to them"*

P19: *"I would keep my friends and family privacy to be safe. They are my most dear relations and I want to keep their information safe. They have immense trust on me and i want to think of their safety first."*

Some participants mentioned that it depends on the type of content that is viewed by a bystander, which would determine if they have violated the trust of the person whose content was viewed. Content such as messages and photos were frequently mentioned concerning content types compared to social media posts. Posts made on social media were not seen as sensitive content and, therefore, not seen as concerning as they were posted on social media and could be viewed by the public. Participants also held the opinion that it depends on the attitude of their friends if they perceive shoulder surfing of their content as concerning or not.

A few participants were more concerned about their personal privacy. Despite whose content was viewed, it was still seen as an invasion of personal privacy. They did not like others knowing what was happening on their phones, as it revealed their lives. It was seen as a personal preference of the participant more than their preference not to let anyone know about the content of their device. Participants mentioned that the smartphone was a personal device to them, and they did not intend to broadcast its information.

P41: *"It's a personal device. If I want to broadcast something then will do it voluntarily."*

A few participants did not mark shoulder surfing as a breach of trust of their friends as it was unintentional and not their fault. The observer invaded the personal space of participants without consent; therefore, participants did not mark the incident as a breach of the trust of their friends. They voiced that they can not have complete control over their surrounding environment but can expect other people to respect their privacy.

On the contrary, some participants were seen as less concerned about other people's privacy. This was due to multiple reasons, including the fact that the bystander does not know the friends of the participants and, therefore, makes no difference if the bystander views the information. Due to the anonymity of the friends, participants felt that there were no real consequences associated with non-permitted viewing of the content of their friends. For anything posted online, having it viewed by the public is an expectation, and this should be understood when posting content online; therefore, anything important or private should not be posted online. They also voiced that a passing glimpse is unavoidable, and their friends should understand this. Participants regarded shoulder surfing as a minor breach which happens all the time.

P65: *"People know that what you share on your phone may not stay private."*

P84: *"It is a small breach but it happens all the time"*



Summary: As seen in prior work, the main concern around shoulder surfing is the privacy of users [85]. However, we also found new discoveries around shoulder surfing in our study, which includes that shoulder surfing is also perceived as a risk leading to more serious threats such as identity or device theft. The concern for other people's privacy varies from one user to another. Due to the differences in the levels of user concern, users can be clustered into different groups based on their concerns and requirements for protection.

4.4.5 Training & Education on Shoulder Surfing

We asked participants if they had received any education or training on protecting their information from shoulder surfing. To further explore participants' perspectives on protection against shoulder surfing, we also asked about their past experiences using any protection method and their willingness to use protection mechanisms in the future.

Awareness, Training & Education on Technology for Assistance in Mitigating Shoulder Surfing

Participants were asked to report if they knew of any technology or security feature that helps mitigate shoulder surfing. About half of the participants were not aware of any technology; many mentioned using a privacy screen, such as a screen protector that hides the display from certain

angles, and a few mentioned turning off the device, lowering screen brightness, changing the font size of the device, using automatic screen lock, and fingerprint scanner. A few participants specifically mentioned banking apps where the user has to long-press a button to reveal the PIN code, which is not visible otherwise. Almost all participants stated they had not received any education or training on protecting their data from shoulder surfing. A few mentioned sitting beside a wall so that no person could make observations behind them, using selective access to apps when in public, and learning about shoulder surfing and protection against it through the internet.

P78: *"Other than making sure nobody can see your screen, I'm not aware of anything."*

P65: *"...when working in public place sit with back to a wall."*

Previously Used Protection Measures

Next, participants were asked if they had used any additional protection measures in the past. The majority of the participants mentioned using none. A few further mentioned using biometrics such as fingerprint scanners so they do not have to type in their passwords, changing their position, updating the lock screen timing, lowering screen brightness, and using privacy screen protectors. Other user-adopted measures included relying on surrounding awareness, avoiding using phones or having selective access to apps and using their hands to cover the screen from potential observations.

P36: *"i just try and make sure anyone around me isnt in eyeline with my screen and cant see"*

P35: *"Not really. I turn the brightness down on my phone when on the bus and hold it close to me to reduce the chances of someone being able to look at the content."*

P72: *"I use my hand as a cover to protect the privacy on my phone."*



Summary: Participants had no prior education or training on protecting their information from shoulder surfing. Participants relied on non-technical user-level protection measures, such as lowering the screen brightness or covering the screen using their hands, to protect privacy and information leakage.

4.5 Discussion & Directions for Future Work

4.5.1 Shoulder Surfing as the Stepping Stone to Other Serious Threats

Shoulder surfing is not just about observing someone's device screen but also about giving the observer the opportunity to misuse the information in any possible way. In our study, participants were concerned about shoulder surfing leading to other threats such as identity or device

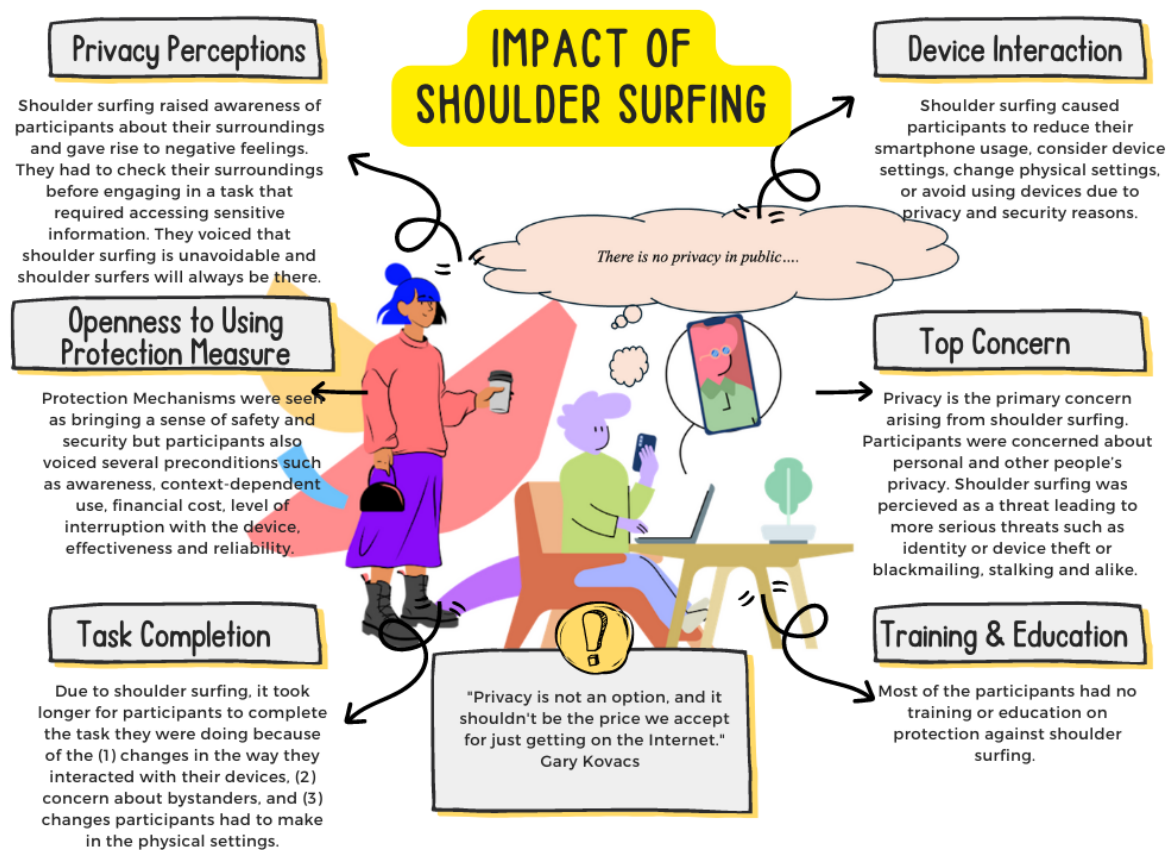


Figure 4.4: High-level summary of the key findings of the impact of shoulder surfing. (The image uses figures by Deivid Saenz and Sofia Salazar [250, 251]. The overall figure was created using CANVA under free license [43]).

theft [324], potential stalking or blackmailing. Previous work has also provided some evidence in this direction where they reported device theft as one of the design factors of solutions for authentication-based shoulder surfing [72]. Another research focused on collecting shoulder surfing experiences reported a story of a participant who expressed concerns about being followed by a bystander who had looked at her Google map address [85]. This shows that there is some real concern involved in shoulder surfing leading to some serious threats. However, due to limited evidence, future work must look into verifying these concerns.



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

4.5.2 Shoulder Surfing by Children Puts Them at Risk

One of the novel concerns raised in the study is when children shoulder surf, as they might see something inappropriate that they may or may not fully understand. Shoulder surfing by children is concerning as it could negatively impact children's perspectives, views, or behaviour. Further, children might shoulder surf authentication credentials, such as PINs, to gain access to their parents' devices. Observing such information can not only give unauthorized access to their parents' devices, but they could also share it with others either involuntarily or through social engineering or exploitation, which would bring even more harm to the parties involved. When having access to parents' devices, children can be manipulated to access and share sensitive information with others. A series of negative events happening one after another can be seen as a consequence of shoulder surfing by children.

Previous work has explored safeguarding children from the harms of technology, focusing on various aspects, such as risks involved in the adoption of online services [296], privacy and security challenges with educational technologies [48], children's AI systems [297], parental concerns around social Virtual Reality [102] and much more. However, shoulder surfing is another concern associated with the use of technology for children, which has not yet been investigated. One way to mitigate shoulder surfing by children is using gaze data to detect the observer's age, as recent research shows age can be inferred from eye movements [172]. This appears to be a promising direction to protect children from unwanted device observations. It must be noted that this approach comes with the challenge of safeguarding bystander's privacy [152]. Therefore, an approach that detects the age of the bystander without compromising the privacy of the bystander should be explored and evaluated.



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

4.5.3 Self-Equipping Users for Protection Against Shoulder Surfing

In our study, participants voiced that they had no training or education on protecting their information from shoulder surfing. This finding is similar to many other related works where participants have voiced that they had received no training or education on protecting their visual privacy. For example, a white paper on visual data security revealed that 98% of respondents agreed that they had no knowledge or training on protecting their visual privacy. This white paper was published in 2012, and our study conducted in 2024 provides the same results. This shows a continuous trend of the lack of education and training on protecting users' privacy. Related work on educating and teaching users has shown promising results in enabling users to be more aware and informed about privacy practices. For example, Khan et al. [164] evaluated the course outcome of privacy threats of Tracking and Pervasive Personalisation in school classrooms, and the results showed students developed transferable knowledge of the privacy implications. Similarly, Smith et al. [268] tested the efficacy of short videos for educating users about targeted advertising on Facebook and showed videos significantly increased user engagement with Facebook advertising preferences. Albayram et al. [9] found that videos conveying risk communication and self-efficacy impact people's intention to use multi-factor authentication. In line with this research, a plethora of other research focuses on educating users using educational video interventions for secure behaviour [30, 71]. Considering the workaround and the success of training and educating users for various security and privacy issues, training and educating users on shoulder surfing looks like a promising solution to help users mitigate the risk. It will be interesting to explore how training through different forms such as posters on public transport, training videos and alike on protection from shoulder surfing could help in protecting the privacy of users.



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

4.5.4 User Awareness Alone Won't Prevent Shoulder Surfing Risks

Participants frequently mentioned awareness of their surroundings in various instances. Participants paid more attention to who was around them and what information they accessed on their smartphones. User awareness appears to be a promising solution to mitigate shoulder surfing as it gives control to the user to decide when the protection is needed and when it is not needed. Prior work also suggests user awareness as the solution for a range of other threats that exist in the surrounding of the user as well such as charging attacks, reflection-based attacks or smudge attacks [47, 210, 240, 313]. However, relying on user awareness may still not be a viable solution for a number of reasons, including that shoulder surfing often goes unnoticed because of the cognitive load induced by the task the user is performing [115]. Therefore, the user can-

not be relied on to be constantly aware of the surroundings. The constant awareness of one's surroundings can also negatively impact the productivity of the user. A constant lookout on the surroundings may lead to user frustration and fatigue. More importantly, shoulder surfing is not the only threat that exploits user unawareness for privacy invasion; there exist many other threats that could be performed by exploiting the unawareness of users, such as reflection-based attacks [240], smudge attack [47] or thermal attacks [2, 25]. Considering the limitations of relying on the users' awareness of the surroundings, it can not be used to solve multiple attacks. Reliance on consistent, secure user behaviour has been criticised in prior work as the unreliable solution for mitigating threats [89, 198]. This instead motivates viable solutions that are not reliant on constant user awareness.



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

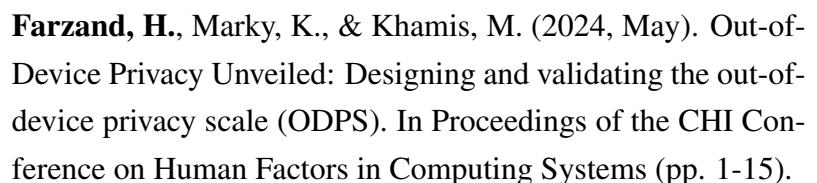
4.6 Conclusion

In this paper, we investigated the aftermath of shoulder surfing with $N=91$ participants who have experienced the threat. We focused the questions around (1) privacy perceptions, (2) interaction with the device after shoulder surfing, (3) user concerns around shoulder surfing, and (4) training and education on shoulder surfing. Our results show that shoulder surfing is a high privacy risk that violates the user's and other people's privacy when data is being observed. Shoulder surfing was perceived as a privacy threat that led to more serious threats, such as identity or device theft. We also found that users received no training or education about protecting their data from shoulder surfing and protection. This work motivates investigating and mitigating everyday life shoulder surfing by following a user-centred design approach. It paves the way to exploring the consequences of shoulder surfing with specific user groups for more ethical and safer technology use.

V

Out-of-Device Privacy Unveiled: Designing and Validating the Out-of-Device Privacy Scale (ODPS)

Publication 4



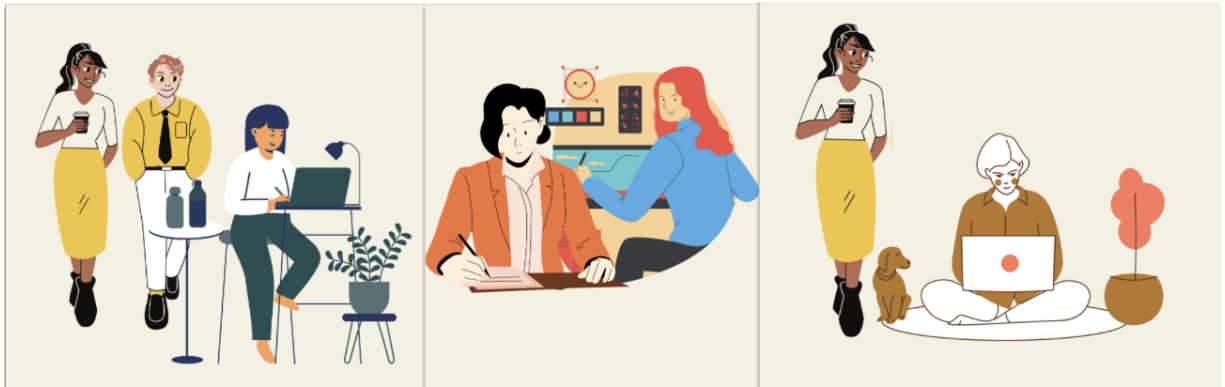


Figure 5.1: The figure shows daily life scenarios when out-of-device privacy threats in the physical world, such as shoulder surfing, take advantage of the user’s physical surroundings to invade data privacy without the user realizing it. (The image was created using Canva under free license [43].)

5.1 Introduction

“There are things known, and there are things unknown, and in between are the doors of perception.”

Aldous Huxley, 1954

Threats to information privacy are not only restricted to device use, such as GUI confusion attacks [29] since the technology surrounding us continuously collects sensitive information and can be used maliciously. Everyday scenarios, such as withdrawing cash at an ATM and being recorded by CCTV [51, 267] or travelling on a bus and being shoulder surfed [85, 94, 95] - all these scenarios make the user’s data susceptible to attacks in the physical world. As we transition into a society increasingly reliant on technology, privacy concerns are becoming more pervasive.

While some attacks on user privacy require the advanced, sophisticated expertise of the attacker, the increased usage of (mobile) devices and tools has enabled such attacks with only little expertise. For example, shoulder surfing can be done through direct observation [85] or recording videos [309]. Moreover, user privacy can be violated simply by using technology gadgets, such as a thermal camera [16] that can infer sensitive input entered on keyboards [2, 12]. The combination of little required expertise for attack execution and increased availability of resources amplifies the vulnerability to privacy attacks. Due to this, anyone could invade anyone’s privacy, putting everyone’s privacy at risk. Privacy researchers have proposed numerous mechanisms to mitigate the out-of-device privacy threats in the physical world. Such mechanisms include visual filters, generating fake text, icon overlaying and vibratory alerts [156, 246, 320]. However, the one-size-fits-all approach cannot be applied. For example, shoulder surfing - a privacy threat that exists out of the device is perceived as concerning by some people, whereas some people do not consider shoulder surfing a risk [85, 127]. In contrast, others switch off or

cover the device with their hand when suspecting a shoulder surfing attack [85, 94, 127]. The differences in reaction towards out-of-device privacy invasions reflect the differences in users' out-of-device privacy profiles. Therefore, precisely mapping mechanisms to user profiles is challenging without knowing users' privacy profiles. Safeguarding privacy from out-of-device threats requires investigating how much importance users prescribe to such threats defined by how users use tech and respond to privacy violations. We propose utilising the notion of "*out-of-device privacy*" to capture this.

While literature lists several privacy-related measures like IUIPC [199], they are limited to specific scopes; for example, the IUIPC precisely measures online information privacy concerns. To date, there is no standard scale to measure users' associated importance towards threats in the physical world. To explore users' importance towards protecting personal information from threats in the physical world, we first propose a definition for "*out-of-device privacy*" and second present an 18-item psychometric scale instrument to measure the importance a person attributes to protecting personal information from out-of-device threats in the physical world. Our scale development process involved three steps: (1) item development, (2) scale development, and (3) scale validation. In the item development phase, we aimed for content validity by following deductive and inductive approaches to collect an initial item pool from literature and experts (N=13). Next, we pre-tested the items with experts and the target audience (N=48), which assisted in refining the wording and provided initial insights into the variability of responses. Finally, we deployed the survey online (N=382) in the scale development phase and used the data to extract underlying factors. Lastly, we performed dimensionality, reliability, and validity tests on a dataset of N=935 participants in the scale validation phase. The scale was iteratively developed and refined throughout all stages in multiple studies involving N=1378 participants. Finally, we confirmed the scale structure and presented the 18-item Out of Device Privacy Scale (ODPS).

Our scale establishes a foundation for assessing out-of-device privacy, facilitating systematic analysis and comparison. The scale provides a lightweight method for security and privacy researchers and technology developers to evaluate and predict users' behaviour to protect the users' data from out-of-device privacy threats in the physical world.

5.2 Background

This section overviews existing privacy scales and discusses the research gap.

5.2.1 Measures of Privacy

Information *privacy* refers to one's desire to control data related to access, use, and sharing [26]. Privacy has been thoroughly investigated in the psychology literature, and numerous attempts have been made to define and measure it. Questionnaires such as IUIPC [199], Privacy Attitude

Questionnaire (PAQ) [57], Westin's Privacy Segmentation Index [143], Concern for Information Privacy (CIFP) [269], Global Information Privacy Concern (GIPC) [199], Online Privacy Concern [36] are among the popular privacy scales in the literature.

Internet Users' Information Privacy Concern (IUIPC) [199] measures the information concern of internet users. While this is a reliable and valid instrument, it is limited to internet users only. However, non-internet applications also require consideration of user privacy, such as photos in the phone gallery app. Alan Westin presented Westin's Privacy Segmentation Index to measure privacy perspectives over time; however, the scale only focuses on the organisation's collection and handling of information. Similarly, the Global Information Privacy Concern Scale covers privacy issues related to online companies but lacks evidence of how the statements comprising the scale were selected. The Concern for Information Privacy (CFIP) [269] scale considers consumer online privacy but it lacks the definition of concern. However, it is a well-validated instrument that can only be used in consumer online privacy contexts. Further, the Privacy Attitude Questionnaire (PAQ) [57] considers the privacy concept as a whole and is unsuitable for measuring a specific attribute of privacy. Most importantly, the scale questionnaires mentioned above only consider online information privacy, not privacy in the physical world.

To sum up, the scales detailed above either focus on a specific attribute or capture the concept of privacy as a whole. Moreover, there is a lack of definitional clarity regarding the objectives of some scales. Finally, these scales only focus on internet use and do not consider privacy in the physical world. Regarding privacy invasions in the physical world, physical world elements, such as awareness, influence the user preferences for protection [91, 93, 94]. There is a need, therefore, for a validated psychometric instrument to measure and capture people's out-of-device privacy.

5.2.2 Out-of-Device Privacy in the Literature

Oates et al. [222] conducted a study to explore differences between the privacy mental models of experts and laypersons by asking an open-ended question to express what privacy means to them. Most participants expressed opinions about privacy in the physical world. This indicates that while protecting user's privacy online is essential, protecting it in the physical world is equally important. Further, in a related research study by Gerber et al. [110], they found that most participants are unaware of the effects of privacy violations and that the users perceive most privacy protections as too fatiguing and complicated. This might be due to the differences in individual perceptions and needs. This highlights the need for user's personalized privacy protection measures. To offer customised privacy protection to users, we must first understand their expectations and preferences for privacy.

Further, assessments of individual attacks have shown that users are impacted negatively due to privacy violations in the physical world. For example, Eiband et al. [85] reported that shoulder surfing gave rise to awkward situations among users. Similarly, further studies have

shown that shoulder surfing causes awkwardness and discomfort and has resulted in interaction time wastage with the device and provided evidence that users are likely to adopt a privacy safeguarding mechanism [94,95]. Following the same line of research, Farzand et al. [93] proposed a typology of perceived sensitive content in response to the users' accounts of shoulder surfing. However, it only provides a list of content types that require protection in different locations but does not consider the user's privacy profile. Cross-culture examinations of privacy concerns have revealed that privacy violations such as observing someone's screen without permission can have severe impacts on the social lives of users in the Eastern world compared to the Western world, such as defamation and spying [252]. Muslukhov et al. [214] investigated users' concerns about unauthorized access and reported that participants were highly concerned about insiders (e.g. friends) having unauthorized access to their devices. This shows that privacy violations and concerns are found in public places and private environments, such as one's home. The work mentioned above illustrates the significance of addressing privacy threats in the physical world and designing countermeasures that suit individual needs and requirements.

Apart from designing countermeasures, one way of mitigating privacy risks is through user awareness. Users' awareness and knowledge of privacy threats assist them in better protecting and handling their data. With the spread of awareness information about protecting data from online threats, users have become more conscious of how they handle the information. For example, in a study by Jiang et al. [147], only 14.1% were unaware of malware-based threats. On the contrary, out-of-device privacy threats, such as shoulder surfing, often go unnoticed [115], and users remain unaware of the privacy invasion. Likewise, while people are aware of emerging technologies such as thermal cameras, they don't always envisage these technologies in the context of privacy bypasses [25]. To improve the awareness of privacy threats in the physical world, there is a need to systematically capture users' out-of-device privacy so that adequate awareness plans and evaluations can be conducted.

A reliable and standardized method is needed to capture users' out-of-device privacy information. Such an instrument would measure the out-of-device privacy perception of users that will assist in the design of personalized privacy settings, which would offer an appreciable user experience while maintaining user privacy from privacy threats in the physical world. The scale would also benefit developers in developing privacy-aware technologies, attracting more users to adopt technology as they adopt technologies devoted to protecting their privacy [81].

5.3 Stage 1: Item Development

This section describes our iterative approach to developing and refining the items to be included in the out-of-device privacy scale.

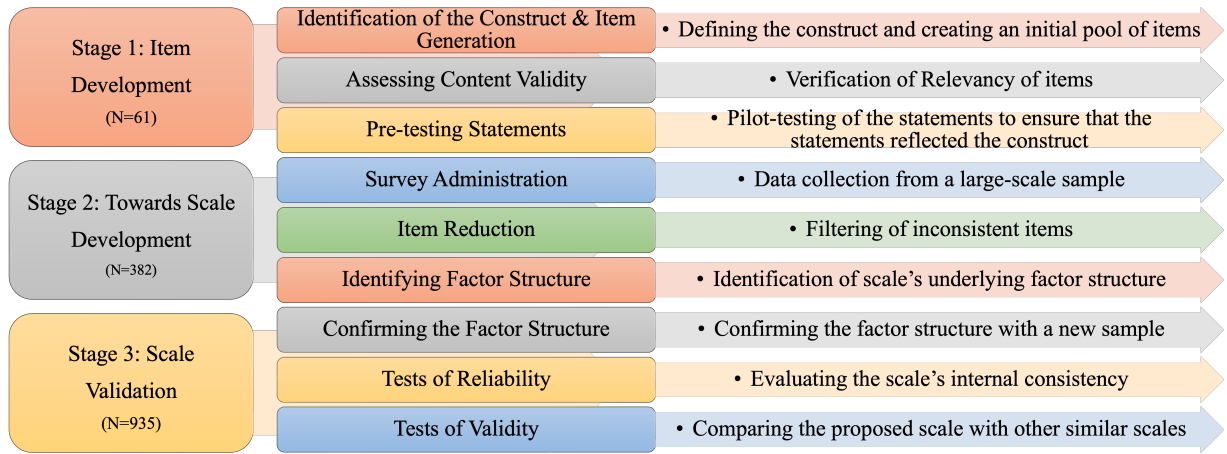


Figure 5.2: We followed three high-level stages to develop the scale: 1) item development, 2) scale development, and 3) scale validation. At each stage, we followed the recommendations from the literature to refine and develop the scale iteratively. The figure shows the breakdown of the high-level phases carried out in the development of **Out-of-Device Privacy Scale (ODPS)** along with the sample sizes in each phase.

5.3.1 Identification of Construct

Our goal was to develop a scale that assesses out-of-device privacy. Towards developing the scale, our first step was to identify the construct and develop a precise definition using simplistic terms. For creating a construct definition, it is essential to consider that it reflects a measurable concept and is sufficiently distinct from other definitions of related constructs. For this, one researcher defined out-of-device privacy. Next, two researchers discussed the definition and iteratively refined it in multiple rounds. This refinement process resulted in the basic definition of out-of-device privacy that we define as follows:

"the importance a person attributes to protecting personal information from out-of-device threats in the physical world"

5.3.2 Initial Item Pool Generation

After establishing the construct definition, our next step in scale development was to create an initial pool of items. There are two commonly adopted approaches for generating an item pool: (1) deductive and (2) inductive. The deductive approach implies extracting items from a theoretical perspective based on, for example, a literature review. In contrast, the inductive approach suggests creating items by asking people's viewpoints on a particular subject [133]. Following a mixed process of deductive and inductive approaches has been recommended as a better alternative than using either method in isolation [31, 212] as it overcomes the limitations of using each method independently. Therefore, we used both ways to derive an initial item pool.

To generate an initial pool of items, we performed the following steps:

1. **Reviewing Existing Literature:** We reviewed existing literature to understand people's experiences and concerns regarding out-of-device threats in the physical world. To the best of our knowledge, we looked for published work where users have reported their concerns or privacy protection practices towards out-of-device threats that match the construct definition, such as shoulder surfing, thermal attacks, smudge attacks and unauthorized access to their device. The reviewed literature included [25, 85, 91, 94, 213, 256]. A total of 20 statements were derived using this approach;
2. **Item Generation by Researchers:** Two authors (N=2) individually created new items related to the construct definition. A total of 24 statements were developed using this approach;
3. **Item Generation by a Larger Group of Researchers:** Fellow researchers (N=11) at our institute with expertise in security and privacy and human-computer interaction participated in a short survey. The survey inquired how they would ask people about out-of-device threats in the physical world. A total of 23 statements were constructed using this approach; (Note: A similar item generation approach has been followed by [128, 199].)

This procedure of item generation ensured a broad coverage of the construct. The total number of items generated at this point was 67 (the reader is referred to Appendix D.1 for the complete list of items constructed using the various approaches detailed above). This number of items is more than twice the number in the final set (presented in section 5.5), which fulfils the recommendation by Kline and Schinka et al. [31, 167, 255].

5.3.3 Refining Items & Assessing Content Validity

Refining items and assessing content validity are crucial in the scale development process and were the next steps after generating an initial pool of items. Moreover, prior work has shown a gap between what privacy scales measure and how they are understood by the general public [62]. Therefore, items should be formulated to exhibit minimal subjective interpretation and be easily understandable by the general public and precise wording [31].

To refine the items and assess content validity, we asked a fellow human-computer interaction (HCI) researcher with a psychology background and English as the native language to review the items and check for four main aspects to account for content validity [305]:

1. Identification of duplicates or similar worded items,
2. Verification of item relevance to the construct definition,
3. Checking of subjective interpretation, and

4. Inspection of linguistic accuracy.

Out of 67 items, 32 were marked as duplicates, and four were marked as irrelevant to the construct definition. The remaining items were checked and rewritten (if needed) for linguistic accuracy and to minimise subjective interpretation. After the items were reviewed by an HCI expert with a psychology background, two researchers rechecked them and refined them based on the feedback. The items list was reduced to 31 items (see Appendix D.2).

Pilot Testing

Pilot testing is an essential step before running a study as it helps ensure the smooth running of the study and produces results per the researcher's expectations. Before proceeding with our questionnaire study, we pilot-tested the items from the previous step to check for two things:

1. **Understanding of Statements:** if the items produced valid measurements based on how easily the public can understand them.
2. **Variability in Responses:** if the items show wide variability across responses.

The Ethics Committee approved the study at our institute. We deployed the items in an online survey using Qualtrics [237] and advertised it through Prolific [236]. We collected data from 50 participants from the UK. Participants were directed to review item statements concerning privacy and to rate the statements on a 7-point Likert scale based on to what extent they agreed or disagreed with the statement. Additionally, the participants were instructed to identify and report any problems they faced while answering the questions concerning understanding and linguistic accuracy. Keywords, such as "privacy", are often linked to bringing social desirability bias. Researchers warn against the use of such words [84], and the most popular approach to avoid this bias is to use the social desirability scale [67]. However, recent research indicates that the social desirability bias scale does not measure the intended construct [181, 291]. Therefore, we refrained from using the social desirability bias scale. As an alternative, we checked for data skewness and looked for ways to increase data variability by revising the wording of items, which is explained below.

We used attention checks to ensure response accuracy [229] and removed the data of two participants who failed these checks. Among the remaining 48 participants, 13 identified as male, 34 as female, and one as non-binary/third gender. Twenty-nine participants were employed full-time, and eight were employed part-time. Four participants were unemployed, three were retired, two were homemakers, and two were students. Participants aged between 21 years and 68 years ($M=37.89$, $SD=13.56$). The median time to complete the questionnaire was 6.32 minutes. Participants were compensated with 1.10 USD, following the set standard by Prolific for their time.

Most of the statements were easily understood by participants, and participants did not report any significant issues. Participants mentioned a few problems regarding some item statements; for example, "I use biometric authentication to avoid someone observing my password and/or to avoid any oily or heat residues on the screen." was not clear as to which biometric authentication is being referred. Based on the feedback from the participants, we revised the wording of several item statements. Next, we checked for variability by observing descriptive statistics and noted that wide variability was found across most items. No items were removed based on their variability. Finally, two researchers reviewed the complete statements again and inspected for issues or similar wording. A few item statements were removed as they were very similarly worded to other statements. After this step, 26 item statements were retained for further analysis (see Appendix D.3).

5.4 Stage 2: Towards Developing the Scale

Towards developing our out-of-device privacy scale, the next step after item generation was developing the scale. This section explains the data collection process, the participants' details, our data checks, and the results of the exploratory factor analysis.

5.4.1 Initial Data Analysis

A sample of $N=400$ participants was recruited on Prolific to investigate our 26-item questionnaire from the previous step. The sample size was determined following recommendations Nunnally [221], which shows there should be at least ten responses per statement. Further, ten responses per item are among the best practices for scale development [310]. Participants who participated in the pilot study were excluded from taking part in this study. All questions were randomized to avoid order effects.

Eighteen participants were removed from the analysis as they failed the attention check. Out of the remaining $N=382$ participants, $N=135$ identified as male, $N=242$ as female, $N=3$ preferred not to disclose, and $N=2$ self-described as third gender/non-binary. Participants were, on average, 41.16 years old ($SD=13.5$, $Min=18$, $Max=83$). $N=214$ participants were full-time employed, whereas $N=86$ were part-time employed. Twenty participants were unemployed, $N=14$ students, $N=17$ homemakers, and $N=31$ retired. All participants were based in the UK and were compensated for participation by the Prolific recommendation.

Before proceeding with the factor analysis, we checked the data for variability, which included checking for descriptive statistics. The means of the statements were between 3.5 and 5.9, except for two items, 2.13 and 2.104. The SDs were between 1 and 2. Medians ranged from 3.5 to 6 except for two items: (1) *"To avoid people nearby from looking at my smartphone screen, I specifically use a privacy-protecting screen cover (e.g., tampered glass protector)"*, and

(2) "I press extra keys after I have entered my PIN at the atm to avoid anyone taking a heat-trace picture of my PIN". No items were removed based on their response distribution.

Next, we calculated the item-total correlation of items and four items were removed as their item-total correlation was less than 0.30 [31]. We then checked for internal consistency amongst the remaining 22 items using Cronbach's alpha [66]. The items exhibited high internal consistency ($\alpha=0.884$).

5.4.2 Exploratory Factor Analysis

As a pre-requisite to establishing the number of factors and their structure, we first evaluated the suitability of our dataset, whether it measured common factors, and whether they were correlated. We checked this by performing the Kaiser-Meyer-Olkin (KMO) Measures of Sampling Adequacy (MSA) test [46]. KMO indicates how much a correlation matrix contains factors or simple chance correlations. A KMO value of 0.60 or higher is appropriate for factor analysis [305]. In our case, the entire dataset had a KMO value of 0.914, considered "marvelous" [150] and thus well within the bounds of adequacy. None of the items had a lower KMO (*i.e.*, less than 0.5). Bartlett's test of sphericity ($\chi^2 = 2561.179$, $p < .001$) further confirmed that the set of items was suitable for factor analysis [271, 310].

Next, the visual inspection of the scree plot revealed that the kink was between two and three factors, as seen in Figure 5.3. The "kink" in the scree plot indicates the number of factors we should be looking for [40]. Using the elbow method, the scree plot suggested a single-factor solution. To confirm the interpretation, we explored two and three-factor solutions. We performed principal axis factoring with varimax rotation using a loading cut-off of 0.35, the recommended threshold [31, 125]. The three-factor solution did not give a meaningful output, and two of the factors had a conceptual overlap. Therefore, we next explored a two-factor solution. The two-factor solution produced a simple structure. To decide between the two-factor solution and a single single-factor solution, we checked for correlations between the factors in the 2-factor solution and calculated the Pearson correlation.

For this purpose, scores of each factor were calculated by averaging the constituent items. There was a statistically significant positive correlation between the two factors ($r=0.635$, $p < .001$). The high correlation between the factors, the scree plot interpretation and the above discussion suggested a single-factor solution would be suitable. To further confirm this, we explored multi-factor solutions using an oblique rotation (*i.e.* direct oblimin) as detailed in Appendix D.5. This further analysis confirmed that a single-factor solution is more suitable.

After deciding on the single-factor solution, we proceeded with further analysis. Four items loaded below 0.40, the recommended minimum threshold of loading [305]. We removed three out of four items for this reason. Still, we kept the item (*item 5*) with a loading of 0.371 as we felt this item represented a particular attribute of out-of-device privacy, *i.e.* concern for other people's privacy, and was not captured elsewhere in the set of item statements. Further,

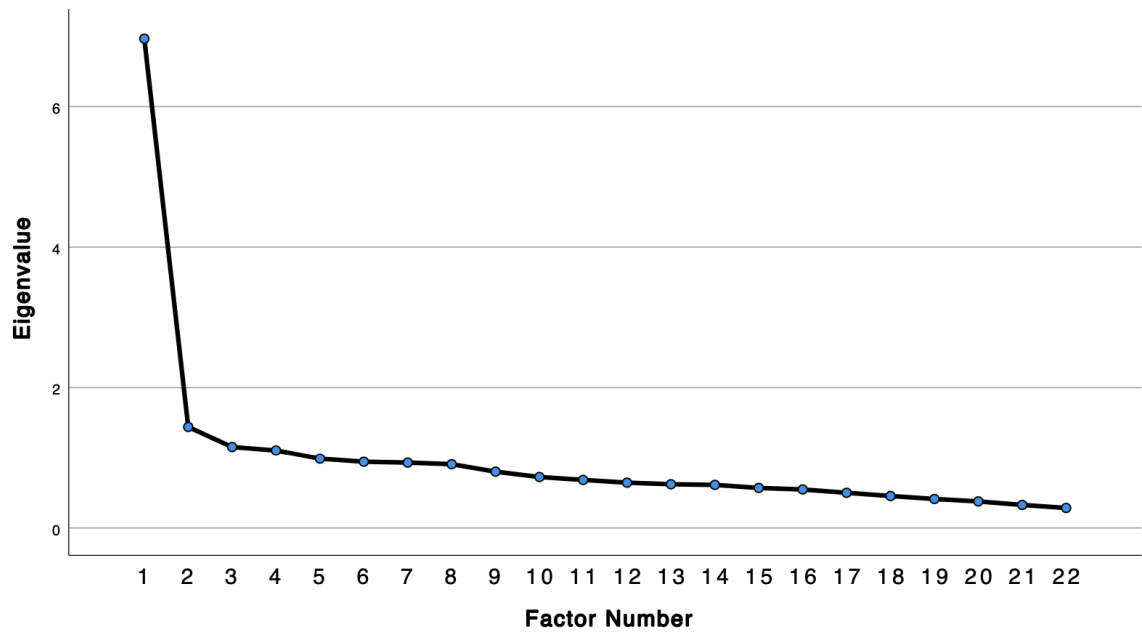


Figure 5.3: The figure shows the scree plot produced using the data for Exploratory Factor Analysis to determine the appropriate number of factors.

the loading of this particular item was not lower than 0.35 (unlike the remaining), which is the minimum threshold and was close to 0.4. For this reason, *item 5* was included in the scale questionnaire. The three removed items are marked in red in Table 5.1. Next, we checked for Cronbach's alpha after removing the three items: ($\alpha=0.888$). The 19 items from this step were retained for further analysis in the following steps.

5.5 Stage 3: Final Scale Validation

We performed a confirmatory factor analysis to confirm the previous section's explored factor structure. For this, we deployed the 19-item questionnaire using Qualtrics as an online questionnaire on Prolific. Participants from previous studies (pilot test and study 1) were excluded from participation, ensuring a new independent sample [31].

5.5.1 Study Design

The online questionnaire included the 19 items shortlisted from the previous section. In the questionnaire, we also had the items from the IUIPC [199] and CFIP [269], which measure on-line privacy concerns to investigate how closely our proposed scale is related to other privacy constructs¹ All items from IUIPC and CFIP used a 7-point Likert scale, and responses ranged from "strongly disagree" to "strongly agree". All questions were randomized to avoid sequence

¹Please, note: We are aware that the CFIP "collection" subscale is repeated in the 10-item IUIPC scale, but we included it anyway and made the comparison as both subscales differ slightly in items' wording. We report the results with both subscale "collection" versions.

IN	Item Statement	FL
21	It is important for me to protect my screen content from people around me on public transport	0.77
25	I am worried that someone might access my information by spying on what I am doing on my smartphone	0.684
26	I get anxious when someone from my surroundings invades my privacy by looking at the screen	0.711
24	I am a privacy-centred person	0.643
17	I consider my data to be a target for external threats to my device such as shoulder surfing	0.609
18	I believe my data is worth protecting from external threats to my device	0.452
20	It is not fine for me to have my smartphone screen visible to the public	0.591
23	I mind if a stranger sitting next to me takes a look at my smartphone while I am watching a private video	0.512
19	Privacy invasion by people surrounding us is effective in leaking information	0.513
14	The increasing availability and affordability of audio, video and photo recording devices are a threat to everyone's privacy	0.449
9	I feel concerned when using ATMs that use cameras for recording purposes	0.456
15	I would like my device to do something to alert me every time someone looks at it without my permission	0.429
8	I would change all of my passwords immediately if my smartphone was lost	0.451
5	If someone sees my friend's content on my screen, it feels like a breach of my friend's trust in me to keep their content private	0.371
12	Among the reasons I use auto-fill for passwords on my smartphone, is to avoid anyone overseeing what I enter	0.477
16	I scroll quickly when I sense someone is looking at my smartphone's screen	0.606
1	I try to adjust my hand position when using my smartphone so that no one can see the information shown on it	0.557
13	I check for any surrounding people when I am doing something on my smartphone in public places	0.644
2	If anyone looks at my screen without permission, I tend to put my smartphone away	0.576
4	I lower my screen brightness so that no one around me can take a look at what is shown on it	0.337
3	To avoid people nearby from looking at my smartphone screen, I specifically use a privacy-protecting screen cover (e.g. tampered glass protector)	0.306
6	I use fingerprint (or other biometric methods) mainly to avoid someone observing my password	0.306

Table 5.1: The Table shows the results of Exploratory Factor Analysis. The items marked in **red** (last three items) were removed from further analysis as they did not load sufficiently high. IN = Item Number; FL = Factor Loading.

effects [242]. We also used attention check questions for participants' attention and responsiveness towards the study [229].

5.5.2 Participants

We collected data from 1,000 participants, out of which N=65 failed the attention check, and therefore, their data was excluded from the analysis. From the remaining N=935, N=554 self-identified as females, N=371 as males, N=8 as non-binary/third gender, and N=2 preferred not to say. Participants were aged between 19 and 90 (Mean=43.39, SD=13.81). Most participants were employed full-time (N=515), while N=179 were employed part-time. N=83 participants were retired, N=68 were unemployed, N=52 were homemakers, and N=38 were students. All participants were based in the UK and were compensated for their time per the Prolific's recommended rate.

5.5.3 Initial Data Analysis

Before proceeding with the confirmatory factor analysis, we checked the data's suitability by computing the Kaiser-Meyer-Olkin (KMO) Measures of Sampling Adequacy (MSA) test. The full dataset has KMO = 0.956, and none of the items had a lower KMO than 0.907 [310]. Bartlett's test of sphericity ($\chi^2 = 7562.784$, $p < .0005$) further confirmed that the set of items was suitable for factor analysis [271].

5.5.4 Confirmatory Factor Analysis

We performed a confirmatory factor analysis to provide statistical support to the explored factor structure in the previous section. We calculated the following fit indices: the Root Mean Square Error of Approximation (RMSEA), the Comparative Fit Index (CFI), and the Tucker-Lewis Index (TLI) [31]. We intentionally did not consider chi-square goodness-of-fit as it is reported to be unreliable for large data samples [137, 261]. The results revealed that $CFI = 0.911$, $TLI = 0.889$, and $RMSEA = 0.068$. While RMSEA and CFI indicated acceptable fit, TLI was slightly lower than the recommendation (i.e. should be greater than 0.9) [219].

We followed a step-wise model selection procedure with backward elimination to improve TLI by checking for item loadings. The item with the lowest loading was removed to see if it improved TLI. The item with the least loading was *item 9*. We found that by eliminating *item 9*, all indices resulted in a good model fit (i.e. $CFI=0.923$, $TLI= 0.903$, $RMSEA=0.066$) [27, 165, 197, 219]. We assume that this may be because only *item 9* related to using ATMs. In contrast, no other items were associated with or about ATMs. Thus, our final scale contains 18 items, as shown in Table 5.3.

5.5.5 Tests of Reliability

Reliability is the internal consistency commonly measured using Cronbach's alpha [40, 66]. A coefficient of 0.70 or higher is considered acceptable. For the 18 items, Cronbach's alpha was 0.917, well above the recommendation of 0.70 [31]. Next, we computed the composite reliability score [241], which turned out to be 0.922, high above the recommended threshold of 0.60 [24].

5.5.6 Construct Validity

Scale validity refers to whether the measured concept fully corresponds to the construct it aims to measure [40]. This defines construct validity, which is the foundation of any questionnaire [41]. We performed a convergent validity analysis to assess the construct validity of ODPS.

We compared ODPS with the 10-item IUIPC and CFIP to assess convergent validity. We hypothesized a positive relation between the subscales of IUIPC and CFIP overall, as all three scales relate to privacy but capture different dimensions of privacy. Table 5.2 shows the results of the correlations and percentage variability along with the reliability score calculated using Cronbach's alpha [66] for each of the subscales of IUIPC and CFIP. Our scale demonstrated positive correlations with all subscales of IUIPC and CFIP ($p<0.001$). However, none of the correlations exceeds 14.44% variability, showing a maximum of 14.44% conceptual overlap of ODPS with the compared subscales. This much overlap is expected as online privacy and out-of-device privacy, both fall under the privacy umbrella. However, 85.56% total variability cannot be explained by concerns about how organizations handle data privacy or online privacy concerns.

		τ	Variability %	α
IUIPC	Control	0.368	13.54	0.727
	Awareness	0.38	14.22	0.732
	Collection	0.359	12.89	0.904
CFIP	Errors	0.303	9.18	0.86
	Unauthorized Use	0.222	4.93	0.827
	Improper Access	0.304	9.24	0.804
	Collection	0.327	10.69	0.93
	Overall CFIP	0.377	14.21	0.898

Table 5.2: The Table shows (1) the correlation (Kendall’s Tau) between ODPS and IUIPC & CFIP and (2) the reliability score of each of the subscales in our dataset of the second study.

Therefore, we conclude that our scale (ODPS), which measures out-of-device privacy, differs from how organizations collect, process, store, and use information (i.e. IUIPC and CFIP).

5.6 Discussion

In this paper, we contribute a reliable and valid psychometric instrument to measure the out-of-device privacy of users that describes the importance a person attributes to protecting personal information from threats out of the device in the physical world. We detail the rigorous methodology adapted to develop and refine the scale questionnaire. The 18-item scale fills the gap in protecting against out-of-device threats in the physical world.

5.6.1 Obstructions in Scale Development Studies

Prior work has identified two key obstructions in scale development studies: 1) understanding of scale statements by the general public and 2) verifying if the scale measures the construct it aims to measure [62]. Assessing and ensuring these two key points are crucial in the scale development study as they provide accurate measurements. In our research, we took extra care to ensure both key points were accessed and checkmarked. For example, before beginning the factor analysis, we confirmed whether the general public understood the scale statements accurately. For this, the statements were checked and revised by an HCI expert with a psychology background for relevancy to the construct definition and subjective interpretation. Two researchers then rechecked the items to double-ensure the results. The items were then pilot-tested with a small sample from the general public to check for understanding (see Section 5.3.3). Further, after finalising the scale statements through factor analysis and confirmatory factor analysis, we performed tests for convergent validity to ensure that the scale fully corresponds to the construct it aims to measure (see Section 5.5.6). Therefore, we conclude that we have confidently assessed and ensured high-quality scale development while eliminating the obstacles.

5.6.2 Using ODPS to Measure Out-of-Device Privacy

ODPS will be helpful to researchers who aim to mitigate privacy threats in the physical world. It can be easily deployed in an online questionnaire format and distributed on a large scale. ODPS would provide insights into the user privacy profile, which could then be used to inform the design of protection mechanisms. Further, researchers can utilize it to measure the privacy behaviour of a user group. The scale can help explore how privacy perception changes over time and across different user groups. ODPS can offer to answer research questions like: *To what degree are users concerned about protecting their information from privacy threats in the physical world?* or *What is the users' level of awareness of privacy threats in the physical world?* or *How much users are willing to do to protect their privacy from threats in the physical world?*.

5.6.3 Using ODPS to design Protection Mechanisms

ODPS will be advantageous in designing protection methods against threats in the physical world, such as shoulder surfing. For example, a low ODPS score would indicate that the user prefers a light protection method. In contrast, a high ODPS score would mean the user is highly concerned about privacy and prefers a strong protection method. In the same way, the ODPS score could reflect user awareness of privacy threats in the physical world. This could empower users to defend their privacy with and without a device-based mechanism. Researchers could develop awareness strategies based on the scores to educate users on privacy violations.

Further, ODPS could also be used to enhance the design of protection mechanisms by controlling participants' out-of-device privacy attitudes. For example, in a usability or user experience evaluation study of a protection mechanism, ODPS could serve as a covariate to ensure that the participant's experience outcome is the result of the change in the design of the protection mechanism and not due to the differences in their out-of-device privacy. In summary, ODPS could offer to investigate research questions like: *What is users' level of awareness of privacy threats in the physical world?* or *How can the design of protection mechanisms improve to reflect the user's out-of-device privacy perception better?*.

5.6.4 Using ODPS to measure Privacy Culture

The perception of privacy changes as we move across cultures [252]. For example, shoulder surfing can have severe consequences in some cultures like the Middle East, whereas it is sometimes ignored in Western cultures [85, 252]. ODPS would help measure the privacy culture, which could be incorporated into the tech devices. Based on this, users can be offered personalized protection based on their cultural setting.

Item	Statement
1	It is important for me to protect my screen content from people around me on public transport
2	I am worried that someone might access my information by spying on what I am doing on my smartphone
3	I get anxious when someone from my surroundings invades my privacy by looking at the screen
4	I am a privacy-centred person
5	I consider my data to be a target for external threats to my device such as shoulder surfing
6	I believe my data is worth protecting from external threats to my device
7	It is not fine for me to have my smartphone screen visible to the public
8	I mind if a stranger sitting next to me takes a look at my smartphone while I am watching a private video
9	Privacy invasion by people surrounding us is effective in leaking information
10	The increasing availability and affordability of audio, video and photo recording devices are a threat to everyone's privacy
11	I would like my device to do something to alert me every time someone looks at it without my permission
12	I would change all of my passwords immediately if my smartphone was lost
13	If someone sees my friend's content on my screen, it feels like a breach of my friend's trust in me to keep their content private
14	Among the reasons I use auto-fill for passwords on my smartphone, is to avoid anyone overseeing what I enter
15	I scroll quickly when I sense someone is looking at my smartphone's screen
16	I try to adjust my hand position when using my smartphone so that no one can see the information shown on it
17	I check for any surrounding people when I am doing something on my smartphone in public places
18	If anyone looks at my screen without permission, I tend to put my smartphone away

Table 5.3: The table shows the final look of the 18-item Out-of-Device Privacy Scale (ODPS)

5.6.5 Using ODPS in Combination with Other Privacy Scales

ODPS, in combination with other privacy scales such as UIIPC [199], can help construct a privacy profile of users which would explain users' perceptions of privacy in the online and physical world, summing up as a complete privacy profile. This privacy profile could then be used to provide holistic protection to user's information online and in the physical world.

5.6.6 Instructions for Scoring

ODPS is a psychometric instrument developed to measure the out-of-device privacy of users. To use the scale questionnaire, the statements should be presented using a Likert scale with 7 points, starting from strongly disagree to strongly agree. All items are mandatory to answer, and no item requires reverse scoring. The scale statements should be randomized to avoid order effects. The scale score can be calculated by averaging the components' scores.

5.6.7 Limitations & Future Work

Scale validation is a continuous process. While we followed the best practices from the literature in iteratively developing and refining the scale, further studies must be conducted to provide statistical strength to ODPS. Second, while we recruited a large number of participants, all participants were based in the United Kingdom. This might have introduced selection bias. Further studies with participants from different geographic locations should be conducted to strengthen the validation of the scale. Third, while we followed the most recommended approach for item generation and item elimination, it may be possible that some possible factors were not captured during our process. Although our items produce reliable and valid results, future work

should expand on the findings. Lastly, we propose that in future studies, the scale should be administered in mechanisms developer studies to investigate ODPS's impact on the design of privacy protection mechanisms.

5.7 Conclusion

In this paper, we present a reliable and valid 18-item psychometric scale, the "out-of-device Privacy Scale (ODPS)", to capture the out-of-device privacy of users. We followed the best scale development practices from the literature, ensuring a rigorous methodology. We present a detailed description of each step of the development and validation of the scale. With the aid of ODPS, privacy and security researchers will be assisted in designing user-centred protection mechanisms offering personalized and holistic protection against out-of-device threats in the physical world.

5.8 Acknowledgements

We thank all participants for their time and participation. We are also grateful to Prof Paul Cairns (University of York), Dr Graham Wilson and Dr Shaun Macdonald (University of Glasgow) for their support and guidance throughout the project. This publication was supported by an Excellence Bursary Award by the University of Glasgow, the Scottish Informatics & Computer Science Alliance (SICSA), an EPSRC New Investigator Award (grant number EP/V008870/1), and the PETRAS National Centre of Excellence for IoT Systems Cybersecurity, which is also funded by the UK EPSRC under grant number EP/S035362/1. This work was supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972. Lastly, we would like to acknowledge CANVA for offering support in the form of a Free Content License (Figure 2.1 was created using Canva [43] under Free Content License).

VI

Chapter 6

SoK: Privacy Personalised - Mapping Personal Attributes & Preferences of Privacy Mechanisms for Shoulder Surfing

Abstract: Shoulder surfing is a byproduct of smartphone use that enables bystanders to access personal information (such as text and photos) by making screen observations without consent. To mitigate this, several protection mechanisms have been proposed to protect user privacy. However, the mechanisms that users prefer remain unexplored. This paper explores correlations between personal attributes and properties of shoulder surfing protection mechanisms. For this, we first conducted a structured literature review and identified ten protection mechanism categories against content-based shoulder surfing. We then surveyed N=192 users and explored correlations between personal attributes and properties of shoulder surfing protection mechanisms. Our results show that users agreed that the presented mechanisms assisted in protecting their privacy, but they preferred non-digital alternatives. Among the mechanisms, participants mainly preferred an icon overlay mechanism followed by a tangible mechanism. We also found that users who prioritized out-of-device privacy and a high tendency to interact with technology favoured the personalisation of protection mechanisms. On the contrary, age and smartphone OS did not impact users' preference for perceived usefulness and personalisation of mechanisms. Based on the results, we present key takeaways to support the design of future protection mechanisms.

Publication 5

SoK: Privacy Personalised - Mapping Personal Attributes & Preferences of Privacy Mechanisms for Shoulder Surfing

Abstract: Shoulder surfing is a form of eavesdropping on the victim's screen as they use a personal device. This paper presents a systematic literature review (SLR) of the state-of-the-art in shoulder surfing research. The review identifies the research gaps in the field and provides a framework for future research. The review also identifies the research gaps in the field and provides a framework for future research. The review also identifies the research gaps in the field and provides a framework for future research.

Farzand, H., Marky, K., & Khamis, M. (2025, May).
SoK: Privacy Personalised - Mapping Personal Attributes & Preferences of Privacy Mechanisms for Shoulder Surfing. Under review at IEEE Security & Privacy 2025.
<https://arxiv.org/abs/2411.18380>

6.1 Introduction

By the end of 2023, 70% of the world's population was using smartphones [280]. Smartphone users are increasing every day and are expected to reach 62.53 million users alone in the UK by 2029 [281]. Smartphones are no longer just phones but the interfaces to users' personal lives. With the use of smartphones comes the threat of privacy invasions, with shoulder surfing being one of the most frequently reported privacy threats [94]. Shoulder surfing - belonging to the novice attack category in the ecosystem of social engineering and side-channel attacks, refers to observing someone's device screen without permission [?, 85]. Possibly, the reason behind the existence of shoulder surfing lies in its ease of execution. For example, shoulder surfing only requires an observer to be close to the victim user and carefully observe the device content [89]. Shoulder surfed content can be classified into two categories: authentication, such as passwords or PINs [158], and content, such as photos or text [85, 93, 94]. While both categories of shoulder surfing have been reported by users, content-based shoulder surfing is more frequently reported by users [85, 91, 93, 94]. To protect users' privacy from content-based shoulder surfing, researchers have proposed several device-based mechanisms that range from applying a filter over the full screen, such as grayscale [320], to customized content hiding, such as blackout or crystallise filter [156, 295].

The device-based mechanisms may deliver effectiveness in terms of security and usability, but they may not be ideal for every user group as every user has their own preferences and needs. Therefore, applying a one-size-fits-all approach to all users is challenging. This is also evident from research on user interface design that a one-size-fits-all solution rarely meets the demand for appreciable user experiences [65]. This signifies the importance of designing mechanisms that tailor every user group's needs and preferences. Providing a personalized user experience while considering users' personal attributes advocates for users' tailored privacy. Further, the literature presents several such examples that provide evidence that personal attributes such as age, gender, and technical affinity impact users' privacy-related behaviors [13, 192].

However, the present research lacks an understanding of how personal attributes shape a user's preference for protection mechanisms against shoulder surfing which is a frequently occurring incident. Knowing how to build user-centred privacy protection mechanisms targeted at specific user groups is important to offer adequate protection to users against shoulder surfing. To address this missing puzzle piece, our first research question is:

RQ₁: Protection Mechanisms: What are the existing protection mechanisms against shoulder surfing?

Following the exploration of available protection mechanisms, the next step is to inform the design of protection mechanisms. For this, the first step is to understand what properties of protection mechanisms are important to users. For example, in an interview study, users reported having a mechanism that communicates irrelevant information to the observers so that

the observer knows that they have been caught shoulder surfing by the user [91]. Therefore, we assess the properties of mechanisms: ability to alert the user, ability to mitigate the observation, conveying irrelevant information to the bystander, conveying bystander information, and unnoticeable (non-visual) mechanisms. This is important to know for future researchers focusing on the design of protection mechanisms. This motivates our next research question:

RQ₂: Perception of Privacy Protection Mechanisms Against Shoulder Surfing: How do users perceive different privacy protection mechanisms developed for protection against shoulder surfing?

The next step towards designing user-centred protection mechanisms is to look into how users' personal attributes correlate with their perceptions of specific properties of protection mechanisms. To this end, our final research question in this investigation is:

RQ₃: Personal Attributes & Properties for Protection Mechanisms: Which personal attributes (for example, age, gender, importance for out-of-device privacy) correlate with properties of protection mechanisms?

To answer the above-listed research questions, we opted for descriptive research that focuses on already existing protection mechanisms [79, 279]. We conducted a survey of the literature to answer **RQ₁** and narrowed down protection mechanisms against content-based shoulder surfing for smartphones. We then conducted an online survey with a sample from the UK (N=192) to answer **RQ_{2,3}**. The questionnaire focused on exploring people's general perception of those protection mechanisms and capturing personal attributes that describe our participants, such as age, gender, importance for out-of-device privacy or affinity for technology.

We found that participants agreed that the presented mechanisms offered privacy protection. However, they preferred non-digital alternatives, such as covering the screen using their hands, to device-level protection mechanisms, such as screen visibility filters. Moreover, participants expressed that they would not go out of their way to install the mechanisms on their devices if they were not installed by default (sec 6.6.3). Among all mechanism categories, the icon overlay, which shows an alerting icon on the top of the screen to indicate bystanders, was most favoured by participants, followed by haptic feedback, physical tangible objects, and adjusting screen brightness to protect privacy (sec 6.6.4). Further, we found that the general perception of mechanisms can be categorised into two components: perceived usefulness and personalisation of privacy protection mechanisms (sec 6.6.5). Participants who viewed out-of-device privacy as highly important were more likely to prefer and personalise protection mechanisms. Participants with a high tendency to engage with technology scored low on the perceived usefulness of mechanisms but preferred personalisation more. Our findings also showed that there are no differences in preferences for perceived usefulness and personalisation of mechanisms between iOS and Android users. Our research presents evidence of how personal attributes such as age and preferences for privacy play a role in shaping preferences for protection against shoulder

surfing. For example, participants who viewed out-of-device privacy as highly important were more likely to favour the usefulness and personalisation of protection mechanisms. Moreover, age did not impact users' preference and personalisation of mechanisms (sec 6.6.6). Based on the results, we present design guidelines for developing protection mechanisms to assist developers and researchers (see section 6.7.2).

Contribution Statement:

1. **Literature Survey:** We present the results of a survey that narrows down the list of content-based protection mechanisms against shoulder surfing.
2. **User Perception Investigation:** We evaluate the users' perception of protection mechanisms extracted from the literature review to identify the influence of personal attributes towards preference and design of protection mechanisms.
3. **Key Takeaways:** Based on the results, we present key takeaways useful for designers and researchers for building novel mechanisms.

6.2 Background & Related Work

This section synthesises existing research around protection mechanisms for content-based shoulder surfing and presents an overview of the role of personal attributes in shaping privacy preferences.

6.2.1 User-Level & Device-Level Protection Mechanisms

Numerous studies focusing on shoulder surfing have provided evidence for users' concerns around shoulder surfing [85, 91, 93, 94]. Studies report that users are concerned about their and other people's privacy who's data is viewed [85]. Users also reported that shoulder surfing is not just a breach of privacy but also creates negative feelings between the user and the observer [85, 91, 94]. Due to privacy and social concerns arising from shoulder surfing, users opt for various user-level i.e. manual protection measures such as tilting the device, switching between apps, or turning off the phone [85, 91, 94]. Users have also reported using a privacy screen as a protective measure to safeguard their devices from shoulder surfing [85]. Use of these measures has been shown as dependent on the relationship between the observer and the user [91]. While these measures provide some basic protection against shoulder surfing, they are limited in their efficacy as they can only hide the screen content from specific angles [162]. Moreover, the user also needs to always remain alert to spot potential shoulder surfers and use user-level manual protection measures, which may not always be feasible. Researchers have proposed several device-level i.e., software-based mechanisms to overcome the limitations of user-level manual

protection measures and provide an enhanced privacy experience. Such mechanisms include lowering the screen brightness [320] or replacing the content displayed on the screen with randomly generated content [211]. Researchers have also explored haptic-based mechanisms, such as device vibrations as a way to alert the user for shoulder surfing [246]. Related work pins down several similar mechanisms that offer content-specific protection, such as for photos or text [292] or full-screen protection regardless of content [156]. Despite the huge effort of researchers in developing novel ways to mitigate shoulder surfing and protect the privacy of users, a holistic list of the proposed protection mechanisms remains unexplored. This is important to know as it provides evidence of what protection ideas have been developed and evaluated and also paves the way for further improvement and refinement of those protection mechanisms. Having this knowledge allows researchers to expand on the existing ideas and research on undiscovered aspects of mitigating shoulder surfing.

6.2.2 Personal Attributes & Privacy Preferences

Users vary in their needs and preferences for privacy and, therefore, need to be clustered based on their privacy profiles. One commonly used user profiling method is Westin's three categories: unconcerned, fundamentalists, and pragmatists [177]. However, recent work has argued that Westin's three categories might not be related to users' corresponding behaviour [64, 304]. In response to this criticism, Dupree et al. suggested five privacy personas (fundamentalists, lazy experts, technicians, amateurs, and marginally concerned) [83]. While the method of Dupree et al. provided an overall picture of user profiles, researchers have also looked at profiling users for specific topics. For example, for smartphone privacy settings [107], app permissions [189, 192], location sharing [64], or social media privacy behavior [303]. In addition to profiling methods, researchers have also proposed various scales to capture granular concepts such as preferences or concerns to improve users' experience with technology. For example, Internet Users Information Privacy Concerns was proposed by Malhotra et al. to capture the privacy concerns of internet users [199]. Hasan et al. proposed a psychometric scale to capture the importance of other people's privacy [128]. For threats that exist outside the device, such as shoulder surfing, Farzand et al. proposed an out-of-device privacy scale to measure the importance users attribute towards protecting their information from out-of-device threats [96]. While literature presents an enormous collection of profiling users based on their privacy preferences, expectations, and concerns, it remains unclear how these measurements correlate with users' preferences for privacy mechanisms.

6.2.3 Research Gap

Extensive research has been carried out exploring ways to mitigate shoulder surfing in the daily lives of users [156, 211, 320]. However, the one-size-fits-all approach cannot be applied due to

individual differences. To this end, we explore how personal attributes shape a user's preference for protection mechanisms against shoulder surfing.

6.3 Stage 1: Collecting Content-Based Protection Mechanisms against Shoulder Surfing

This section describes conducting the systematic literature review to answer **RQ₁**. Our search methodology was as follows:

1) Keywords and Search Space: Two researchers from the field of Usable Security & Privacy discussed the keywords to perform the search and finalized the search query: [All: "shoulder surfing"] OR [All: "shoulder surfing attack*"] OR [All: "shoulder-surfing attack*"] AND [E-Publication Date: (01/01/1999 TO *)]. For the search space, we selected the top 10 venues in "Human-Computer Interaction" and the top 10 in "Computers Security & Cryptography" according to Google Scholar's ranking system (date assessed: July 2024). We selected the time frame of research publication after 1999 as 1999 is the year when one of the most influential human-centred security papers was published [6].

2) Exclusion Criteria: From the search results, we excluded a paper if it did not include the keywords in the full text. We also excluded a paper if it was a poster, a survey or a literature review paper. Further, we excluded a paper that presented an authentication-based mechanism as this paper focuses on mechanisms for content (such as text or photos) or targets a device other than a smartphone or a tablet. We included tablets as smartphones and tablets follow similar design principles. The main search resulted in five papers.

3) Forward and Backward Search: For each paper identified in Step 2, we performed a backwards and forward search to identify relevant papers published elsewhere. This was done to ensure a broad coverage of research contributions in content-based shoulder surfing protection mechanisms. We then reapplied the exclusion criteria to the papers from the forward and backward search. Nine papers were identified through forward and backward search. Table 6.1 presents an overview of the search results.

4) Extraction of Mechanisms: For each of the papers identified from the main search and extended search, we extracted the protection mechanisms. A total of 27 mechanisms were extracted.

Computers & Security Top 10 Venues			
	Venue	Resulted Papers	Selected Papers
1	IEEE Symposium on Security and Privacy	30	0
2	USENIX Security Symposium	35	2
3	IEEE Transactions on Information Forensics and Security	30	0
4	Computers & Security	48	0
5	ACM Symposium on Computer and Communications Security	32	0
6	Network and Distributed System Security Symposium (NDSS)	4	0
7	IEEE Transactions on Dependable and Secure Computing	18	0
8	Journal of Information Security and Applications	22	0
9	International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT)	0	0
10	international Cryptology Conference (CRYPTO)	0	0
Total		219	2
HCI Top 10 Venues			
	Venue	Resulted Papers	Selected Papers
1	Computer Human Interaction (CHI)	102	2
2	Proceedings of the ACM on Human-Computer Interaction	9	0
3	International Journal of Human-Computer Studies	10	0
4	International Journal of Human-Computer Interaction	12	0
5	IEEE Transactions on Affective Computing	0	0
6	Behaviour & Information Technology	7	0
7	Virtual Reality	18	0
8	Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies	20	0
9	International Journal of Interactive Mobile Technologies	26	1
10	ACM/IEEE International Conference on Human Robot Interaction	0	0
Total		204	3
Forward & Backward Search (N=5)		262	9

Table 6.1: The Table shows the results of the systematic literature review conducted on the top 10 venues in HCI and Computer Security according to Google Scholar (accessed: July 2024).

6.4 Stage 2: Categorisation of Mechanisms

After identifying the mechanisms against shoulder surfing in the literature, the next step was categorising them into groups. This section explains our rationale and categorisation strategy for the mechanisms.

6.4.1 Categorisation Strategy

In this stage, we categorised the mechanisms resulting from Stage 6.3 based on how the information is displayed on the screen. For this, one researcher extracted all mechanisms proposed in each of the papers along with their pictorial representations and descriptions. Then, the researcher identified commonalities in the design of information presentation in the presence of a shoulder surfer. Mechanisms with similar designs were grouped under one category. This resulted in a total of ten mechanism categories. Table 6.2 presents each mechanism's categorisation and source. A group description for each of the mechanism categories was then formulated. Next, two researchers reviewed the categorisation and the group descriptions, and any disagreements were resolved in a meeting. The categorisation and descriptions were revised based on the discussion. Next, we created videos of all mechanisms showcasing their functionality and included them as a group mechanism in the survey. To ensure an accurate reflection of each mechanism, we first checked for if a video representation of the mechanism had been made available by the researchers. If it was available, we used the respective mechanism video. In case a video was not available, we relied on the information available in the paper to develop a video prototype. This ensured that participants received a complete and accurate idea of all mechanisms in each category.

6.5 Stage 3: Data Collection

After identifying and categorising the protection mechanisms in the literature, our next step was to develop a questionnaire and collect data. This section details our methodology and data analysis and presents the questionnaire's results.

6.5.1 Questionnaire Design

Our goal was to collect user preferences for protection mechanisms against content-based shoulder surfing. To collect data from a large and diverse population, we developed an online questionnaire on Qualtrics [237]. The questionnaire comprised of the following components:

1. **Information Sheet & Consent:** Before beginning the questionnaire, we presented participants with an information sheet detailing the aim and required tasks for the completion

Mechanism Category	Description	Source
Display Color Change	a mechanism that changes the display into a monochrome combination of black and white upon the detection of bystanders	[320]
Screen Brightness	a mechanism that lowers the screen brightness to make the content less visible from a distance	[52, 187, 316, 320]
Selective Visibility	a mechanism that offers a selective viewing experience by making the part the user gazes at visible while making the rest invisible to the human eye	[156, 295, 320]
Distortion	a mechanism that obfuscates the image into small pixels	[156, 283, 285, 292, 320]
Blurry	a mechanism that makes the device screen unclear, reducing the sharpness of the display	[70, 285, 292]
Replacement by Protective Text	A mechanism that replaces the content of the device screen by randomly generated unmeaningful text is activated.	[211]
Replacement by Meaningful Text	a mechanism replaces the content of the device screen with randomly generated meaningful text	[156]
Physical Tangible Component	a mechanism that relies on physical components, i.e. external to the device screen itself, not involving rendering on display - is activated, such as an LED light, which is an external part of the device but not the screen display.	[246]
Icon Overlay	an icon-like mechanism that is placed on the top of the screen to indicate bystanders	[246]
Haptic	A mechanism that relates to the sense of touch is activated. In the case of shoulder surfing, the user will be alerted through phone vibrations	[246]
Combination	A mechanism that combines multiple features into one mechanism is activated upon the detection of a shoulder surfer. For example, it adjusts font size, color scheme, and screen brightness - all of them together.	[184, 239]

Table 6.2: The Table shows an overview of the ten mechanism categories derived from literature.

of the study. We presented the participants with information on shoulder surfing with a detailed description and pictorial representation. The participants were then asked to electronically sign the consent form and confirm they were aged 18+ if they wished to proceed.

2. **Demographics:** We asked our participants to indicate their age, gender, education, employment status, daily usage of smartphones (in hours), and the smartphone OS they used.
3. **Importance for Privacy:** Privacy preferences were captured through collecting importance for out-of-device privacy [96]. The out-of-device privacy scale captures the importance an individual attributes towards protecting their information from out-of-device threats. This contrasts online information privacy concerns captured through scales such as UIIPC [199], which specifically focus on online information. Since shoulder surfing is one of the out-of-device threats, we selected ODPS to capture users' importance of privacy.
4. **Familiarisation with Technology:** To assess users' tendency to actively engage in or avoid intensive technology interaction, we used Affinity for Technology Scale [105].
5. **Mechanism-Related Questions:** Each mechanism category was first introduced with a description and video representation of all mechanisms that fall under the mechanism

category. Participants were asked to focus on the presentation of the information in the presence of a shoulder surfer and then answer the follow-up questions. In the follow-up questions, we asked participants questions around (1) use, (2) importance, (3) protection, (4) preference for the mechanism or similar digital alternative, and (5) preference for a non-digital alternative in comparison to the presented mechanism. Each question was presented on a 7-point Likert scale (1=strongly disagree to 7=strongly agree).

6. **General Items:** In addition to mechanism-specific questions, we also asked participants questions about (1) perceived usefulness and (2) trust in privacy protection mechanisms. Each question was presented on a 7-point Likert scale (1=strongly disagree to 7=strongly agree).

6.5.2 Pilot Study

The questionnaire was first internally tested by N=7 experts with expertise in different domains under human-computer interaction. Experts provided feedback mainly around the wording of questions. Following the feedback from experts, it was then tested externally with N=10 participants recruited through Prolific. Participants were asked to report any issues related to understanding the questions or playing the videos in an open-ended question. They were also asked to indicate their browser-in-use to understand if playing the videos was an issue specific to a browser. Participants did not experience any issues in playing the videos. However, a few participants mentioned some ambiguities in the checks we had placed to ensure video watching. The questions were improved based on participants' feedback. All participants were compensated as per Prolific's recommendation. Overall, pilot testing with experts and with the target audience ensured that our study was focused on the research questions and was precisely understood by the general audience.

6.5.3 Ethical Considerations

Our study was approved by the Ethics Committee at our institute. The study started with presenting an information sheet to participants detailing the study's aim, data collection, data usage, and data protection. We then presented them with a consent form to electronically sign if they wished to proceed. Participants had to be above the age of 18 to be eligible to participate in the study. We also turned off recording all respondents' IP addresses and location data collected through Qualtrics. To preserve anonymity, we deleted the Prolific's IDs after compensating all participants. Participants were compensated £8.08 per hour for their time and participation.

6.5.4 Data Quality Checks

Online data collection brings the advantage of collecting data from a large and diverse sample. However, it also brings the challenge of ensuring good-quality data collection. For this purpose, we undertook various measures such as (1) multiple **attention checks** in the questionnaire to check if participants were paying attention. We used the following attention check:

Research shows that some participants in online studies do not pay attention. Please help us monitoring the quality of our study results by answering this question with somewhat disagree.

(2) We used **comprehension checks** to ensure that the participant had correctly understood the terminology and topic under investigation. In case of incorrect answers, participants were allowed to reread the information provided and then answer the questions again. As part of comprehension checks, participants were asked to indicate if the following statements were true or false:

(a) *Shoulder surfing refers to observing someone's device screen without permission. Please indicate if this statement is true or false.* (b) *To perform a shoulder surfing attack, one must be close to the device screen being observed. Please indicate if this statement is true or false.*

(3) To ensure that participants viewed all videos in each mechanism category, we asked **an additional question** after the videos were showcased related to the content shown in the videos. If participants answered incorrectly, they were not allowed to proceed but were asked to rewatch the videos and re-answer the questions. An example of such a question is

The above videos show examples of screen brightness for

Participants could then choose between (i) text messages only, (ii) text messages, chart visualisation, and photos, and (iii) text messages and photos based on the content shown in the videos. (4) Finally, we utilised the feature of **bot detection** provided by Qualtrics to avoid unwanted submissions.

6.6 Results

The goal of this study is to understand user Personalisation mechanisms against shoulder surfing. In this section, we present the results of user preferences for ten protection mechanism categories evaluated with a UK-based population.

6.6.1 Recruitment & Participants

We recruited N=226 participants from the UK through Prolific. Twenty-five participants' data was removed as they failed to pass the attention checks. On average, participants took 25 minutes to complete the questionnaire (sd=11.20). Participants who took less than half the average time were removed from the analysis (N=9). No submission was marked as a bot submission. Out of the remaining N=192 participants, N=93 self-identified as man, N=95 as woman, N=3 as non-binary, and one participant preferred not to say. Participants' mean age was 42.78 (sd=13.94, min=18, max=78). More than half of the participants were employed full-time (N=103), N=34 were employed part-time, and N=20 were unemployed. Fourteen participants were retired, N=9 homemakers, and N=8 were students. Most participants held a 4-year degree (N=61) or a professional degree (N=42), followed by some college (N=40). Twenty-nine participants were high school graduates, N=10 held two-year degrees, and a few (N=5) had doctorates or had education less than high school. Most participants (N=96) reported to spend between 2 and 5 hours per day interacting with smartphones. A majority of participants (N=44) spent less than 2 hours, N=33 spent between 5 and 7 and a small group (N=19) spent more than 7 hours per day interacting with smartphones. A vast majority of participants were Android smartphone users (N=113), while N=79 participants were iOS users.

6.6.2 Experience with Shoulder Surfing

More than half of the participants agreed that they had been shoulder surfed (N=113), while a large group of participants could not recall (N=57), and a small group of participants disagreed (N=22). When eliciting the specific role in a shoulder surfing situation, almost half of the participants agreed that they experienced shoulder surfing as a victim and also as an observer (N=80). Some participants shared they had shoulder-surfed someone (N=44), they were shoulder-surfed by someone (N=39), and a few participants preferred not to answer (N=29). Thirty-six participants recalled having the latest experience of shoulder surfing in the last six months, N=35 participants never had an experience, N=30 experienced in the last few days, followed by more than a year ago (N=27) and in the last three months (N=26). Twenty-three participants experienced it last month, and N=15 experienced it a few weeks ago. Almost all participants (N=175) held the opinion that they are responsible for protection against shoulder surfing, and a few (N=13) expressed that both the manufacturer and the user are responsible for protecting against it. Only a few participants felt that the device manufacturer was responsible for protection against shoulder surfing (N=3).

6.6.3 Perceptions of Protection Mechanisms

Overall Perception: Overall, our participants slightly agreed that the mechanisms would help in protecting their privacy (protection.median= 5, st dev=1.66, mean=4.34), but they also held

the opinion that they would prefer having non-digital alternatives than the presented mechanisms (alternate.median= 5, st dev=1.64, mean=4.76). When enquired about if participants would use the mechanism, would like to have it installed on their phone, or if not installed, then they would install it or look for an alternate, participants slightly disagreed (availability.median = 3, st dev =1.78, mean=3.26). Participants held similar views regarding whether they would like to use the protection mechanisms (use.median=3, st dev=1.82, mean=3.5) and if it's important for them to have the mechanism installed on their devices (own.median=3, st dev=1.74, mean=3.35).

When comparing individual mechanisms, our participants somewhat agreed that they would prefer non-digital alternatives to all the presented mechanisms, such as covering the screen using their hands (alternate.median= 5). Participants disagreed or somewhat agreed with installing the mechanism on their phones if not installed by default for all mechanisms except haptic and icon overlay, where participants were found to be neutral (availability.median = 4). Similar views were seen when asked if participants would prefer installing the mechanism and working on their devices. Most mechanisms were not favoured, and participants disagreed or somewhat disagreed except for icon overlay and haptic, where participants were found to be neutral (own.median = 4). Participants expressed agreement for using icon overlay to protect their privacy (use.median=5), whereas they were found to be neutral for tangible and haptic (own.median=4) and disagreed for all the rest of the mechanisms (use.median=3-2).

Similarities & Differences between Mechanisms: We next analysed the distance between mechanisms to see if mechanisms were perceived as similar or different. For this, we calculated Euclidean distance (d) between all mechanisms' mean responses. The smallest distance ($d=11.221$) was seen between replacement by meaningful text and combination mechanisms. Similarly, smaller distances were observed between distortion, selective visibility, replacement by meaningful text, replacement by protective text, and combination ($12.207 < d < 12.787$). On the contrary, the largest distance was observed between display colour change and icon overlay ($d=22.631$). Distances close to each other indicate that mechanisms were perceived similarly, whereas larger distances indicate that the perception of mechanisms differed greatly. Table 6.4 presents the detailed results.

6.6.4 Ranking of Mechanisms

Figure 6.2 shows participants' ranking of the ten mechanism categories. Icon overlay was most favoured (median=4), followed by haptic, physical tangible, and screen brightness (median=5). All remaining mechanisms, including baseline (i.e. no protection mechanisms), were least preferred by participants ($6 < \text{median} < 7$). A Friedman test found significant differences between the ranking of mechanisms ($\chi^2(10) = 102.063, p < 0.001$). Pairwise comparisons were performed with a Bonferroni correction for multiple comparisons. Rankings were statistically significant between different mechanisms. Post hoc analysis revealed significant differences between (1) icon overlay and distortion, selective visibility, combination, display color change, re-

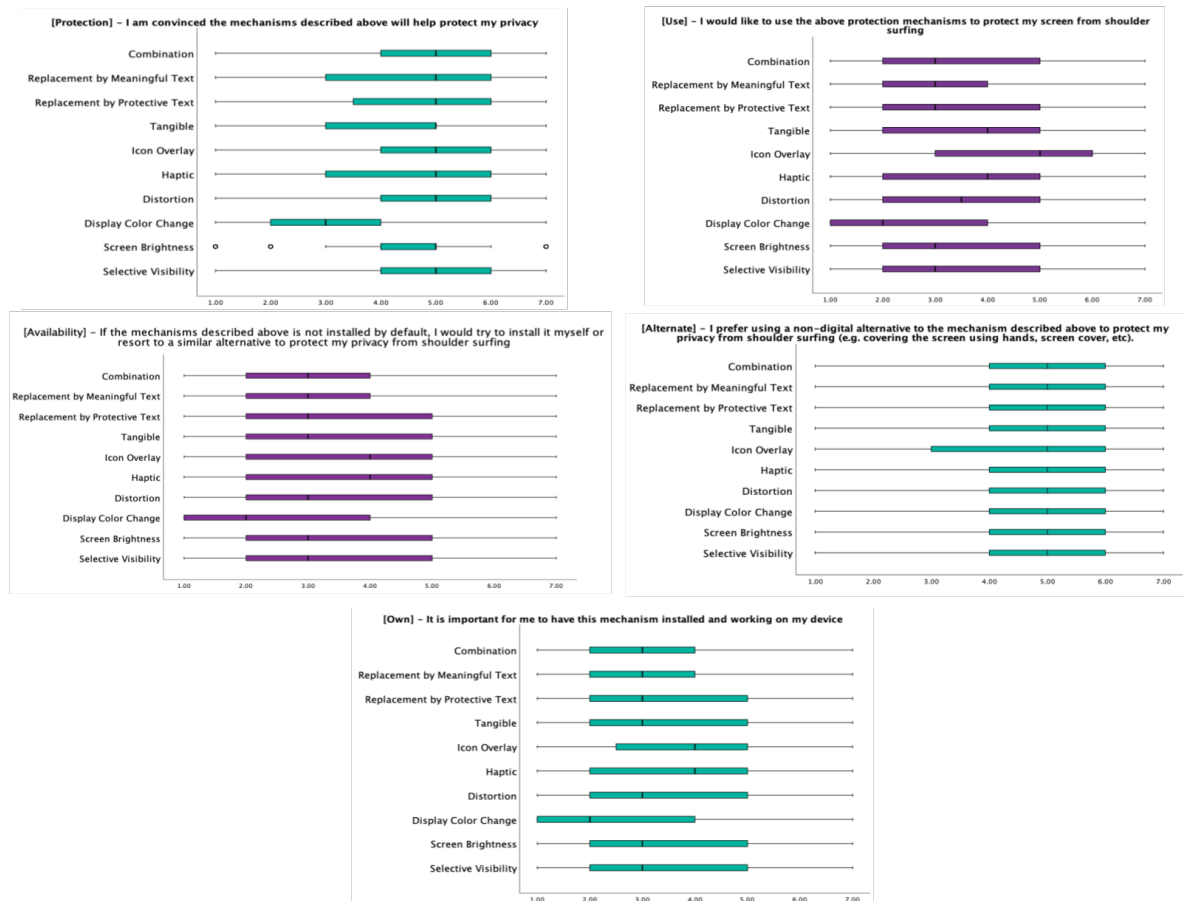


Figure 6.1: The Figure shows participants’ feedback on each protection mechanism category. Participants could select from a 7-point Likert scale ranging from strongly disagree (1) to strongly agree (7).

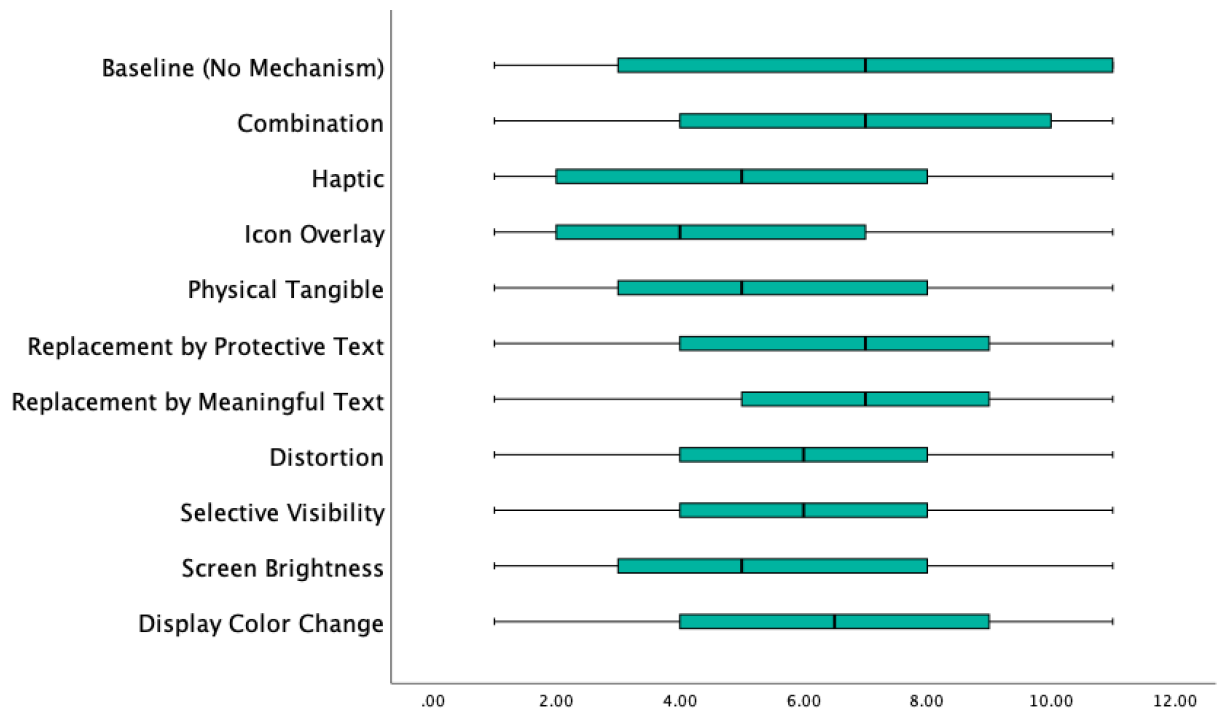


Figure 6.2: The figure shows the ranking of protection mechanism categories.

placement by protective text, replacement by meaningful text, and baseline (no protection), (2) physical tangible and replacement by meaningful text and baseline (no protection), (3) haptic and combination, display colour change, replacement by protective text, replacement by meaningful text and baseline (no protection), and (4) icon overlay and distortion, selective visibility, combination, display color change, replacement by protective text, replacement by meaningful text and baseline (no protection).

6.6.5 General Perception of Mechanisms

After assessing the presented mechanisms, we looked into the overall perception of protection mechanisms by asking questions about (1) Personalisation and (2) Perceived Usefulness.

Participants agreed that an understanding of these mechanisms to protect their privacy was easy (median=6). Participants also somewhat agreed (median =5) that protecting text and photos from shoulder surfing was important to them. They also felt that they would be more comfortable using their smartphones in public if the mechanisms were installed on their phones, which would help safeguard their privacy (median =5). Participants also expressed trust in mechanisms for protecting their privacy, and having access to mechanisms would make them consider more about their privacy and be aware of their surroundings (median =5). They would prefer having mechanisms on their phone rather than none, and the presented mechanisms better protect their privacy than purely non-digital alternatives such as covering my hands (median =5). Participants also felt that having a mechanism that only alerts them about shoulder surfing is sufficient for them (median =5). Participants were found to be neutral that the mechanism must convey

Statements	Median	Mean	Standard Deviation
Protecting text and photos from shoulder surfing is important to me.	5	4.62	1.63
I would feel more comfortable using my smartphone in public if it has privacy protection mechanisms.	5	4.61	1.62
Having protection mechanisms will safeguard my privacy.	5	5.20	1.32
Understanding how these mechanisms protect my privacy is easy.	6	5.53	1.28
I trust the presented mechanisms to protect my privacy from shoulder surfing.	5	4.55	1.43
Having these mechanisms makes me aware of my surroundings	5	5.11	1.26
Having access to the mechanisms described above makes me consider using them to protect my privacy.	5	4.62	1.68
I prefer using the presented mechanisms rather than having none to protect my device from shoulder surfing.	5	4.37	1.73
The presented privacy mechanisms better protect my privacy from shoulder surfing than non-digital alternatives, such as covering the screen using my hands or screen cover.	5	4.51	1.57
Having a mechanism that only alerts me about shoulder surfing is sufficient for me.	5	4.89	1.38
The protection mechanism must convey irrelevant information (such as random unmeaningful text) to the observer to let them know they have invaded my personal space.	4	3.91	1.62
A protection mechanism that covers the entire display is suitable for me.	4	4.09	1.61
The protection mechanism should tell about who the observer is as well.	4	3.80	1.50
The observer should not know that I have a protection mechanism.	4	4.29	1.68

Table 6.3: The Table shows the overall perception of protection mechanisms (general)

irrelevant information to the observer to let them know they have invaded their personal space (median =4). Furthermore, they also held a neutral opinion that the protection mechanism should tell about who the observer is, but simultaneously, the mechanism should not let the observer know that the user has a mechanism activated on their phones (median =4). Lastly, participants were also neutral on having a mechanism that covers the entire display (median =4). Table 6.3 shows the descriptive results for participants' perspectives on general mechanisms.

We then conducted a principal component analysis to determine if multiple privacy items are related to the same factors. A principle component analysis with oblique promax rotation resulted in three factors, one of which had only two items loaded onto it. A visual inspection

	Selective Visibility	Screen Brightness	Display Color Change	Distortion	Haptic	Icon Overlay	Tangible	Rep. by Protective Text	Rep. by Meaningful Text
Screen Brightness	14.78								
Display Color Change	15.949	16.664							
Distortion	12.787	14.72	16.773						
Haptic	16.506	19.256	20.254	15.729					
Icon Overlay	17.084	18.753	22.631	16.465	14.319				
Tangible	16.302	18.654	19.406	17.128	15.191	14.564			
Rep. by Protective Text	15.039	17.678	19.507	14.165	16.034	16.2	17.401		
Rep. by Meaningful Text	14.22	16.072	15.687	12.549	16.08	16.62	15.78	12.311	
Combination	13.022	14.969	16.731	12.207	15.623	16.204	15.473	13.492	11.221

Table 6.4: Distances between Mechanisms indicating similarities and differences

of the scree plot also suggested factors between two or three. Before finalising the solution, we calculated reliability using Cronbach's alpha, which resulted in poor reliability for the third factor (which had only two items). Further, considering the best principles and recommendations around dimension reduction, we explored two-factor solutions. The two-factor solution resulted in an improved, simple solution. We then again checked for reliability, and in the case of a two-factor solution, appreciable reliability was achieved for both factors (> 0.70). We named the factors "Perceived Usefulness" ($\alpha = 0.797$) and "Personalisation" ($\alpha = 0.876$). Perceived usefulness represents if users do prefer having the mechanism to protect from shoulder surfing. Next to determining if the participants want a mechanism, the component "Personalisation" captures how the user wants the mechanism to be that is tailored to their preferred personalisation.

Table 6.5 presents the results of the two-factor solution of principle component analysis.

6.6.6 Correlation between Personal Attributes & Perception of Protection Mechanisms

Out-of-Device Privacy Scale: First, we analysed the reliability of Out-of-Device Privacy Scale which resulted in optimum reliability ($\alpha = 0.918$). Next, we analysed the link between ODPS and components of protection mechanisms. There was a strong positive association between ODPS and Personalisation, which was statistically significant ($\tau = 0.549$, $p < 0.001$). ODPS had a weak positive association with Perceived Usefulness, which was statistically significant ($\tau = 0.300$, $p < 0.001$).

Affinity for Technology Interaction: Acceptable internal consistency was observed across the dataset of Affinity for Technology Interaction scale ($\alpha = 0.891$). There was a strong positive correlation between Personalisation and ATI ($\tau = 0.105$, $p = 0.037$), but a weak association was observed with Perceived Usefulness which was not found to be statistically significant ($\tau = .109$, $p = 0.032$). This shows that users with high ATI scores prefer mechanisms that raise Personalisation, but the ATI score does not impact Perceived Usefulness.

Age: All participants shared a similar out-of-device privacy scale (ODPS) score regardless of the age group. Participants between the ages of 18 and 30 had a median score of 5.11 for Out-of-Device Privacy; participants between the ages of 31 and 60 also had a median score of 5.11, and participants between the ages of 61 and 78 had a median score of 5.17. Next, we calculated Kendall's tau correlation to test the relationship between ODPS and age. The results showed a weak correlation ($\tau = 0.028$) but were not found to be significant ($p = 0.566$). We next compared age with Personalisation ($\tau = 0.030$, $p = 0.545$) and Perceived Usefulness ($\tau = -0.037$, $p = 0.457$) but did not observe significant differences. This shows that age does not play a part in forming preferences for protection mechanisms and neither in the level of concern for out-of-device privacy.

Gender: Table 6.6 presents a descriptive summary of participants' perceptions of general privacy mechanisms. The mean responses for both components of general privacy mechanisms

		Loadings	
Percieved Usefulness	Having a mechanism that only alerts me about shoulder surfing is sufficient for me	-0.708	0.847
	Having protection mechanisms will safeguard my privacy		0.809
	Understanding how these mechanisms protect my privacy is easy		0.78
	I trust the presented mechanisms to protect my privacy from shoulder surfing		0.717
	Having these mechanisms makes me aware of my surroundings		0.609
	The presented privacy mechanisms better protect my privacy from shoulder surfing than non-digital alternatives, such as covering the screen using my hands or screen cover	0.415	0.426
Personalisation	The protection mechanism must convey irrelevant information (such as random unmeaningful text) to the observer to let them know they have invaded my personal space.	0.763	
	Protecting text and photos from shoulder surfing is important to me.	0.711	
	A protection mechanism that covers the entire display is suitable for me.	0.709	
	I prefer using the presented mechanisms rather than having none to protect my device from shoulder surfing.	0.681	
	I would feel more comfortable using my smartphone in public if it has privacy protection mechanisms.	0.678	
	The protection mechanism should tell about who the observer is as well.	0.617	
	Having access to the mechanisms described above makes me consider using them to protect my privacy.	0.549	0.431
	The observer should not know that I have a protection mechanism.		

Table 6.5: The Table shows the result of the Principle Component Analysis representing components structure. The statement highlighted in red was removed as it did not load sufficiently high (> 0.30).

		Personalisation			Perceived Usefulness		
gender	n	mean	st dev	median	mean	st dev	median
man	93	4.16	1.27	4.14	4.94	1.01	5.17
woman	95	4.43	1.19	4.43	4.99	0.94	5
prefer not to say	1	4.71	-	-	5.5	-	-
non-binary	3	3.38	1.39	3.71	4.78	1.17	4.67

Table 6.6: The Table shows Participants’ perception of general privacy mechanisms in relation to their gender.

were found to be close between male and female subsets. We compared the subset of male and female responses for the two components of general privacy mechanisms. We found Kendal Tau’s correlation for Personalisation ($\tau = 0.020$, $p = 0.782$) and for Perceived Usefulness ($\tau = 0.036$, $p = 0.630$). None of the correlations was found to be significant. This shows that there are no differences in preferences among users based on gender.

Device Operating System: Among our sample, $N=79$ participants were iOS users, while most were Android users ($N=113$). We then assessed the relationship between the use of smart-phone OS and components of general privacy protection mechanisms. We observed a negative association between iOS and Android users for Personalisation, but it was not found to be significant ($\tau = -0.030$, $p = .702$). On the contrary, no correlation was found between Android and iOS users for Perceived Usefulness ($\tau = 0$, $p=.997$).

6.7 Discussion

Our goal was to assess the role of personal attributes in forming preferences for privacy protection mechanisms against shoulder surfing. In this section, we discuss key takeaways based on the results and propose future work directions.

6.7.1 Privacy Mechanisms for General Population


Overall, our participants agreed that the presented mechanisms would offer protection, but they also expressed that they would prefer non-digital alternatives as opposed to device-based mechanisms. Participants also shared that they would not go out of their way to have the mechanism installed on their devices except for icon overlay or haptics. This shows that mechanisms should be available by default, and the user should not have to search or install mechanisms. Holistically, users perceived the understanding of how the protection mechanisms functioned as easy. Despite the easy understanding of the mechanisms’ functionality, participants generally favoured icon overlay, haptic, and tangible mechanisms among all mechanisms. Echoing previous work, this finding shows that participants are more inclined towards alerting and un-

obtrusive mechanisms than mitigation mechanisms [91, 94]. This indicates that future design of protection mechanisms should consider mechanisms similar to icon overlay, haptics, or tangible mechanisms.

6.7.2 Key Takeaways

-  **Design Equity regardless of Smartphone OS:** Android and iOS are the two popular operating systems with different ecosystems. Research on privacy concerns of iOS and Android users reveals that none of the architectures is a winner regarding privacy [171]. Similar to other privacy concerns, we did not observe differences between iOS and Android users for perceived usefulness and personalisation of protection mechanisms against shoulder surfing. Based on this, designers can develop mechanisms without considering the smartphone OS specifications or target audience.
-  **Age-Independent Mechanisms:** Level of privacy concerns change as we move across different age groups, for example, young adults are often seen as engaging more in privacy-protective behaviours while older adults are seen as concerned for other individuals [153]. However, in our study, we observed that age does not play a part in forming preferences for perceived usefulness and personalisation of mechanisms. This shows that while designing mechanisms, age does not play the role of a confounding variable.
-  **User-Tailored Privacy:** Our results showed a positive and significant correlation between the Out-of-Device Privacy score and perceived usefulness and personalisation. This shows that researchers should incorporate user-tailored privacy, which recommends analysing user privacy profiles and then recommending privacy solutions. This finding echoes prior work that advocates for user-tailored privacy [168, 169].
-  **Increased Personalisation with Increased Affinity for Technology Interaction:** In our study, users that had a high tendency to engage with technology-preferred mechanisms preferred personalization of mechanisms [105]. This shows that tech-savvy users prefer mechanisms that they can adjust and modify according to their preferences. This trend is also seen in tangible privacy research that provides evidence that users with a high affinity for technology interaction prefer tangible mechanisms [73].
-  **Importance of the Out-of-Device Privacy:** Users with high ODPS scores preferred usefulness and personalisation of privacy protection and vice versa. This shows that peo-

ple who are highly concerned about their out-of-device privacy would need privacy protection more than people with low importance for out-of-device privacy [96]. This finding resonates with profiling users based on their privacy profiles [202].

-  **Designing Discrete Mechanisms:** Among all mechanism categories presented to participants, participants favoured discreet mechanisms the most especially icon overlay followed by haptic and tangible. This aligns with previous work that reported that users prefer unobtrusive and alerting mechanisms [91, 94].

6.7.3 Future Work

In this paper, we explored how personal attributes such as gender, affinity for technology, or importance for out-of-device threats impact user preferences for protection mechanisms against shoulder surfing. The next step in this direction invites researchers to validate the relationship findings by running studies in the wild. Running studies in the wild would also help to overcome the potential presence of privacy paradox in users' responses. Further, the results of our study showed that overall, participants mainly preferred icon overlay, haptic, and tangible mechanisms. Considering users' preferences, another future research direction is to explore how the current design of icon overlay, haptic, and tangible can be improved to offer an improved privacy experience. Some interesting research directions to explore include what information can be conveyed to the user about the bystander through these mechanisms and how these mechanisms impact user experience. For example, in the case of haptics, the vibration pattern has to be different from the standard vibration pattern so that the user can distinguish between general notifications and bystander alert notifications. This becomes more complicated when users have customised vibrations for different notification types. In such cases, it can be hard for the user to keep track and remain aware of which vibration format conveys that information. In the case of tangible mechanisms, this mechanism category can be further expanded by including phone accessories (for example, phone covers) as bystander alert mechanisms. Prior work has investigated using tangible items for authentication and shown promising results [201]; exploring phone accessories as tangible mechanisms for communicating with bystanders might reveal interesting results as well.

6.8 Conclusion

In this paper, we aimed to explore correlations between personal attributes and preferences for protection mechanisms against content-based shoulder surfing. For this, we first identified existing protection mechanisms through a systematic literature review. We then categorised them based on design similarities. We then presented the mechanism categories to 192 participants

and inquired about their preferences. Our results showed that users agree that the presented mechanisms assist in protecting their privacy but they would prefer using non-digital alternatives such as using the hand to cover the screen. Moreover, among the mechanisms, participants mainly preferred icon overlay. We also found that no significant differences exist in preferences between male and female iOS and Android users. Based on the results, we present design guidelines to support the design of future protection mechanisms.

VII

Chapter 7

Final Reflections

"Great things are not done by impulse, but by a series of small things brought together."

— Vincent Van Gogh

This thesis made the following statement at the beginning of Chapter 1:

This thesis develops an understanding of shoulder surfing - an everyday life privacy violation and presents a user-centred approach to safeguard users' privacy from shoulder surfing. Categorising users to offer personalised experiences while understanding the needs of specific user groups is a well-established approach in the literature. This thesis presents a novel psychometric scale instrument to cluster users based on their privacy profiles and the importance of protection against out-of-device threats. It first categorises social engineering and side channel attacks on mobile devices based on attack resources. Using the categorisation, it identifies shoulder surfing as a novice attack that exclusively relies on human capabilities, manual tools, and basic hardware tools. Then, an exploration study of shoulder surfing in users' daily lives is conducted. It then highlights the need to address shoulder surfing by conducting an assessment of the impact of shoulder surfing through the eyes of the victims. This thesis proposes and develops a scientific instrument based on empirical investigations to cluster users based on their privacy profiles. This thesis concludes with investigations on exploring correlations between users' personal attributes and preferences for privacy protections against shoulder surfing, exploring correlations to inform the design of protection mechanisms.

In the previous chapters (Chapters 2-6), research work was presented to answer the five Research Questions. Each of the research questions was answered in the individual chapters. Table 7.1 provides an overview of where each RQ is answered.

RQ #	Research Question Statement	Chapter #	Thesis Section	Publication #
RQ1	Where does shoulder surfing fit in the ecosystem of social engineering and side channel attacks?	2	Section 2.6	1
RQ2	How is a user's privacy violated through shoulder surfing in the real world on a day-to-day basis?	3	Section 3.5	2
RQ3	How does shoulder surfing impact victims' social and device interaction?	4	Section 4.4	3
RQ4	How can we measure users' privacy perceptions in the context of shoulder surfing?	5	Section 5.5	4
RQ5	How can the design of technical protections against shoulder surfing be informed to reflect users' privacy profiles?	6	Section 6.7.2	5

Table 7.1: An Overview of Research Questions answered individually in each chapter.

7.1 Reflecting on the Findings

Among the plethora of social engineering and side-channel attacks, shoulder surfing is a "novice attack" that does not require sophisticated setup or expert resources to invade a user's privacy. Shoulder surfing only requires being close in distance to the victim user and utilising the human capability of making observations to uncover the device content. Due to the low-effort requirement of shoulder surfing, it can be easily executed on a large scale. Further, because shoulder surfing does not require any sophisticated setup and expertise, it can happen anywhere – public or private environments – by anyone – known or unknown. However, shoulder surfing is frequently experienced in public transport, and smartphones are the most shoulder-surfed devices. It can reveal authentication-based information (such as PINs or passwords) and content-based information (such as text messages or photos), while content-based shoulder surfing is more frequently reported. While we have advanced mechanisms for protecting PINs and passwords, such as biometrics, device content, such as text and photos, are still vulnerable to shoulder surfing.

The findings of this thesis present evidence that shoulder surfing impacts different victim users differently and is seen as unavoidable and frequently occurring. Moreover, shoulder surfing is seen as the stepping stone to other threats, such as identity or device theft. This makes shoulder surfing a further serious concern as it does not stop the harm on one level, but is also seen as leading to more harm. This makes addressing and mitigating shoulder surfing highly critical. To protect privacy against shoulder surfing, users are willing to use software-based mechanisms; however, the pre-conditions such as effectiveness, reliability, availability, and financial cost are among the various consideration factors voiced by users. These factors show that designing a mechanism alone is insufficient; researchers should also consider other factors that may impact users' willingness to use a protection mechanism. Along with the mechanism, researchers must also think about communicating its efficacy, reliability, and financial cost to users. Consideration of these factors also means that users may again be divided into different groups based on what they perceive as acceptable vs not.

Since the impact and perception of shoulder surfing are highly individual, a psychometric scale instrument is a valuable contribution to scientific knowledge that helps to group users based on their privacy profiles. This is necessary to offer users a personalised, privacy-protected experience against shoulder surfing. Using the scale in combination with users' personal attributes such as age, we explore correlations between personal attributes of users and preferences for protection mechanisms to assist in uncovering how user's personal profile, which includes age, smartphone OS, privacy preferences, affinity with technology and similar can reflect and inform the design of protection mechanisms. Such guidelines help to design mechanisms that would suit the needs and preferences of specific user groups.

7.2 Contributions

This thesis makes five fundamental contributions: (1) conceptual, (2) empirical, (3) theoretical, (4) methodological, and (5) design guidelines. We discuss the contributions below:

7.2.1 Conceptual Contributions:

We present a categorisation of social engineering and side channel attacks based on the attack resources (chapter 2). The categorisation guide can be used to evaluate novel attacks, and in doing so, we can estimate the share of the population capable of executing a particular attack, which would indicate the ubiquity of the attack. *The categorisation is an evaluation tool for existing and novel attacks to help researchers develop effective protection solutions.*

7.2.2 Empirical Contributions:

This thesis contributes an in-depth investigation of shoulder surfing in the daily lives of users (chapter 3). Through a month-long diary study with 23 participants, we present evidence that content-based shoulder surfing, i.e. text and photos, happens more frequently than authentication-based information such as PINs or passwords. Users experience shoulder surfing in public and private environments. It most frequently occurs in public transport and during evening and nighttime. Anyone, related or unrelated, could be a shoulder surfer. Smartphones are the most shoulder-surfed devices. Moreover, shoulder surfing is not only seen as a privacy invasion but is also perceived as wasting the victim's device interaction time. *On the whole, empirical findings inform security and privacy researchers of the potential frequently occurring locations and contexts of shoulder surfing where users' privacy is likely to be violated.*

7.2.3 Theoretical Contributions:

After discovering the occurrences of shoulder surfing, in Chapter 4, we present a microscopic view of the impact of shoulder surfing on victims of shoulder surfing towards privacy perceptions

and willingness to use smartphones and their social interaction. The research bridges the gap between investigations of episodes of shoulder surfing in the wild and the need for privacy protection methods. Our findings show that the perception of shoulder surfing differs from one user to another. Moreover, shoulder surfing is seen as unavoidable and frequently occurring, leading to increased time for task completion. Users are concerned not only for their own privacy but also for other people's privacy, whose content is seen by the shoulder surfers. Shoulder surfing is not only seen as revealing personal information to others without consent, but it is also seen as leading to other more serious threats, such as identity or device theft. While users are willing to use software-based protection mechanisms for protection against shoulder surfing, this comes with user-defined criteria, such as effectiveness, affordability, reliability, and availability. *Overall, the results make a theoretical contribution by providing evidence on how users differ in their perception towards shoulder surfing.* Based on the findings, we reflect and provide future work directions to address the challenges in mitigating the negative impact of shoulder surfing on diverse users, including vulnerable user groups such as children.

7.2.4 Methodological Contributions:

In Chapter 5, we first identify and highlight the need for a method to cluster users based on their privacy profiles concerning out-of-device threats. To this end, based on multiple studies, we propose an Out-of-Device Privacy Scale (ODPS) to capture users' importance in protecting their information from out-of-device threats such as shoulder surfing. *The Out-of-Device Privacy scale provides a methodology for clustering users based on their privacy profiles.*

7.2.5 Design Guidelines Contributions:

In Chapter 6, *we present design* guidelines for developing protection mechanisms against shoulder surfing following users' personal attributes. The design guidelines assist researchers and developers in paving the way towards offering a personalised privacy experience to users against shoulder surfing.

7.3 Pathways for Continued Exploration

Research is a journey that always continues. In this thesis, we present (1) a thorough investigation of shoulder surfing from literature and users' daily lives, (2) explore the impact of shoulder surfing, (3) propose a user-centred method for mitigating shoulder surfing, and (5) recommend design guidelines for developing protection mechanisms based on users' personal attributes. The succeeding steps in advancing the knowledge around shoulder surfing are:

7.3.1 Beyond W.E.I.R.D. Populations

The research presented in this thesis collected data from participants residing in the W.E.I.R.D. (Western, Educated, Industrialized, Rich and Democratic) contexts [129, 190]. For example, in Chapter 2, we collected data from Australia, New Zealand, and the UK in Chapters 3, 4, and 5. Prior work has also primarily focused on the investigation of shoulder surfing in W.E.I.R.D. contexts, for example, Marques et al. [203], and Muslukhov et al. [214] conducted studies on unauthorized access of devices, which is a vector of shoulder surfing, and had participants from Europe, the US, and Canada. Saad et al. [249] investigated shoulder surfing in public transport and had participants from Germany. Eiband et al. [85] investigated Germany, the US, and Egypt, but only 16% of the participants belonged to Egypt. Only the work by Saleh et al. [252] looked into occurrences of shoulder surfing with participants from Saudi Arabia, Egypt, and Germany and provided evidence that shoulder surfing can have far more serious consequences in low socio-economic groups, potentially leading to defamation and severely compromising familial reputation. An overview of the investigations around shoulder surfing shows that most work has been focused on W.E.I.R.D. countries. However, there are differences between literacy rates, mobile users, and income as we move from W.E.I.R.D. to non-W.E.I.R.D. countries, which may bring differences in privacy perceptions and attitudes. Cultural, religious, and familial differences may impact how shoulder surfing is seen and impacted, like other privacy perceptions, behaviours, and beliefs [218]. Furthermore, mobile ownership has increased significantly in the last few years in the global South [54], making addressing shoulder surfing even more crucial.

Future Research Direction



How do users experience, perceive, and are impacted by shoulder surfing across different cultures?

7.3.2 Inclusive Security & Privacy Practices

Developing equitable and privacy-protection technology has acquired urgency in HCI. The needs of marginalised groups, such as victims of intimate partner abuse or people with disabilities, are often ignored in the process of designing technology due to the social and privacy concerns of such groups [254]. Shoulder surfing is a concern which can escalate to huge problems, especially for marginalised groups. For example, victims of intimate partner abuse can face serious consequences if their partner's shoulder surfs them. Therefore, the needs of such groups must be considered and addressed to move forward and acquire equitable privacy for all.

Future Research Direction



How does shoulder surfing impact marginalised groups?

7.3.3 Evaluation of Protection Mechanisms & Need for Vigilance

Security and usability evaluations are commonly conducted when a new mechanism is proposed, as seen in the work of shoulder surfing mechanisms proposed [3, 161]. In this thesis, we found additional factors that should be evaluated to understand the willingness of users to use a mechanism. For example, in Chapter 3, participants voiced that they were interested in knowing how effective a mechanism was before using it, echoing recent work which found that the verifiability of security mechanisms is key to user sentiment [200]. This can be explored, and evidence can be provided through security evaluations. Next, participants also voiced that they would like to know how easy it is to use a mechanism and how much the mechanism interferes with the device's interaction. This is similar to the findings reported in Chapter 3, where participants were presented with various mechanisms and were asked to select the most appropriate one. Participants were seen as inclined towards unobtrusive alerting mechanisms instead of mitigating mechanisms. One of the probable reasons for the preference could be that alerting mechanisms are unobtrusive, do not cover the whole screen, and only occupy a small space on the screen display. The preconditions listed by participants show that they would like to be given a choice to select the most appropriate mechanism to use for them. This can be due to varied user preferences, which indicates that no one-size-fits-all approach can be applied. It is also recognised in prior work on interface design that the one-size-fits-all approach hardly leads to an appreciable user experience [65]. Interestingly, participants also mentioned "financial cost" and "availability" as the determining factors for using a mechanism. However, these may not apply to all mechanism types, such as device-level mechanisms like visual filters like grayscale [320] or low brightness [187, 320]. Since some of our participants were aware of privacy screen protectors, they may be referring to the availability and financial cost of tangible privacy mechanisms [7, 74, 286]. This leads to exploring tangible solutions for protection against shoulder surfing or a combination of tangible solutions with software-based solutions, as they would provide users with increased feasibility of using them as required.

Future Research Direction



How can we develop a framework for evaluating protection mechanisms?

7.3.4 Unconcerned Users or Vulnerable Users?

In Chapter 3, we observed that a small group of participants were unconcerned and not impacted by shoulder surfing. This is similar to the findings by Harbach et al. [127] that reported that users are aware of shoulder surfing as a privacy threat but are not much bothered. However, just because users do not perceive shoulder surfing as a threat, it does not qualify as a non-threat. The differences in opinions on perceiving shoulder surfing reflect the differences in users' profiles in the same way that users vary in general privacy profiles. On the contrary, this also invites investigation into whether unconcerned users are the most vulnerable.

Future Research Direction



To what extent does being unconcerned put the user on the edge of attack vulnerability?

7.3.5 Roleplay of Privacy Paradox

In this thesis, we collected data from participants through self-reporting. For example, in Chapter 3, we asked participants to report their experiences of shoulder surfing through a diary study. Then, in Chapter 4, we asked participants for their perspectives and opinions on the impact of shoulder surfing. Similarly, in Chapter 5 and 6, we collected data where participants self-expressed their perspectives, preferences, and behaviours. Through the user reports, we extracted meaningful data and translated it into research findings. However, the privacy paradox [109, 170] might come into play when users practically use mechanisms in their daily lives. Therefore, we propose future work to look into navigating through the privacy paradox.

Future Research Direction



What role does privacy paradox play in the reporting and adoption of shoulder surfing protection mechanisms?

7.3.6 Creating Contextual Privacy Settings

As seen in Chapter 3, shoulder surfing happens in public and private environments, and the dynamics of relationships and content type under observation play a role in establishing if and what sort of protection mechanism users prefer. Prior work also presents evidence that users consider their relationship with the observer when determining the type of mechanism [91], and the perceived privacy for each content type is different [93]. While these findings imply that the

user-observer relationship and content type play a role, they also imply that the overall context plays a role. Therefore, future work on developing protection mechanisms must look into supporting the multidimensional nature of privacy.

Future Research Direction



How can contextual privacy settings be included in the design of protection mechanisms?

7.3.7 Remote vs In-Person Data Collection

In this thesis, the data was collected remotely and advertised through Prolific or social media platforms. While in-person studies can elicit more details and present the opportunity for follow-up questions, remote data collection allowed us to reach a broader group of participants with diverse demographics. Furthermore, the users recruited through online methods are accustomed to working with tech and are better informed than the average user. This puts them in a better position to be aware of potential threats and possible countermeasures.

Future Research Direction



How do the empirical findings collected through remote methods translate into empirical findings collected through in-person methods?

VIII

Chapter 8

Conclusion

"We are all apprentices in a craft where no one ever becomes a master."

— Ernest Hemingway

Research evolves with time, and there is always more to do. In this thesis, we look into everyday life privacy violations, specifically shoulder surfing. We first developed an understanding of shoulder surfing through literature-based evidence and user experiences in the wild. Based on the understanding of shoulder surfing, we then propose and present a user-centred methodology to inform the design of protection mechanisms. Overall, based on data collected from N=2632 participants, this thesis develops an in-depth understanding of shoulder surfing and proposes a user-centred methodology to inform the design of protection mechanisms. This thesis concludes by drawing a discussion on future work directions.

Appendix A

A.1 Papers Included in the Systematic Literature Review

Table A.1: The Table shows the list of papers extracted from the selected publication venues which are included in the systematic literature review.

Papers Included in the Categorisation (I)	Reference
Main Search List	
Undermining User Privacy on Mobile Devices Using AI	[121]
Charging Me and I Know Your Secrets!: Towards Juice Filming Attacks on Smartphones	[210]
Boosting the Guessing Attack Performance on Android Lock Patterns with Smudge Attacks	[47]
Find me a safe zone: A countermeasure for channel state information based attacks	[313]
EvoPass: Evolvable graphical password against shoulder-surfing attacks	[311]
Smartphone speech privacy concerns from side-channel attacks on facial biomechanics	[116]
Inferring User Routes and Locations Using Zero-Permission Mobile Sensors	[217]
MISSILE: A System of Mobile Inertial Sensor-Based Sensitive Indoor Location Eavesdropping	[319]
Stealing Passwords by Observing Hands Movement	[264]
We Can Track You if You Take the Metro: Tracking Metro Riders Using Accelerometers on Smartphones	[138]
Peeking into your app without actually seeing it: {UI} state inference and novel android attacks	[53]
Armageddon: Cache attacks on mobile devices	[191]
Security analysis of Unified Payments Interface and payment apps in India	[176]
A Stealthy Location Identification Attack Exploiting Carrier Aggregation in Cellular Networks	[179]
Cashtags: Prevent leaking sensitive information through screen display	[211]
A closer look at recognition-based graphical passwords on mobile devices	[82]
An empirical study of wireless carrier authentication for SIM swaps	[183]
Hit by the Bus: QoS Degradation Attack on Android	[142]
ProcHarvester: Fully Automated Analysis of Procs Side-Channel Leaks on Android	[276]
WaveSpy: Remote and Through-wall Screen Attack via mmWave Sensing	[186]

Table A.2: The Table shows the list of papers extracted by performing Backward Search which are included in the systematic literature review.

Papers Included in the Categorisation (II)	Reference
Backward Search List	
Practical memory deduplication attacks in sandboxed javascript	[118]
Memento: Learning secrets from process footprints	[145]
Scandroid: Automated side-channel analysis of android apis	[277]
Os-level side channels without procs: Exploring cross-app information leakage on ios	[317]
Accessory: password inference using accelerometers on smartphones	[230]
A pilot study on the security of pattern screen-lock methods and soft side channel attacks	[18]
When CSI meets public wifi: Inferring your mobile phone password via wifi signals	[185]
Cracking android pattern lock in five attempts	[309]
Blind recognition of touched keys on mobile devices	[312]
Privacy leakage in mobile sensing: your unlock passwords can be leaked through wireless hotspot functionality	[314]
Routedetector: Sensor-based positioning system that exploits spatio-temporal regularity of human mobility	[299]
Mobile social networking under side-channel attacks: Practical security challenges	[225]
Smartphone passcode prediction	[56]
iSpy: Automatic reconstruction of typed input from compromising reflections	[240]
Pin skimmer: Inferring pins through the camera and microphone	[265]
Niffler: A contextaware and user-independent side-channel attack system for password inference	[284]
Single-stroke language-agnostic keylogging using stereo-microphones and domain specific machine learning	[216]
PIN Skimming: Exploiting the Ambient-Light Sensor in Mobile Devices	[274]
What the App is That? Deception and Countermeasures in the Android User Interface	[29]
Don't Interrupt Me While I Type: Inferring Text Entered Through Gesture Typing on Android Keyboards	[266]
Exploiting Data-Usage Statistics for Website Fingerprinting Attacks on Android	[275]
A Study on Power Side Channels on Mobile Devices	[307]
Return-Oriented Flush- Reload Side Channels on ARM and Their Implications for Android Devices	[318]

Table A.3: The Table shows the list of papers extracted by performing Forward Search which are included in the systematic literature review.

Papers Included in the Categorisation (III)	Reference
Forward Search List	
Deciphering text from touchscreen key taps	[123]
Exploring energy consumption of juice filming charging attack on smartphones: a pilot study	[147]
Draw it as shown: Behavioral pattern lock for mobile user authentication	[175]
Syspal: System-guided pattern locks for android	[58]
A new smart smudge attack using CNN	[263]
Inference attack in android activity based on program fingerprint	[308]
Inferring UI States of Mobile Applications Through Power Side Channel Exploitation	[122]
No pardon for the interruption: New inference attacks on android through interrupt timing analysis	[77]
MagneticSpy: Exploiting Magnetometer in Mobile Devices for Website and Application Fingerprinting	[206]
Using hover to compromise the confidentiality of user input on Android	[290]
Textlogger: inferring longer inputs on touch screen using motion sensors	[232]
Clickshield: Are you hiding something? Towards eradicating clickjacking on Android	[234]
Hidemyapp: Hiding the presence of sensitive apps on android	[231]
Gui-squatting attack: Automated generation of android phishing apps	[55]
{AttriGuard}: A practical defense against attribute inference attacks via adversarial machine learning	[146]
Resource Race Attacks on Android	[38]
What Mobile Ads Know About Mobile Users.	[272]
Grand pwning unit: Accelerating microarchitectural attacks with the GPU	[106]
Truspy: Cache side-channel information leakage from the secure world on arm devices	[315]
Schrodintext: Strong protection of sensitive textual content of mobile applications	[17]
ICAUTH: Implicit and continuous authentication when the screen is awake	[306]
Tivos: Trusted visual i/o paths for android	[101]

A.2 Codebook Used for Coding the Attack Requirements

Table A.4: The Table shows the codebook for Attack Infrastructure Requirement Categories

Category	Description	Examples
Manual Tools	Refers to non-electronic/non-powered devices or tools	Pen, box, papers, sealed box
Software Tools	programs that make use of sophisticated algorithms	Smug attack tool, n-gram Markov Model, image matching algorithm, Probabilistic Hough Transformation, Android Background Service, CSI Measurement Tool, Voice Training Data from the accomplice, VGA2USB driver, Remote Server, Probabilistic Password Model (eg n-gram Markov Model), Supervised Machine Learning Model, Model Classifier Configurations, Android Framework Services, Edge Detection Algorithm, Edge dilation, CV algorithm, open-source cellular projects. Edge Detection Algorithm, Tracking Learning Detection, Dynamic Time Wrapping, Video Editing Tool, Fine-Grained Accelerometer Data, Keypress segmentation, Probabilistic Keypress Classification, Probabilistic Error Model, Search Algorithm, Graph construction, Android NDK, ADB, CSI Measurement Tool, discrete wavelet decomposition, Threshold Quantification, Random Forest, Skin Detection Algorithm, Inverse Wavelet Transform, Dynamic Time Warping, AdSDK, Symbolic Aggregate approximation (SAX), LibSVM, exotic atomic operation loop, cache profiling tool, sticky background service, LibSVM, malloc implementation (GNU C Library), signal processing scheme, wavelet-based response analysis, Support Vector Machine (SVM), K-Nearest Neighbor (KNN), standard Android Framework services, alternate soft-keyboards, deformable part-based model (DPM), k-means clustering algorithm, APK tool, Homography, Keras, ADB shell, Tensorflow, AdSDK.
Mobile Phone Application	An application that needs to be installed on the target's mobile device	Malicious application, legitimate spyware, privileged application, Trojan application, phishing application, malware, non-malicious application
Advanced Programming	Advanced programming expertise from specialized fields of programming	Image Processing, Perspective Transform Technique, Canny Edge Detection, Hough Circle Transform, Deep Neural Network, C++/Java, Hidden Markov Model, Machine Learning, Supervised Learning Scheme, Genetic and Detection Algorithm, Pattern Matching Algorithm, Recurrent Neural Network, Neural Network Processes, Deep Learning, Weka Toolkit, Convolutional Neural Network, Python, OCR Techniques, Matlab LTE Toolkit, Computer Vision, Skin Segmentation Techniques, finger detection classifier, Supervised Learning Scheme, Support Vector Machine, OpenCV, Classifier, Language Model, regression model, classifier, Javascript, C/C++, genetic and detection algorithm, Gaussian filter, pattern matching algorithm, Recurrent neural network (RNN), Java/C language, Java-ML Library, matlab LTE toolbox, cascade classifier training, Matlab's Statistics Toolbox, sandbox app, Symlet Filter, natural language processing algorithms, signal processing techniques, scikit-learn library, kernel privileges, Return-Oriented Programming, code injection
Hardware Tools	External electronic tools required to be connected with the attack setup	VGA/USB interface, Micro USB connector, Mobile High Definition Link (MHL) standard, computer, Raspberry Pi, High-resolution camera, flash lightning system, wireless router, video recorder, Bluetooth Low Energy Beacon (BLE), Low Power Microcontroller, EspressifESP32 chip, a dual-core Tensilica Extensa LX6 processor, High Frequency Analog to Digital Converter, smartphone, USB outlet, charging cable, power bank, voltage monitor, SD card, software-defined radio device, camcorder, surveillance camera, public geographical data, a similar device as victim's, FMCW mmWave probe, frequency-modulated continuous-wave (FMCW) radar, Panasonic Lumix DMC-TZ5 compact camera, Gorilla Glass screen, USB microscope with 400x magnification, FLIR E30, hard light source, Digital Single-Lens Reflex (DSLR), laptop with Intel 5300 NIC, smart device with hotspot functionality, external sound card, Monsoon Power Monitor, smart device with hotspot functionality, Freescale i.MX53 development board running CortexA-8 processor
User Phone Permissions	Permissions requested by the attacker to access different services or sensors on the mobile device	Access to camera, microphone, accelerometer sensor, orientation sensor, internet, external storage, get_tasks, system_alert, gyroscope, magnetometer, Bluetooth, WRITE_EXTERNAL_STATE, Receive SMS, Read Phone State, GET_TASKS permissions, motion sensor
Human Capabilities	Resources within the scope of human physical and personal abilities	Close proximity with the target, direct observation, the human memory. physical access to the target device, physical walk through the target's location, context information about the victim, access to public geographical information, access to a reference image of the phone, Victim's phone number and name,

Appendix B

B.1 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)
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.

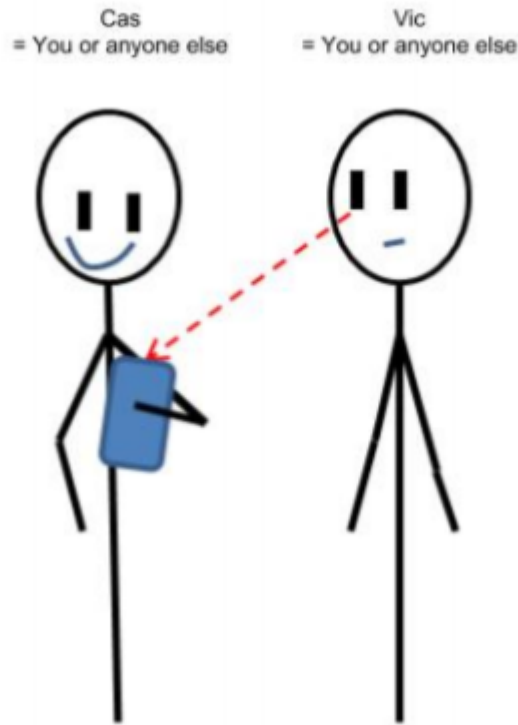


Figure B.1: (The image was taken from the work by Eiband et.al. [85] on shoulder surfing to better illustrate the meaning of shoulder surfing.)

- (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.



Figure B.2: 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

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?

B.2 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 of playing game such as "playing game"

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

Appendix C

C.1 Survey Format for the Impact Study

Shoulder Surfing refers to observing someone's device screen without permission. Shoulder surfing can happen anytime and by anyone, requiring no particular expertise or equipment but careful observation. Among all devices, smartphones are the most shoulder-surfed devices. For this reason, in this study, we focus on experiences of shoulder surfing on smartphones only. Considering this definition, please answer the following questions.

1. When did you experience shoulder surfing most recently?
 - Yesterday or today,
 - A few days ago,
 - Less than a month ago,
 - A few months ago.
2. For the statement, "I am shoulder surfed almost daily":
 - Strongly disagree
 - Somewhat disagree
 - Neither agree nor disagree
 - Somewhat agree
 - Strongly agree
3. Please describe the latest shoulder surfing experience which you experienced. Please provide as much details as possible.

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

4. For the statement: “I continue using the smartphone and accessing information in the same setting where I experienced shoulder surfing”, you:

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

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

5. For the statement: “The shoulder surfing experience affected my perceptions towards my privacy”, you:

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

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

6. For the statement, “ If someone sees my friend’s content on my screen (e.g., a picture or a message of my friend), it feels like a breach of my friend’s trust in me to keep their content private”, you:

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

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

7. For the statement: “Experiencing shoulder surfing prevented me or slowed me down from what I wanted to do on the device”, you:

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

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

8. For the statement: “Experiencing shoulder surfing impacted negatively the way I use my device”, you:

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

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

9. For the statement: “Experiencing shoulder surfing impacted positively the way I use my device”, you:

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

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

10. List your three biggest concerns around shoulder surfing. Please provide as much details as possible.
11. Are you aware of any technology or security features that can help prevent or mitigate shoulder surfing? Please provide as much details as possible.

12. Have you received any education or training on protecting yourself from shoulder surfing, personally or through your workplace or educational institution? Please provide as much details as possible.
13. Have you used additional privacy protection measures to protect your privacy from shoulder surfing? Please provide as many details as possible.
14. For the statement: "I would use additional privacy measures or tools to prevent shoulder surfing incidents", you:
 - Strongly disagree
 - Somewhat disagree
 - Neither agree nor disagree
 - Somewhat agree
 - Strongly agree

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

C.2 Codebook for the Impact Study

In this section, we provide the codebook used to analyse the questionnaire responses.

Code	Description
shoulder_surfing_by_child	referring to a child
context_specific	factors of situational information
frequent_shoulder_surfing	describing the frequency of shoulder surfing
location_specific_concern	describing concerns that are specific to a certain location
need_of_privacy	information that conveys the need for privacy
negative_feelings	words that describe unfavourable emotions
no_effect	phrases that describe no effect
privacy_invasion	phrases that describe a violation of privacy or personal space
rethinking_accessing_of_information	phrases that describe where participants had to reconsider about accessing information
shoulder_surfers_will_always_be_there	phrases that describe the prevalence of shoulder surfing
surrounding_awareness	phrases that relate to the awareness of the surrounding
use_of_privacy_measures	actions that indicate user-level efforts for privacy protection
app_access	phrases that communicate selective app access
shoulder_surfing_awareness	phrases that describe awareness of participants on shoulder surfing
continued_use_without_change	phrases where participant continued the device usage without making changes
device_use	phrases that describe how a device is used
perspective	phrases that describe how participant's opinion
unavoidable	phrases that describe when something can not be avoided
user_position	phrases that describe the positioning of the participant
application_specific	where participants described something specific to a certain application
availability	where participants described of something being able to use
awareness	knowledge of participants
ease_of_use	words that describe easy and simple to use
invasive	words that describe how much something intervenes user experience
prevention	phrases that show how something could be prevented from happening
privacy_screen	a screen protector that can be applied on the smartphone's screen to avoid viewing from certain angles
public_spaces	a location with a dense number of people
safety	phrases that describe the condition of protection
screen_lock	phrases that describe mechanisms that lock the device screen from use
security	phrases that describe the state of being free from the threat of something
tool_cost	phrases that describe the financial cost of a tool
tool_dependent	phrases that describe some conditions of a tool
unnecessary	phrases that describe something is unrequired
avoid	keeping away from something
discomfort	negative feeling of being uncomfortable
increased_time	additional period of time to accomplish a task
task_interruption	disruption to the task being performed
concern	a matter of interest or importance that causes worry
considerate	being careful of not letting harm to oneself
neutral	state of being neither agreeing nor disagreeing
other_people_privacy	someone else's right to keep their information private
personal_privacy	referring to one's right to be free from interference and intrusion
unintentional	accidental, involuntary
negative_impact	adverse affects, consequences
unclear	uncertainty phrases
blackmailing	forcing someone to do something
content_specific_concern	concerns specific to a content type
identity_theft	using another person's identity
inappropriate_content	disturbing or upsetting content
information_theft	immoral gaining of data
misuse_of_personal_information	improper use of information
personal_space	distance from another person where one feels comfortable
information_privacy	data privacy
self_perception_from_the_eyes_of_others	viewing oneself from the lens of others
stalker	a person who pursues someone obsessively
unauthorized_access	gaining access to something without permission
unethical	not confirming to high moral standards

Table C.1: Codebook Used to Analyse Questionnaire Responses

Appendix D

D.1 Item Generation Phase

This section lists the total items created in the initial item generation phase using literature-based and empirical approaches.

D.1.1 Items Created Using Literature-Based Approach

1. I turn off my device's display if I notice someone looking over my screen without my permission [85]
2. I adjust my position when browsing through my smartphone so that no one can take a look at it [91]
3. I hide the screen with my hands if I notice someone looking at my screen [94]
4. I usually avoid accessing apps that contain private information when I am around others [85]
5. If someone looks at my screen without permission, I usually ignore them [85]
6. To avoid surrounding people from looking at my screen, I use a tampered privacy protector on my device [91]
7. I lower my screen brightness so that no one around me can take a look at my screen [94]
8. I am concerned about my reputation if someone oversees my device screen without my permission [91]
9. If someone oversees my screen content, I would feel uncomfortable, because I feel like those people trusted me to keep their data private [85]
10. I often clean my device screen to remove any oily residues so that no one can use them to trace what I entered on the device [256]

11. I use biometric authentication to avoid someone observing my password and/or to avoid any oily or heat residues on the screen [25]
12. I backup my valuable data often for safety in case of theft or lost [213]
13. I carry a small paper book to save my contacts in case my device is lost/stolen [213]
14. I back up my data frequently [213]
15. I do not trust the security of smartphones and therefore do not store any sensitive information on them [213]
16. I would change all my passwords immediately in my smartphone is stolen or lost [213]
17. I do not leave my device unattended around others to avoid giving anyone the opportunity to unlock it [25]
18. I am concerned when using ATMs that use cameras for recording purposes [25]
19. I wear gloves to avoid anyone taking heat traces picture of my PIN when I use ATM [25]
20. I press extra keys after I have entered my PIN at the ATM [25]

D.1.2 Items Constructed Through Deductive Approach - Researchers Developed Items

21. I clear my location track history because in case my phone is lost then someone might be able to track down my home
22. I access sensitive data only on personal PC
23. I keep my security knowledge up to date
24. I use auto-fill in passwords to avoid anyone over seeing my passwords when I enter on my smartphone
25. I am concerned about my reputation if I see someone looking over my screen without permission
26. I check for my surrounding people when I use my smartphone at public places
27. The surveillance cameras concern me as I fear that they might be recording my device interaction
28. The increasing availability and cost feasibility of devices like thermal cameras are a threat to everyone's privacy

29. I clean my smartphone screen often to clear off any smudges left behind after interaction
30. I use two smartphones, one for private and indoor usage and one for outdoor purposes so I don't have to worry in case of smartphone theft
31. Along with taking care of threats within the device such as phishing emails, I also take care of threats outside the device, for example device observations by surrounding people
32. I get annoyed when I catch someone looking over my device screen
33. I often catch people looking over my device screen without permission which irritates me
34. I would like my device to do something everytime someone looks at it without my permission
35. I hide my screen when I am in public areas
36. I hide my screen when I am viewing sensitive information on my phone
37. I scroll quickly when I sense someone is looking at my phone's screen
38. I switch off my phone when I sense someone is looking at my phone's screen
39. I don't view sensitive messages, play sensitive voice messages, or view perform sensitive actions (e.g., online banking) on my phone when I am in a public area
40. I place my palm on touchscreens after I have entered sensitive information, to reduce the chances for thermal attacks to succeed
41. I press random keys on touchscreens to add noise to thermal imaging data
42. I wipe my phone's screen with a cloth to prevent smudge attacks
43. I don't leave my phone unattended to make sure no one attempts to use it or try to unlock it
44. I keep my phone near me and visible to me all the time to make sure it is not compromised

D.1.3 Items Constructed Through Deductive Approach - Items by Larger Pool of Researchers

45. I ensure no one is looking at my screen when I am entering passwords
46. I use separate devices for private and non-private stuff
47. I get anxious when someone from my surrounding invades my device privacy

48. I am worried that someone might access my information by spying on what I am doing on my smartphone
49. I am a privacy-centred person
50. I would be embarrassed if information found on my smartphone is leaked to my surrounding people
51. I keep myself updated on how someone around me can unlock my smartphone without my permission
52. I consider my data as a target from device external threats
53. I believe my data is worth protecting from device external threats
54. I protect my device from being observed by others
55. I believe there are no data privacy threats outside of the device
56. I am well aware of how to protect my data from device external threats
57. I believe device external threats are not a serious privacy threat to be concerned of
58. Device external threats are not effective in leaking private information
59. I value protecting information from device external threats
60. Device external threats are not a concerning threat to privacy
61. It is fine for me to unveil my phone screen to the public
62. It is important for me to protect from screen content from people around me in public transport
63. I do not believe that someone could use my screen traces to attack my phone
64. I don't mind if someone sitting next to me takes a look at my smartphone while I am watching a video
65. I am concerned by the CCTC cameras as they might capture what I am doing on my device
66. I protect my data from surrounding people
67. I take all actions to keep my data safe from device external threats

D.2 Items Used in the Pre-Testing Phase

1. I try to adjust my hand position when using my smartphone so that no one can see the information shown on it
2. I hide my smartphone screen with my hands if I notice anyone looking at it
3. If anyone looks at my screen without permission, I tend to put my smartphone away
4. To avoid people nearby from looking at my smartphone screen, I specifically use a privacy-protecting screen cover (e.g. tampered glass protector)
5. I lower my screen brightness so that no one around me can take a look at what is shown on it
6. If someone sees my friend's content on my screen, it feels like a breach of my friend's trust in me to keep their content private
7. I use fingerprint (or other biometric methods) mainly to avoid someone observing my password
8. I trust the security system of smartphones and therefore store any sensitive information on them
9. I would change all of my passwords immediately if my smartphone was lost
10. I feel concerned when using ATMs that use cameras for recording purposes
11. I wear gloves to avoid anyone taking a heat-trace picture of my PIN when I use an ATM
12. I press extra keys after I have entered my PIN at the atm to avoid anyone taking a heat-trace picture of my PIN
13. I access all sorts of data on my smartphone, including sensitive data
14. Among the reasons I use auto-fill for passwords on my smartphone, is to avoid anyone overseeing what I enter
15. I check for any surrounding people when I am doing something on my smartphone in public places
16. The increasing availability and affordability of audio, video and photo recording devices are a threat to everyone's privacy
17. I would like my device to do something to alert me every time someone looks at it without my permission

18. I scroll quickly when I sense someone is looking at my smartphone's screen
19. I place my palm on touchscreens after I have entered sensitive information, to reduce the chances for thermal attacks to succeed
20. I press random keys on touchscreens to add irrelevant signals to thermal imaging data
21. I ensure no one is looking at my screen when I am typing in passwords
22. I consider my data to be a target for external threats to my device such as shoulder surfing
23. I believe my data is worth protecting from external threats to my device
24. Privacy invasion by people surrounding us is effective in leaking information
25. It is not fine for me to have my smartphone screen visible to the public
26. It is important for me to protect my screen content from people around me on public transport
27. I believe that someone could use any finger tip traces on my screen to reveal my password
28. I mind if a stranger sitting next to me takes a look at my smartphone while I am watching a private video
29. I am a privacy-centred person
30. I am worried that someone might access my information by spying on what I am doing on my smartphone
31. I get anxious when someone from my surroundings invades my privacy by looking at the screen

D.3 Items Explored in the Exploratory Factor Analysis

1. I try to adjust my hand position when using my smartphone so that no one can see the information shown on it
2. If anyone looks at my screen without permission, I tend to put my smartphone away
3. To avoid people nearby from looking at my smartphone screen, I specifically use a privacy-protecting screen cover (e.g. tampered glass protector)
4. I lower my screen brightness so that no one around me can take a look at what is shown on it

5. If someone sees my friend's content on my screen, it feels like a breach of my friend's trust in me to keep their content private
6. I use fingerprint (or other biometric methods) mainly to avoid someone observing my password
7. I trust the security system of smartphones and therefore store any sensitive information on them
8. I would change all of my passwords immediately if my smartphone was lost
9. I feel concerned when using ATMs that use cameras for recording purposes
10. I press extra keys after I have entered my PIN at the atm to avoid anyone taking a heat-trace picture of my PIN
11. I access all sorts of data on my smartphone, including sensitive data
12. Among the reasons I use auto-fill for passwords on my smartphone, is to avoid anyone overseeing what I enter
13. I check for any surrounding people when I am doing something on my smartphone in public places
14. The increasing availability and affordability of audio, video and photo recording devices are a threat to everyone's privacy
15. I would like my device to do something to alert me every time someone looks at it without my permission
16. I scroll quickly when I sense someone is looking at my smartphone's screen
17. I consider my data to be a target for external threats to my device such as shoulder surfing
18. I believe my data is worth protecting from external threats to my device
19. Privacy invasion by people surrounding us is effective in leaking information
20. It is not fine for me to have my smartphone screen visible to the public
21. It is important for me to protect my screen content from people around me on public transport
22. I believe that someone could use any finger tip traces on my screen to reveal my password
23. I mind if a stranger sitting next to me takes a look at my smartphone while I am watching a private video

Item Statement	Literature-Based	Reference	Empirically (by Researchers)	Empirically (by Experts)
It is important for me to protect my screen content from people around me on public transport				✓
I am worried that someone might access my information by spying on what I am doing on my smartphone				✓
I get anxious when someone from my surroundings invades my privacy by looking at the screen				✓
I am a privacy-centred person				✓
I consider my data to be a target for external threats to my device such as shoulder surfing				✓
I believe my data is worth protecting from external threats to my device				✓
It is not fine for me to have my smartphone screen visible to the public				✓
I mind if a stranger sitting next to me takes a look at my smartphone while I am watching a private video				✓
Privacy invasion by people surrounding us is effective in leaking information				✓
The increasing availability and affordability of audio, video and photo recording devices are a threat to everyone's privacy			✓	
I would like my device to do something to alert me every time someone looks at it without my permission			✓	
I would change all of my passwords immediately if my smartphone was lost	✓	[213]		
If someone sees my friend's content on my screen, it feels like a breach of my friend's trust in me to keep their content private	✓	[85]		
Among the reasons I use auto-fill for passwords on my smartphone, is to avoid anyone oversteering what I enter			✓	
I scroll quickly when I sense someone is looking at my smartphone's screen			✓	
I try to adjust my hand position when using my smartphone so that no one can see the information shown on it	✓	[91]		
I check for any surrounding people when I am doing something on my smartphone in public places			✓	
If anyone looks at my screen without permission, I tend to put my smartphone away	✓	[91]		

Table D.1: The Table shows the list of items included in the final version of the ODPS and the corresponding sources.

24. I am a privacy-centred person

25. I am worried that someone might access my information by spying on what I am doing on my smartphone

26. I get anxious when someone from my surroundings invades my privacy by looking at the screen

D.4 Final Set of Items & The Respective Sources

The table below presents the items from the final version of the out-of-device Privacy Scale and lists the corresponding sources from which the items were derived.

D.5 Exploring Multi-Factor Solutions - Additional Analysis

To finalize the factor solution, we explored factor solutions using direct oblimin (oblique) as the rotation method. We present and discuss the results below.

First, we explored a four-factor solution using 0.4 as the recommended loading cut-off value. The Table D.2 below presents the results. It can be observed that no item is loaded onto the fourth factor. Therefore, we next explored a three-factor solution. Table D.3 shows the output of a 3-factor solution. It can be observed that only two items are loaded onto the second factor, whereas at least three items must be loaded onto a factor for it to be considered a factor. Therefore, we dropped the three-factor solution and next explored a two-factor solution. The 2-factor solution (presented in Table D.4 gave a simple structure; however, before finalizing it, we checked for the following descriptives:

1. Correlation between the two factors: The correlation between the two factors turned out to be .553, indicating a high correlation.
2. Reliability: We then checked for reliability, which appeared to be 0.857 for the first and 0.664 for the second factors. While the first factor gave a good reliability score, the reliability of the second factor was unacceptable.

While the above recommends opting for a single-factor solution, we further explored essential statistics. We collected a new dataset with $N=1000$ participants. Out of $N=1000$, 69 failed the attention check and were removed from further analysis. On the remaining $N=931$ participants' data, we performed the following tests. We again checked for a correlation between the two factors in the new dataset collected. The correlation between the two factors in the latest dataset was 0.590, indicating a high correlation. We then extracted loadings using Principle Axis Factoring (PAF) and CFA (Confirmatory Factor Analysis) for the two factors. For the loadings received using PAF (two-factor solution), the average variance extracted for each factor was 0.469 and 0.234, respectively. We then checked for the square root of AVE and compared it to the correlation. The square root of AVE was higher for only one factor (0.684) and not the other factor (0.483). For the loadings received using CFA, the average variance extracted for each factor was 0.47817 and 0.3207, respectively. We then checked for the square root of AVE and compared it to the correlation. The square root of AVE was higher for only one factor (0.691) and not the other factor (0.566). In both cases, insufficient discriminant validity was observed as factor correlation was not lower than the square root of AVE for Factor 2. Further, the AVE for each factor is less than 0.5, which is unacceptable as greater than 0.5 is the recommended threshold. Even with all these methods, TLI remains below the threshold of 0.9 (0.872). Given all these results, we opted for a single-factor solution.

Item Statements	Factor			
	1	2	3	4
I am worried that someone might access my information by spying on what I am doing on my smartphone	0.726			
I consider my data to be a target for external threats to my device such as shoulder surfing	0.701			
I am a privacy-centred person	0.546			
Privacy invasion by people surrounding us is effective in leaking information	0.49			
The increasing availability and affordability of audio, video and photo recording devices are a threat to everyone's privacy	0.455			
I believe my data is worth protecting from external threats to my device	0.447			
I mind if a stranger sitting next to me takes a look at my smartphone while I am watching a private video	0.443			
I feel concerned when using ATMs that use cameras for recording purposes				
It is not fine for me to have my smartphone screen visible to the public				
I would like my device to do something to alert me every time someone looks at it without my permission				
Among the reasons I use auto-fill for passwords on my smartphone, is to avoid anyone oversteering what I enter		0.517		
To avoid people nearby from looking at my smartphone screen, I specifically use a privacy-protecting screen cover (e.g. tampered glass protector)		0.448		
I use fingerprint (or other biometric methods) mainly to avoid someone observing my password		0.406		
I lower my screen brightness so that no one around me can take a look at what is shown on it				
I would change all of my passwords immediately if my smartphone was lost				
I check for any surrounding people when I am doing something on my smartphone in public places			-0.681	
If anyone looks at my screen without permission, I tend to put my smartphone away			-0.63	
I scroll quickly when I sense someone is looking at my smartphone's screen			-0.565	
I try to adjust my hand position when using my smartphone so that no one can see the information shown on it			-0.526	
I get anxious when someone from my surroundings invades my privacy by looking at the screen	0.432		-0.459	
It is important for me to protect my screen content from people around me on public transport			-0.445	
If someone sees my friend's content on my screen, it feels like a breach of my friend's trust in me to keep their content private				

Table D.2: The table shows the results of a 4-factor solution using a loading cut-off value of 0.4.

Item Statements	Factor		
	1	2	3
I consider my data to be a target for external threats to my device such as shoulder surfing	0.651		
I believe my data is worth protecting from external threats to my device	0.57		
I am worried that someone might access my information by spying on what I am doing on my smartphone	0.553		
The increasing availability and affordability of audio, video and photo recording devices are a threat to everyone's privacy	0.523		
Privacy invasion by people surrounding us is effective in leaking information	0.492		
It is not fine for me to have my smartphone screen visible to the public	0.452		
I am a privacy-centred person	0.447		
It is important for me to protect my screen content from people around me on public transport	0.443		-0.41
I feel concerned when using ATMs that use cameras for recording purposes	0.423		
I mind if a stranger sitting next to me takes a look at my smartphone while I am watching a private video			
I would like my device to do something to alert me every time someone looks at it without my permission			
I would change all of my passwords immediately if my smartphone was lost			
Among the reasons I use auto-fill for passwords on my smartphone, is to avoid anyone oversteering what I enter		0.526	
To avoid people nearby from looking at my smartphone screen, I specifically use a privacy-protecting screen cover (e.g. tampered glass protector)		0.449	
I use fingerprint (or other biometric methods) mainly to avoid someone observing my password			
I lower my screen brightness so that no one around me can take a look at what is shown on it			
I check for any surrounding people when I am doing something on my smartphone in public places			-0.66
I scroll quickly when I sense someone is looking at my smartphone's screen			-0.617
I try to adjust my hand position when using my smartphone so that no one can see the information shown on it			-0.589
I get anxious when someone from my surroundings invades my privacy by looking at the screen			-0.555
If anyone looks at my screen without permission, I tend to put my smartphone away			-0.501
If someone sees my friend's content on my screen, it feels like a breach of my friend's trust in me to keep their content private			

Table D.3: The Table shows the 3-factor solution using a loading cut-off value of 0.4.

Item Statements	Factor	
	1	2
It is important for me to protect my screen content from people around me on public transport	0.673	
I am worried that someone might access my information by spying on what I am doing on my smartphone	0.649	
I am a privacy-centred person	0.632	
I consider my data to be a target for external threats to my device such as shoulder surfing	0.63	
I believe my data is worth protecting from external threats to my device	0.619	
I get anxious when someone from my surroundings invades my privacy by looking at the screen	0.619	
The increasing availability and affordability of audio, video and photo recording devices are a threat to everyone's privacy	0.551	
I mind if a stranger sitting next to me takes a look at my smartphone while I am watching a private video	0.545	
It is not fine for me to have my smartphone screen visible to the public	0.539	
Privacy invasion by people surrounding us is effective in leaking information	0.533	
I feel concerned when using ATMs that use cameras for recording purposes		
I would like my device to do something to alert me every time someone looks at it without my permission		
If anyone looks at my screen without permission, I tend to put my smartphone away		
I would change all of my passwords immediately if my smartphone was lost		
If someone sees my friend's content on my screen, it feels like a breach of my friend's trust in me to keep their content private		
Among the reasons I use auto-fill for passwords on my smartphone, is to avoid anyone overseeing what I enter		0.557
I lower my screen brightness so that no one around me can take a look at what is shown on it		0.468
I scroll quickly when I sense someone is looking at my smartphone's screen		0.468
To avoid people nearby from looking at my smartphone screen, I specifically use a privacy-protecting screen cover (e.g. tampered glass protector)		0.465
I try to adjust my hand position when using my smartphone so that no one can see the information shown on it		0.444
I check for any surrounding people when I am doing something on my smartphone in public places		
I use fingerprint (or other biometric methods) mainly to avoid someone observing my password		

Table D.4: The Table shows the 2-factor solution using a loading cut-off value of 0.4

Appendix E

E.1 Questionnaire Format

Introduction

Shoulder Surfing refers to observing someone's device screen without permission. Shoulder surfing can happen anytime and by anyone, requiring no special expertise or equipment but careful observation. Among all devices, smartphones are the most shoulder-surfed device. For this reason, in this study, we focus on experiences of shoulder surfing on smartphones only. The picture below shows an example of everyday life shoulder surfing. In this questionnaire, we will use some words that are worth defining for the sake of clarity:

Content: This refers to any content on the smartphone, e.g. text, pictures, videos, etc.

Device: This refers to the item being attacked. In this study, it will be a smartphone

Interface: This refers to the part of the device you are interacting with. For a smartphone, it is the touchscreen.

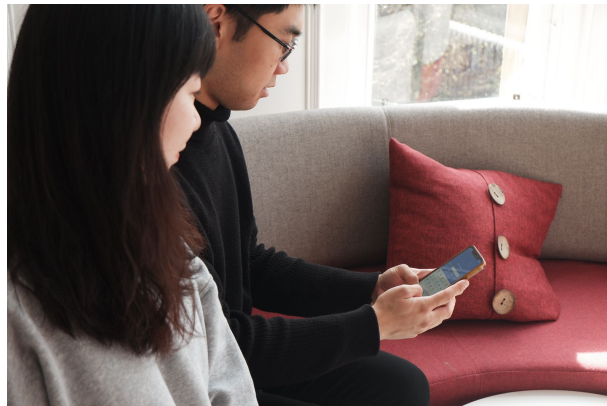


Figure E.1: The figure shows an example of everyday life shoulder surfing

Please answer the following questions to confirm that you understand what is meant by shoulder surfing.

- Shoulder surfing refers to observing someone's device screen without permission. Please indicate if this statement is true or false.
 - True
 - False
- To perform a shoulder surfing attack, one must be close to the device screen being observed. Please indicate if this statement is true or false.
 - True
 - False
- Who, in your opinion, is responsible for protecting you from shoulder surfing attacks?
 - I am responsible
 - The manufacturer of the device is responsible
 - Other:
- Have you ever been shoulder-surfed by someone?
 - Yes
 - No
 - Don't recall
- What is your experience with shoulder surfing?
 - I have intentionally/unintentionally shoulder surfed someone
 - I have intentionally/unintentionally shoulder surfed someone and was shoulder surfed by someone
 - Someone has shoulder surfed me
 - Prefer not to say
- For the statement, "I experience shoulder surfing frequently", do you:
 - Strongly disagree
 - Disagree
 - Somewhat disagree
 - Neither agree nor disagree

- Somewhat agree
 - Agree
 - Strongly agree
- When was the last time you experienced shoulder surfing? Please select the most appropriate choice.
 - Never
 - More than a year ago
 - In the last 6 months
 - In the last 3 months
 - In the last month
 - A few weeks ago
 - A few days ago

Protection Mechanisms

In this section, you will be presented with 10 categories of protection mechanisms and asked to evaluate them. Each category is described, followed by examples of the mechanisms along with their videos. We are interested in your intuitive and honest opinion on these categories of mechanisms. There are no right or wrong answers. We further do not evaluate your performance. You will first be asked to evaluate the mechanisms categories individually. Then, you will be asked to rank all different categories of mechanisms in order of your personal preference.

Selective Visibility: When someone tries to shoulder surf the smartphone, a mechanism is activated that offers a selective viewing experience by making the part the user gazes at visible while making the rest invisible to the human eye. The spots follow your eye movements. To see how the mechanism works, please click on the play button to play the following videos. All the videos present similar features with slight differences. Please make sure to view all videos to get an accurate idea of the mechanism functionality.

Screen Brightness: When someone tries to shoulder surf the smartphone, a mechanism that lowers the screen brightness to make the content less visible from a distance is activated. Below are some examples of this mechanism category. To see how the mechanism works, please click on the play button to play the videos. Please make sure to view all videos to get an accurate idea of the mechanism functionality.

Screen Display Color Change: When someone tries to shoulder surf the smartphone, a mechanism that changes the display into a monochrome combination of black and white upon

the detection of bystanders is activated. Below is an example of this mechanism category. To see how the mechanism works, please click on the play button to play the video.

Distortion: When someone tries to shoulder surf the smartphone, a mechanism that obfuscates the image into small pixels or blocks out the faces in the photos upon detection of bystanders is activated. Below are some examples of this mechanism category. To see how the mechanism works, please click on the play button to play the videos. Please make sure to view all videos to get an accurate idea of this specific mechanism category functions.

Haptic: When someone tries to shoulder surf the smartphone, a mechanism that relates to the sense of touch is activated. In the case of shoulder surfing, the user will be alerted through phone vibrations. Below is an example of this mechanism category. To see how the mechanism works, please click on the play button to play the video.

Icon Overlay: When someone tries to shoulder surf the smartphone, an icon-like mechanism that is placed on the top of the screen to indicate bystanders is activated. For example, an alert icon appears on the top of the screen as shown in Figure 1 or a photo of the bystander appears on the device screen that shows who the bystander is. Below are some examples of this mechanism category. To see how the mechanism works, please click on the play button to play the videos. Please make sure to view all videos to get an accurate idea of the mechanism functionality.

Physical Tangible: When someone tries to shoulder surf the smartphone, a mechanism that relies on physical components i.e. external to the device screen itself, not involving rendering on the display - is activated such as a LED light which is an external part of the device but not the screen display. Below is an example of this mechanism category. To see how the mechanism works, please click on the play button to play the video.

Replacement by Protective Text: When someone tries to shoulder surf the smartphone, a mechanism that replaces the content of the device screen by randomly generated unmeaningful text is activated. Below is an example of this mechanism category. To see how the mechanism works, please click on the play button to play the videos.

Replacement by Meaningful Text: When someone tries to shoulder surf the smartphone, a mechanism replaces the content of the device screen with randomly generated meaningful text. Below is an example of this mechanism category. To see how the mechanism works, please click on the play button to play the video.

Combination of Mechanisms: When someone tries to shoulder surf the smartphone, a mechanism that combines multiple features into one mechanism is activated upon the detection of a shoulder surfer. For example, it adjusts font size, color scheme, and screen brightness - all of them together. Below are some examples of this mechanism category. To see how the mechanism works, please click on the play button to play the following videos. Please make sure to view all videos to get an accurate idea of the mechanism functionality.

Considering the main mechanism category presented in all of the videos above, please answer the following questions. (7-point Likert Scale)

- For the statement, "I would like to use the above protection mechanisms to protect my screen from shoulder surfing", you:
- For the statement, "It is important for me to have the mechanisms installed and working on my device", you:
- For the statement, "I am convinced the mechanisms described above will help protect my privacy", you:
- For the statement, "If the mechanisms described above is not installed by default, I would try to install it myself or resort to a similar alternative to protect my privacy from shoulder surfing", you:
- For the statement, "I prefer using a non-digital alternative to the mechanisms described above to protect my privacy from shoulder surfing (e.g. covering the screen using hands, screen cover, etc). ", you:

Questions for General Protection Mechanisms

Please answer the following questions based on your general perception on the use of mechanisms regardless of their design to protect your privacy from shoulder surfing attacks. (7-point Likert Scale)

- Protecting text and photos from shoulder surfing is important to me.
- I would feel more comfortable using my smartphone in public if it has privacy protection mechanisms.
- Having protection mechanisms will safeguard my privacy.
- Understanding how these mechanisms protect my privacy is easy.
- I trust the presented mechanisms to protect my privacy from shoulder surfing
- Having these mechanisms makes me aware of my surroundings

- Having access to the mechanisms described above makes me consider using them to protect my privacy.
- I prefer using the presented mechanisms rather than having none to protect my device from shoulder surfing.
- The presented privacy mechanisms better protect my privacy from shoulder surfing than non-digital alternatives, such as covering the screen using my hands or screen cover.
- Having a mechanism that only alerts me about shoulder surfing is sufficient for me.
- The protection mechanism must convey irrelevant information (such as random unmeaningful text) to the observer to let them know they have invaded my personal space.
- A protection mechanism that covers the entire display is suitable for me.
- The protection mechanism should tell about who the observer is as well.
- The observer should not know that I have a protection mechanism.

Bibliography

- [1] 62443, I. Iec 62443, 2022.
- [2] ABDELRAHMAN, Y., KHAMIS, M., SCHNEEGASS, S., AND ALT, F. Stay cool! understanding thermal attacks on mobile-based user authentication. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (2017), pp. 3751–3763.
- [3] ABDRABOU, Y., KHAMIS, M., EISA, R. M., ISMAIL, S., AND ELMOUGY, A. Just gaze and wave: Exploring the use of gaze and gestures for shoulder-surfing resilient authentication. In *Proceedings of the 11th acm symposium on eye tracking research & applications* (2019), pp. 1–10.
- [4] ABDRABOU, Y., RIVU, R., AMMAR, T., LIEBERS, J., SAAD, A., LIEBERS, C., GRUENEFELD, U., KNIERIM, P., KHAMIS, M., MÄKELÄ, V., ET AL. Understanding shoulder surfer behavior using virtual reality. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)* (2022), IEEE, pp. 576–577.
- [5] ABDRABOU, Y., RIVU, S. R., AMMAR, T., LIEBERS, J., SAAD, A., LIEBERS, C., GRUENEFELD, U., KNIERIM, P., KHAMIS, M., MAKELA, V., ET AL. Understanding shoulder surfer behavior and attack patterns using virtual reality. In *Proceedings of the 2022 International Conference on Advanced Visual Interfaces* (2022), pp. 1–9.
- [6] ADAMS, A., AND SASSE, M. A. Users are not the enemy. *Communications of the ACM* 42, 12 (1999), 40–46.
- [7] AHMAD, I., FARZAN, R., KAPADIA, A., AND LEE, A. J. Tangible privacy: Towards user-centric sensor designs for bystander privacy. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–28.
- [8] ALASZEWSKI, A. *Using diaries for social research*. Sage, 2006.
- [9] ALBAYRAM, Y., KHAN, M. M. H., AND FAGAN, M. A study on designing video tutorials for promoting security features: A case study in the context of two-factor authentication (2fa). *International Journal of Human–Computer Interaction* 33, 11 (2017), 927–942.

- [10] ALDAWOOD, H., AND SKINNER, G. A taxonomy for social engineering attacks via personal devices. *International Journal of Computer Applications* 975 (2019), 8887.
- [11] ALLIANCE, I. G. C. Quick start guide: An overview of isa/iec 62443 standards security of industrial automation and control systems, 2020.
- [12] ALOTAIBI, N., WILLIAMSON, J., AND KHAMIS, M. Thermosecure: Investigating the effectiveness of ai-driven thermal attacks on commonly used computer keyboards. *ACM Transactions on Privacy and Security* 26, 2 (2023), 1–24.
- [13] ALSOUBAI, A., GHAIUMY ANARAKY, R., LI, Y., PAGE, X., KNIJNENBURG, B., AND WISNIEWSKI, P. J. Permission vs. app limiters: profiling smartphone users to understand differing strategies for mobile privacy management. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (2022), pp. 1–18.
- [14] ALT, F., SCHNEEGASS, S., SHIRAZI, A. S., HASSIB, M., AND BULLING, A. Graphical passwords in the wild: Understanding how users choose pictures and passwords in image-based authentication schemes. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services* (2015), pp. 316–322.
- [15] AMAZON. Amazon alexa, 2022. Retrieved February 20, 2022.
- [16] AMAZON. Amazon Listing - PerfectPrime IR203, (IR) Infrared Thermal Imager Camera. <https://amzn.to/3H22Nod>, 2023. Accessed: 2023-01-13.
- [17] AMIRI SANI, A. Schrodintext: Strong protection of sensitive textual content of mobile applications. In *Proceedings of the 15th annual international conference on mobile systems, applications, and services* (2017), pp. 197–210.
- [18] ANDRIOTIS, P., TRYFONAS, T., OIKONOMOU, G., AND YILDIZ, C. A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks* (2013), pp. 1–6.
- [19] ANDROID. Android ndk, 2022. Retrieved February 20, 2022.
- [20] APPLE. Apple siri, 2022. Retrieved February 20, 2022.
- [21] AT WAIKATO UNIVERSITY, M. L. Weka 3 - data mining with open source machine learning software in java, 2021. Retrieved February 20, 2022.
- [22] AVIV, A. J., DAVIN, J. T., WOLF, F., AND KUBER, R. Towards baselines for shoulder surfing on mobile authentication. In *Proceedings of the 33rd Annual Computer Security Applications Conference* (2017), pp. 486–498.

- [23] BÂCE, M., SAAD, A., KHAMIS, M., SCHNEEGASS, S., AND BULLING, A. Privacyscout: Assessing vulnerability to shoulder surfing on mobile devices. *Proceedings on Privacy Enhancing Technologies 1* (2022), 21.
- [24] BAGOZZI, R. P., AND YI, Y. On the evaluation of structural equation models. *Journal of the academy of marketing science* 16 (1988), 74–94.
- [25] BEKAERT, P., ALOTAIBI, N., MATHIS, F., GERBER, N., RAFFERTY, A. C., KHAMIS, M., AND MARKY, K. Are thermal attacks a realistic threat? investigating the preconditions of thermal attacks in users’ daily lives. In *Nordic Human-Computer Interaction Conference* (2022), pp. 1–9.
- [26] BÉLANGER, F., AND CROSSLER, R. E. Privacy in the digital age: a review of information privacy research in information systems. *MIS quarterly* (2011), 1017–1041.
- [27] BENTLER, P. M. Comparative fit indexes in structural models. *Psychological bulletin* 107, 2 (1990), 238.
- [28] BHAGAVATULA, R., UR, B., IACOVINO, K., KYWE, S. M., CRANOR, L. F., AND SAVVIDES, M. Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption.
- [29] BIANCHI, A., CORBETTA, J., INVERNIZZI, L., FRATANTONIO, Y., KRUEGEL, C., AND VIGNA, G. What the app is that? deception and countermeasures in the android user interface. In *2015 IEEE Symposium on Security and Privacy* (2015), IEEE, pp. 931–948.
- [30] BLYTHE, J., CAMP, J., AND GARG, V. Targeted risk communication for computer security. In *Proceedings of the 16th international conference on Intelligent user interfaces* (2011), pp. 295–298.
- [31] BOATENG, G. O., NEILANDS, T. B., FRONGILLO, E. A., MELGAR-QUIÑONEZ, H. R., AND YOUNG, S. L. Best practices for developing and validating scales for health, social, and behavioral research: a primer. *Frontiers in public health* 6 (2018), 149.
- [32] BOLGER, N., DAVIS, A., AND RAFAELI, E. Diary methods: Capturing life as it is lived. *Annual review of psychology* 54, 1 (2003), 579–616.
- [33] BOUWMAN, X., GRIFFIOEN, H., EGBERS, J., DOERR, C., KLIEVINK, B., AND VAN EETEN, M. A different cup of {TI}? the added value of commercial threat intelligence. In *29th USENIX security symposium (USENIX security 20)* (2020), pp. 433–450.
- [34] BROOKE, J. Sus: a “quick and dirty” usability. *Usability evaluation in industry* 189, 3 (1996).

- [35] BRUDY, F., LEDO, D., GREENBERG, S., AND BUTZ, A. Is anyone looking? mitigating shoulder surfing on public displays through awareness and protection. In *Proceedings of The International Symposium on Pervasive Displays* (2014), pp. 1–6.
- [36] BUCHANAN, T., PAINE, C., JOINSON, A. N., AND REIPS, U.-D. Development of measures of online privacy concern and protection for use on the internet. *Journal of the American society for information science and technology* 58, 2 (2007), 157–165.
- [37] BULLING, A., ALT, F., AND SCHMIDT, A. Increasing the security of gaze-based cued-recall graphical passwords using saliency masks. In *Proceedings of the SIGCHI conference on human factors in computing systems* (2012), pp. 3011–3020.
- [38] CAI, Y., TANG, Y., LI, H., YU, L., ZHOU, H., LUO, X., HE, L., AND SU, P. Resource race attacks on android. In *2020 IEEE 27th International Conference on Software Analysis, Evolution and Reengineering (SANER)* (2020), IEEE, pp. 47–58.
- [39] CAINE, K. Local standards for sample size at chi. In *Proceedings of the 2016 CHI conference on human factors in computing systems* (2016), pp. 981–992.
- [40] CAIRNS, P. *Doing better statistics in human-computer interaction*. Cambridge University Press, 2019.
- [41] CAIRNS, P., SOEGAARD, M., AND DAM, R. Experimental methods in human-computer interaction. *Encyclopedia of Human-Computer Interaction* (2016).
- [42] CANNY, J. A computational approach to edge detection. *IEEE Transactions on pattern analysis and machine intelligence*, 6 (1986), 679–698.
- [43] CANVA. Canva, 2022.
- [44] CARTER, S., AND MANKOFF, J. When participants do the capturing: the role of media in diary studies. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (2005), pp. 899–908.
- [45] CENTRE, N. C. S. Threat modelling, 2024. Retrieved March 23, 2025.
- [46] CERNY, B. A., AND KAISER, H. F. A study of a measure of sampling adequacy for factor-analytic correlation matrices. *Multivariate behavioral research* 12, 1 (1977), 43–47.
- [47] CHA, S., KWAG, S., KIM, H., AND HUH, J. H. Boosting the guessing attack performance on android lock patterns with smudge attacks. In *Proceedings of the 2017 ACM on Asia conference on computer and communications security* (2017), pp. 313–326.

- [48] CHANENSON, J., SLOANE, B., RAJAN, N., MORRIL, A., CHEE, J., HUANG, D. Y., AND CHETTY, M. Uncovering privacy and security challenges in k-12 schools. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (2023), pp. 1–28.
- [49] CHANG, B., CHENG, Y., CHEN, B., ZHANG, F., ZHU, W.-T., LI, Y., AND WANG, Z. User-friendly deniable storage for mobile devices. *computers & security* 72 (2018), 163–174.
- [50] CHANG, C.-C., AND LIN, C.-J. Libsvm, 2021. Retrieved February 20, 2022.
- [51] CHATTOPADHYAY, A., AND BOULT, T. E. Privacycam: a privacy preserving camera using uclinux on the blackfin dsp. In *2007 IEEE Conference on Computer Vision and Pattern Recognition* (2007), IEEE, pp. 1–8.
- [52] CHEN, C.-Y., LIN, B.-Y., WANG, J., AND SHIN, K. G. Keep others from peeking at your mobile device screen! In *The 25th Annual International Conference on Mobile Computing and Networking* (2019), pp. 1–16.
- [53] CHEN, Q. A., QIAN, Z., AND MAO, Z. M. Peeking into your app without actually seeing it: {UI} state inference and novel android attacks. In *23rd USENIX Security Symposium (USENIX Security 14)* (2014), pp. 1037–1052.
- [54] CHEN, R. *A demand-side view of mobile internet adoption in the Global South*. World Bank, 2021.
- [55] CHEN, S., FAN, L., CHEN, C., XUE, M., LIU, Y., AND XU, L. Gui-squatting attack: Automated generation of android phishing apps. *IEEE Transactions on Dependable and Secure Computing* 18, 6 (2019), 2551–2568.
- [56] CHEN, T., FARCASIN, M., AND CHAN-TIN, E. Smartphone passcode prediction. *IET Information Security* 12, 5 (2018), 431–437.
- [57] CHIGNELL, M. H., QUAN-HAASE, A., AND GWIZDKA, J. The privacy attitudes questionnaire (paq): initial development and validation. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (2003), vol. 47, SAGE Publications Sage CA: Los Angeles, CA, pp. 1326–1330.
- [58] CHO, G., HUH, J. H., CHO, J., OH, S., SONG, Y., AND KIM, H. Syspal: System-guided pattern locks for android. In *2017 IEEE Symposium on security and privacy (SP)* (2017), IEEE, pp. 338–356.
- [59] CLAISSE, C., KASADHA, B., STUMPF, S., AND DURRANT, A. C. 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* (2022), pp. 1–19.
- [60] CLARKE, N. L., AND FURNELL, S. M. Authentication of users on mobile telephones—a survey of attitudes and practices. *Computers & Security* 24, 7 (2005), 519–527.
- [61] COHEN, J. E. What privacy is for, 2013. Retrieved Aug 17, 2021.
- [62] COLNAGO, J., CRANOR, L. F., ACQUISTI, A., AND STANTON, K. H. Is it a concern or a preference? an investigation into the ability of privacy scales to capture and distinguish granular privacy constructs. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)* (2022), pp. 331–346.
- [63] COMMITTEE, I., AND (TC65WG10), I. T. C. . W. G. . The 62443 series of standards: Industrial automation and control systems security.
- [64] CONSOLVO, S., SMITH, I. E., MATTHEWS, T., LAMARCA, A., TABERT, J., AND POWLEDGE, P. Location disclosure to social relations: why, when, & what people want to share. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (2005), pp. 81–90.
- [65] COOPER, A., REIMANN, R., CRONIN, D., AND NOESSEL, C. *About face: the essentials of interaction design*. John Wiley & Sons, 2014.
- [66] CRONBACH, L. J. Further evidence on response sets and test design. *Educational and psychological measurement* 10, 1 (1950), 3–31.
- [67] CROWNE, D. P., AND MARLOWE, D. A new scale of social desirability independent of psychopathology. *Journal of consulting psychology* 24, 4 (1960), 349.
- [68] CULNAN, M. J., AND ARMSTRONG, P. K. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization science* 10, 1 (1999), 104–115.
- [69] DAILYMAIL. The zzzzivil servant who fell asleep on the train with laptop secrets in full view, 2008.
- [70] DARLING, D., LIU, Y., AND LI, Q. Privacy protection against shoulder surfing in mobile environments. In *International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services* (2022), Springer, pp. 133–152.
- [71] DAS, S., MARE, S., AND CAMP, L. J. Smart storytelling: Video and text risk communication to increase mfa acceptability. In *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)* (2020), IEEE, pp. 153–160.

- [72] DE LUCA, A., HARBACH, M., VON ZEZSCHWITZ, E., MAURER, M.-E., SLAWIK, B. E., HUSSMANN, H., AND SMITH, M. Now you see me, now you don't: protecting smartphone authentication from shoulder surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2014), pp. 2937–2946.
- [73] DELGADO RODRIGUEZ, S., CHATTERJEE, P., DAO PHUONG, A., ALT, F., AND MARKY, K. Do you need to touch? exploring correlations between personal attributes and preferences for tangible privacy mechanisms. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (2024), pp. 1–23.
- [74] DELGADO RODRIGUEZ, S., PRANGE, S., VERGARA OSSENBERG, C., HENKEL, M., ALT, F., AND MARKY, K. Prikey—investigating tangible privacy control for smart home inhabitants and visitors. In *Nordic Human-Computer Interaction Conference* (2022), pp. 1–13.
- [75] DEVELOPERS, G. Detect faces with ml kit on android, 2022. Retrieved June 08, 2022.
- [76] DEVI, M., AND MAJUMDER, A. Side-channel attack in internet of things: a survey. In *Applications of Internet of Things*. Springer, 2021, pp. 213–222.
- [77] DIAO, W., LIU, X., LI, Z., AND ZHANG, K. No pardon for the interruption: New inference attacks on android through interrupt timing analysis. In *2016 IEEE Symposium on Security and Privacy (SP)* (2016), IEEE, pp. 414–432.
- [78] DIBBLE, J. L., LEVINE, T. R., AND PARK, H. S. The unidimensional relationship closeness scale (urcs): Reliability and validity evidence for a new measure of relationship closeness. *Psychological assessment* 24, 3 (2012), 565.
- [79] DISTLER, V., FASSL, M., HABIB, H., KROMBHOLZ, K., LENZINI, G., LALLEMAND, C., CRANOR, L. F., AND KOENIG, V. A systematic literature review of empirical methods and risk representation in usable privacy and security research. *ACM Transactions on Computer-Human Interaction (TOCHI)* 28, 6 (2021), 1–50.
- [80] DO, Q., MARTINI, B., AND CHOO, K.-K. R. The role of the adversary model in applied security research. *Computers & Security* 81 (2019), 156–181.
- [81] DO, Y., ARORA, N., MIRZAZADEH, A., MOON, I., XU, E., ZHANG, Z., ABOWD, G. D., AND DAS, S. Powering for privacy: Improving user trust in smart speaker microphones with intentional powering and perceptible assurance. In *32nd USENIX Security Symposium (USENIX Security 23)* (Anaheim, CA, Aug. 2023), USENIX Association, pp. 2473–2490.

- [82] DUNPHY, P., HEINER, A. P., AND ASOKAN, N. A closer look at recognition-based graphical passwords on mobile devices. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (2010), pp. 1–12.
- [83] DUPREE, J. L., DEVRIES, R., BERRY, D. M., AND LANK, E. Privacy personas: Clustering users via attitudes and behaviors toward security practices. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (2016), pp. 5228–5239.
- [84] EGELMAN, S., AND PEER, E. 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* (2015), pp. 2873–2882.
- [85] EIBAND, M., KHAMIS, M., VON ZEZSCHWITZ, E., HUSSMANN, H., AND ALT, F. Understanding shoulder surfing in the wild: Stories from users and observers. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (2017), pp. 4254–4265.
- [86] EIBAND, M., VON ZEZSCHWITZ, E., BUSCHEK, D., AND HUSSMANN, H. 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* (2016), pp. 2041–2048.
- [87] EPP, F. A., KANTOSALO, A., JAIN, N., LUCERO, A., AND MEKLER, E. D. Adorned in memes: Exploring the adoption of social wearables in nordic student culture. In *CHI Conference on Human Factors in Computing Systems* (2022), pp. 1–18.
- [88] ETTUS. Usrp b210, 2022. Retrieved February 20, 2022.
- [89] FARZAND, H., ABRAHAM, M., BREWSTER, S., KHAMIS, M., AND MARKY, K. A systematic deconstruction of human-centric privacy & security threats on mobile phones. *International Journal of Human–Computer Interaction* (2024).
- [90] FARZAND, H., AL BAIATY SUAREZ, D., GOODGE, T., MACDONALD, S. A., MARKY, K., KHAMIS, M., AND CAIRNS, P. Beyond aesthetics: Evaluating response widgets for reliability & construct validity of scale questionnaires. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2024), CHI EA '24, Association for Computing Machinery.
- [91] FARZAND, H., BHARDWAJ, K., MARKY, K., AND KHAMIS, M. The interplay between personal relationships & shoulder surfing mitigation. In *Mensch und Computer 2021*. 2021, pp. 338–343.

- [92] FARZAND, H., MACDONALD, S., MARKY, K., AND KHAMIS, M. "what you think is private is no longer" – investigating the aftermath of shoulder surfing on smartphones in everyday life through the eyes of the victims, 2024.
- [93] FARZAND, H., MARKY, K., AND KHAMIS, M. " 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* (USA, 2022), USENIX Association.
- [94] FARZAND, H., MARKY, K., AND KHAMIS, M. Shoulder surfing through the social lens: A longitudinal investigation & insights from an exploratory diary study. In *Proceedings of the 2022 European Symposium on Usable Security* (2022), pp. 85–97.
- [95] FARZAND, H., MARKY, K., AND KHAMIS, M. "... it's very unacceptable for someone to peek into your privacy." chronicles of shoulder surfing: Exploring deep into a longitudinal diary study.
- [96] FARZAND, H., MARKY, K., AND KHAMIS, M. Out-of-device privacy unveiled: Designing and validating the out-of-device privacy scale (odps). In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2024), Association for Computing Machinery.
- [97] FARZAND, H., MARKY, K., AND KHAMIS, M. Sok: Privacy personalised – mapping personal attributes & preferences of privacy mechanisms for shoulder surfing, 2024.
- [98] FARZAND, H., MATHIS, F., MARKY, K., AND KHAMIS, M. Trust & privacy expectations during perilous times of contact tracing. In *Symposium on Usable Security & Privacy (USEC)* (2022).
- [99] FELT, A. P., HA, E., EGELMAN, S., HANEY, A., CHIN, E., AND WAGNER, D. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the eighth symposium on usable privacy and security* (2012), pp. 1–14.
- [100] FELT, A. P., AND WAGNER, D. *Phishing on mobile devices*. Citeseer, 2011.
- [101] FERNANDES, E., CHEN, Q. A., ESSL, G., HALDERMAN, J. A., MAO, Z. M., AND PRAKASH, A. Tivos: Trusted visual i/o paths for android. *University of Michigan CSE Technical Report CSE-TR-586-14* (2014).
- [102] FIANI, C., SAEGHE, P., MCGILL, M., AND KHAMIS, M. Exploring the perspectives of social vr-aware non-parent adults and parents on children's use of social virtual reality. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1 (2024), 1–25.
- [103] FOR DEVELOPERS, A. Permissions on android, 2022. Retrieved February 20, 2022.

- [104] FOR VISUAL DATA SECURITY, E. A. Visual data security white paper, 2012.
- [105] FRANKE, T., ATTIG, C., AND WESSEL, D. 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 (2019), 456–467.
- [106] FRIGO, P., GIUFFRIDA, C., BOS, H., AND RAZAVI, K. Grand pwning unit: Accelerating microarchitectural attacks with the gpu. In *2018 ieee symposium on security and privacy (sp)* (2018), IEEE, pp. 195–210.
- [107] FRIK, A., KIM, J., SANCHEZ, J. R., AND MA, J. Users’ expectations about and use of smartphone privacy and security settings. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (2022), pp. 1–24.
- [108] GENTILE, V., FARZAND, H., BONACCORSO, S., ROCCHESSE, D., MALIZIA, A., KHAMIS, M., AND SORCE, S. User-centered evaluation of different configurations of a touchless gestural interface for interactive displays. In *IFIP Conference on Human-Computer Interaction* (2023), Springer, pp. 501–520.
- [109] GERBER, N., GERBER, P., AND VOLKAMER, M. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & security* 77 (2018), 226–261.
- [110] GERBER, N., ZIMMERMANN, V., AND VOLKAMER, M. Why johnny fails to protect his privacy. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (2019), IEEE, pp. 109–118.
- [111] GHASEMPOURI, T., RAIK, J., PAUL, K., REINBRECHT, C., HAMDIOUI, S., ET AL. Verifying cache architecture vulnerabilities using a formal security verification flow. *Microelectronics Reliability* 119 (2021), 114085.
- [112] GOEL, D., AND JAIN, A. K. Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers & Security* 73 (2018), 519–544.
- [113] GOLLE, P., AND PARTRIDGE, K. On the anonymity of home/work location pairs. In *International Conference on Pervasive Computing* (2009), Springer, pp. 390–397.
- [114] GOOGLE. Google assistant, 2022. Retrieved February 20, 2022.
- [115] GOUCHER, W. Look behind you: the dangers of shoulder surfing. *Computer Fraud & Security* 2011, 11 (2011), 17–20.
- [116] GRISWOLD-STEINER, I., LEFEVRE, Z., AND SERWADDA, A. Smartphone speech privacy concerns from side-channel attacks on facial biomechanics. *Computers & Security* 100 (2021), 102110.

- [117] GRÜNERBL, A., MUAREMI, A., OSMANI, V., BAHLE, G., OEHLER, S., TRÖSTER, G., MAYORA, O., HARING, C., AND LUKOWICZ, P. Smartphone-based recognition of states and state changes in bipolar disorder patients. *IEEE journal of biomedical and health informatics* 19, 1 (2014), 140–148.
- [118] GRUSS, D., BIDNER, D., AND MANGARD, S. Practical memory deduplication attacks in sandboxed javascript. In *European Symposium on Research in Computer Security* (2015), Springer, pp. 108–122.
- [119] GUEST, G., NAMEY, E., AND CHEN, M. A simple method to assess and report thematic saturation in qualitative research. *PloS one* 15, 5 (2020), e0232076.
- [120] GUGENHEIMER, J., DE LUCA, A., HESS, H., KARG, S., WOLF, D., AND RUKZIO, E. Colorsnakes: Using colored decoys to secure authentication in sensitive contexts. In *Proceedings of the 17th international conference on human-computer interaction with mobile devices and services* (2015), pp. 274–283.
- [121] GULMEZOGLU, B., ZANKL, A., TOL, M. C., ISLAM, S., EISENBARTH, T., AND SUNAR, B. Undermining user privacy on mobile devices using ai. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security* (2019), pp. 214–227.
- [122] GUO, Y., MA, J., WU, W., AND CHEN, X. Inferring ui states of mobile applications through power side channel exploitation. In *International Conference on Security and Privacy in Communication Systems* (2018), Springer, pp. 210–226.
- [123] GUPTA, H., SURAL, S., ATLURI, V., AND VAIDYA, J. Deciphering text from touch-screen key taps. In *IFIP Annual Conference on Data and Applications Security and Privacy* (2016), Springer, pp. 3–18.
- [124] GUPTA, S., SINGHAL, A., AND KAPOOR, A. A literature survey on social engineering attacks: Phishing attack. In *2016 international conference on computing, communication and automation (ICCCA)* (2016), IEEE, pp. 537–540.
- [125] HAIR, J. F., ANDERSON, R., TATHAM, R., AND BLACK, W. Multivariate data analysis prentice hall. *Upper Saddle River, NJ 730* (1998).
- [126] HANNA, S., HUANG, L., WU, E., LI, S., CHEN, C., AND SONG, D. Juxtapp: A scalable system for detecting code reuse among android applications. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment* (2012), Springer, pp. 62–81.

- [127] HARBACH, M., VON ZEZSCHWITZ, E., FICHTNER, A., DE LUCA, A., AND SMITH, M. 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)* (2014), pp. 213–230.
- [128] HASAN, R., WEIL, R., SIEGEL, R., AND KROMBOLZ, K. A psychometric scale to measure individuals' value of other people's privacy (vopp). In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (2023), pp. 1–14.
- [129] HASEGAWA, A. A., INOUE, D., AND AKIYAMA, M. How weird is usable privacy and security research? In *33rd USENIX Security Symposium* (2024).
- [130] HEARTFIELD, R., AND LOUKAS, G. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys (CSUR)* 48, 3 (2015), 1–39.
- [131] HERBERT, F., BECKER, S., SCHAEWITZ, L., HIELSCHER, J., KOWALEWSKI, M., SASSE, A., ACAR, Y., AND DÜRMUTH, M. A world full of privacy and security (mis) conceptions? findings of a representative survey in 12 countries. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (2023), pp. 1–23.
- [132] HERNANDEZ, J., MCDUFF, D. J., AND PICARD, R. W. Biophone: Physiology monitoring from peripheral smartphone motions. In *2015 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)* (2015), IEEE, pp. 7180–7183.
- [133] HINKIN, T. R. A brief tutorial on the development of measures for use in survey questionnaires. *Organizational research methods* 1, 1 (1998), 104–121.
- [134] HO, T. K. Random decision forests. In *Proceedings of 3rd international conference on document analysis and recognition* (1995), vol. 1, IEEE, pp. 278–282.
- [135] HÖLZL, M., ROLAND, M., AND MAYRHOFFER, R. Real-world identification for an extensible and privacy-preserving mobile eid. In *IFIP International Summer School on Privacy and Identity Management* (2017), Springer, pp. 354–370.
- [136] HP. Stop shoulder surfers with the hp elitebook x360, 2020. Retrieved February 11, 2021.
- [137] HU, L.-T., AND BENTLER, P. M. Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural equation modeling: a multidisciplinary journal* 6, 1 (1999), 1–55.

- [138] HUA, J., SHEN, Z., AND ZHONG, S. We can track you if you take the metro: Tracking metro riders using accelerometers on smartphones. *IEEE Transactions on Information Forensics and Security* 12, 2 (2016), 286–297.
- [139] HUESTEGGE, L., AND PIMENIDIS, L. Visual search in authentication systems based on memorized faces: Effects of memory load and retention interval. *International Journal of Human-Computer Interaction* (2014), 604–611.
- [140] HYLDEGÅRD, J. Using diaries in group based information behavior research: A methodological study. In *Proceedings of the 1st International Conference on Information Interaction in Context* (New York, NY, USA, 2006), IiiX, Association for Computing Machinery, p. 153–161.
- [141] IBM. What is social engineering, 2022. Retrieved March 23, 2025.
- [142] INCI, M. S., EISENBARTH, T., AND SUNAR, B. Hit by the bus: Qos degradation attack on android. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (2017), pp. 716–727.
- [143] INTERACTIVE, H. Privacy on and off the internet: What consumers want. *Privacy and American Business* (2002), 1–127.
- [144] IVATURI, K., AND JANCZEWSKI, L. A taxonomy for social engineering attacks. In *International Conference on Information Resources Management* (2011), Centre for Information Technology, Organizations, and People, pp. 1–12.
- [145] JANA, S., AND SHMATIKOV, V. Memento: Learning secrets from process footprints. In *2012 IEEE Symposium on Security and Privacy* (2012), IEEE, pp. 143–157.
- [146] JIA, J., AND GONG, N. Z. {AttriGuard}: A practical defense against attribute inference attacks via adversarial machine learning. In *27th USENIX Security Symposium (USENIX Security 18)* (2018), pp. 513–529.
- [147] JIANG, L., MENG, W., WANG, Y., SU, C., AND LI, J. Exploring energy consumption of juice filming charging attack on smartphones: a pilot study. In *International Conference on Network and System Security* (2017), Springer, pp. 199–213.
- [148] JOHNSON, A. Side channel attacks and mitigations 2015-2020: A taxonomy of published work. In *European Conference on Cyber Warfare and Security* (2021), Academic Conferences International Limited, pp. 482–XII.
- [149] JOY PERSIAL, G., PRABHU, M., AND SHANMUGALAKSHMI, R. Side channel attack-survey. *Int J Adva Sci Res Rev* 1, 4 (2011), 54–57.

- [150] KAISER, H. F. An index of factorial simplicity. *psychometrika* 39, 1 (1974), 31–36.
- [151] KALAL, Z., MIKOLAJCZYK, K., AND MATAS, J. Tracking-learning-detection. *IEEE transactions on pattern analysis and machine intelligence* 34, 7 (2011), 1409–1422.
- [152] KATSINI, C., ABDRABOU, Y., RAPTIS, G. E., KHAMIS, M., AND ALT, F. 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* (2020), pp. 1–21.
- [153] KEZER, M., SEVI, B., CEMALCILAR, Z., AND BARUH, L. Age differences in privacy attitudes, literacy and privacy management on facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10, 1 (2016).
- [154] KHAMIS, M., ALT, F., HASSIB, M., VON ZEZSCHWITZ, E., HASHOLZNER, R., AND BULLING, A. Gazetouchpass: Multimodal authentication using gaze and touch on mobile devices. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (2016), pp. 2156–2164.
- [155] KHAMIS, M., BANDELOW, L., SCHICK, S., CASADEVALL, D., BULLING, A., AND ALT, F. 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* (2017), pp. 31–35.
- [156] KHAMIS, M., EIBAND, M., ZÜRN, M., AND HUSSMANN, H. Eyespot: Leveraging gaze to protect private text content on mobile devices from shoulder surfing. *Multimodal Technologies and Interaction* 2, 3 (2018), 45.
- [157] KHAMIS, M., FARZAND, H., MUMM, M., AND MARKY, K. 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* (New York, NY, USA, 2022), AVI 2022, Association for Computing Machinery.
- [158] KHAMIS, M., HASSIB, M., ZEZSCHWITZ, E. V., BULLING, A., AND ALT, F. Gaze-touchpin: protecting sensitive data on mobile devices using secure multimodal authentication. In *Proceedings of the 19th acm international conference on multimodal interaction* (2017), pp. 446–450.
- [159] KHAMIS, M., MARKY, K., BULLING, A., AND ALT, F. User-centred multimodal authentication: securing handheld mobile devices using gaze and touch input. *Behaviour & Information Technology* (2022), 1–23.

- [160] KHAMIS, M., PANSKUS, R., FARZAND, H., MUMM, M., MACDONALD, S., AND MARKY, K. Perspectives on deepfakes for privacy: Comparing perceptions of photo owners and obfuscated individuals towards deepfake versus traditional privacy-enhancing obfuscation.
- [161] KHAMIS, M., TROTTER, L., MÄKELÄ, V., ZEZSCHWITZ, E. v., LE, J., BULLING, A., AND ALT, F. Cueauth: Comparing touch, mid-air gestures, and gaze for cue-based authentication on situated displays. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4 (2018), 1–22.
- [162] KHAN, H., HENGARTNER, U., AND VOGEL, D. Evaluating attack and defense strategies for smartphone pin shoulder surfing. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (2018), pp. 1–10.
- [163] KHAN, S. Erving goffman, the presentation of self in everyday life (1959). *Public Culture* 32, 2 (2020), 397–404.
- [164] KHAN, S., IQBAL, M., OSHO, O., SINGH, K., DERRICK, K., NELSON, P., LI, L., SIDNAM-MAUCH, E., BANNISTER, N., CAINE, K., ET AL. Teaching middle schoolers about the privacy threats of tracking and pervasive personalization: A classroom intervention using design-based research. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (2024), pp. 1–26.
- [165] KIM, H., KU, B., KIM, J. Y., PARK, Y.-J., PARK, Y.-B., ET AL. Confirmatory and exploratory factor analysis for validating the phlegm pattern questionnaire for healthy subjects. *Evidence-Based Complementary and Alternative Medicine* 2016 (2016).
- [166] KIRKWOOD, D., TOMBUL, C., FIRTH, C., MACDONALD, F., PRIFTIS, K., MATHIS, F., KHAMIS, M., AND MARKY, K. Pin scrambler: Assessing the impact of randomized layouts on the usability and security of pins. In *Proceedings of the 21st International Conference on Mobile and Ubiquitous Multimedia* (2022), pp. 83–88.
- [167] KLINE, P. *Handbook of psychological testing*. Routledge, 2013.
- [168] KNIJNENBURG, B. P. Privacy? i can’t even! making a case for user-tailored privacy. *IEEE Security & Privacy* 15, 4 (2017), 62–67.
- [169] KNIJNENBURG, B. P., ANARAKY, R. G., WILKINSON, D., NAMARA, M., HE, Y., CHERRY, D., AND ASH, E. User-tailored privacy., 2022.
- [170] KOKOLAKIS, S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security* 64 (2017), 122–134.

- [171] KOLLNIG, K., SHUBA, A., BINNS, R., VAN KLEEK, M., AND SHADBOLT, N. Are iphones really better for privacy? a comparative study of ios and android apps. *Proceedings on Privacy Enhancing Technologies* (2022).
- [172] KRÖGER, J. L., LUTZ, O. H.-M., AND MÜLLER, F. What does your gaze reveal about you? on the privacy implications of eye tracking. In *IFIP International Summer School on Privacy and Identity Management* (2020), Springer, pp. 226–241.
- [173] KROMBHOLZ, K., HOBEL, H., HUBER, M., AND WEIPPL, E. Advanced social engineering attacks. *Journal of Information Security and applications* 22 (2015), 113–122.
- [174] KROMBHOLZ, K., HUPPERICH, T., AND HOLZ, T. Use the force: Evaluating {Force-Sensitive} authentication for mobile devices. In *Twelfth symposium on usable privacy and security (SOUPS 2016)* (2016), pp. 207–219.
- [175] KU, Y., PARK, L. H., SHIN, S., AND KWON, T. Draw it as shown: Behavioral pattern lock for mobile user authentication. *IEEE Access* 7 (2019), 69363–69378.
- [176] KUMAR, R., KISHORE, S., LU, H., AND PRAKASH, A. Security analysis of unified payments interface and payment apps in india. In *29th USENIX Security Symposium (USENIX Security 20)* (2020), pp. 1499–1516.
- [177] KUMARAGURU, P., AND CRANOR, L. F. Privacy indexes: a survey of westin’s studies.
- [178] LA POLLA, M., MARTINELLI, F., AND SGANDURRA, D. A survey on security for mobile devices. *IEEE communications surveys & tutorials* 15, 1 (2012), 446–471.
- [179] LAKSHMANAN, N., BUDHDEV, N., KANG, M. S., CHAN, M. C., AND HAN, J. A stealthy location identification attack exploiting carrier aggregation in cellular networks. In *30th USENIX Security Symposium (USENIX Security 21)* (2021), pp. 3899–3916.
- [180] LANDER, K., BRUCE, V., AND HILL, H. 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.
- [181] LANZ, L., THIELMANN, I., AND GERPOTT, F. H. Are social desirability scales desirable? a meta-analytic test of the validity of social desirability scales in the context of prosocial behavior. *Journal of Personality* 90, 2 (2022), 203–221.
- [182] LAUGWITZ, B., HELD, T., AND SCHREPP, M. Construction and evaluation of a user experience questionnaire. In *Symposium of the Austrian HCI and usability engineering group* (2008), Springer, pp. 63–76.

- [183] LEE, K., KAISER, B., MAYER, J., AND NARAYANAN, A. An empirical study of wireless carrier authentication for {SIM} swaps. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (2020), pp. 61–79.
- [184] LEI, H., WANG, D., PAN, Z., ZOU, Y., AND WU, K. iscreen: A pure software-based screen privacy protection system for mobile devices. In *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)* (2021), IEEE, pp. 9–16.
- [185] LI, M., MENG, Y., LIU, J., ZHU, H., LIANG, X., LIU, Y., AND RUAN, N. When csi meets public wifi: inferring your mobile phone password via wifi signals. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (2016), pp. 1068–1079.
- [186] LI, Z., MA, F., RATHORE, A. S., YANG, Z., CHEN, B., SU, L., AND XU, W. Wavespy: Remote and through-wall screen attack via mmwave sensing. In *2020 IEEE Symposium on Security and Privacy (SP)* (2020), IEEE, pp. 217–232.
- [187] LIAN, S., HU, W., SONG, X., AND LIU, Z. Smart privacy-preserving screen based on multiple sensor fusion. *IEEE Transactions on Consumer Electronics* 59, 1 (2013), 136–143.
- [188] LIKAMWA, R., LIU, Y., LANE, N. D., AND ZHONG, L. Moodscope: Building a mood sensor from smartphone usage patterns. In *Proceeding of the 11th annual international conference on Mobile systems, applications, and services* (2013), pp. 389–402.
- [189] LIN, J., LIU, B., SADEH, N., AND HONG, J. I. Modeling {Users’} mobile app privacy preferences: Restoring usability in a sea of permission settings. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)* (2014), pp. 199–212.
- [190] LINXEN, S., STURM, C., BRÜHLMANN, F., CASSAU, V., OPWIS, K., AND REINECKE, K. How weird is chi? In *Proceedings of the 2021 chi conference on human factors in computing systems* (2021), pp. 1–14.
- [191] LIPP, M., GRUSS, D., SPREITZER, R., MAURICE, C., AND MANGARD, S. {ARMageddon}: Cache attacks on mobile devices. In *25th USENIX Security Symposium (USENIX Security 16)* (2016), pp. 549–564.
- [192] LIU, B., LIN, J., AND SADEH, N. Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help? In *Proceedings of the 23rd international conference on World wide web* (2014), pp. 201–212.

- [193] LIU, P., ZANG, W., AND YU, M. Incentive-based modeling and inference of attacker intent, objectives, and strategies. *ACM Transactions on Information and System Security (TISSEC)* 8, 1 (2005), 78–118.
- [194] LUO, T., JIN, X., ANANTHANARAYANAN, A., AND DU, W. Touchjacking attacks on web in android, ios, and windows phone. In *International Symposium on Foundations and Practice of Security* (2012), Springer, pp. 227–243.
- [195] LUTAAYA, M., BAIG, K., MAQSOOD, S., AND CHIASSON, S. “i’m not a millionaire”: How users’ online behaviours and offline behaviours impact their privacy. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (2021), pp. 1–7.
- [196] MA, J., YANG, W., LUO, M., AND LI, N. A study of probabilistic password models. In *2014 IEEE Symposium on Security and Privacy* (2014), IEEE, pp. 689–704.
- [197] MACCALLUM, R. C., BROWNE, M. W., AND SUGAWARA, H. M. Power analysis and determination of sample size for covariance structure modeling. *Psychological methods* 1, 2 (1996), 130.
- [198] MACDONALD, S. A., FARZAND, H., ALOTAIBI, N., ISLAM, M. S., AND KHAMIS, M. Change policy or users? mitigating the security risks of thermal attacks.
- [199] MALHOTRA, N. K., KIM, S. S., AND AGARWAL, J. Internet users’ information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.
- [200] MARKY, K., MACDONALD, S., ABDRABOU, Y., AND KHAMIS, M. In the quest to protect users from {Side-Channel} attacks—a {User-Centred} design space to mitigate thermal attacks on public payment terminals. In *32nd usenix security symposium (usenix security 23)* (2023), pp. 5235–5252.
- [201] MARKY, K., SCHMITZ, M., ZIMMERMANN, V., HERBERS, M., KUNZE, K., AND MÜHLHÄUSER, M. 3d-auth: Two-factor authentication with personalized 3d-printed items. In *Proceedings of the 2020 chi conference on human factors in computing systems* (2020), pp. 1–12.
- [202] MARKY, K., STÖVER, A., PRANGE, S., BLECK, K., GERBER, P., ZIMMERMANN, V., MÜLLER, F., ALT, F., AND MÜHLHÄUSER, M. Decide yourself or delegate-user preferences regarding the autonomy of personal privacy assistants in private iot-equipped environments. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (2024), pp. 1–20.

- [203] MARQUES, D., GUERREIRO, T., CARRIÇO, L., BESCHASTNIKH, I., AND BEZNOSOV, K. Vulnerability & blame: Making sense of unauthorized access to smartphones. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (2019), pp. 1–13.
- [204] MARQUES, D., MUSLUKHOV, I., GUERREIRO, T., CARRIÇO, L., AND BEZNOSOV, K. Snooping on mobile phones: Prevalence and trends. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)* (2016), pp. 159–174.
- [205] MATAS, J., GALAMBOS, C., AND KITTLER, J. Robust detection of lines using the progressive probabilistic hough transform. *Computer vision and image understanding* 78, 1 (2000), 119–137.
- [206] MATYUNIN, N., WANG, Y., ARUL, T., KULLMANN, K., SZEFER, J., AND KATZENBEISSER, S. Magneticspy: Exploiting magnetometer in mobile devices for website and application fingerprinting. In *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society* (2019), pp. 135–149.
- [207] MAYRHOFER, R., AND SIGG, S. Adversary models for mobile device authentication. *ACM Computing Surveys (CSUR)* 54, 9 (2021), 1–35.
- [208] MAYRING, P., ET AL. Qualitative content analysis. *A companion to qualitative research* 1, 2 (2004), 159–176.
- [209] McDONALD, N., SCHOENEBECK, S., AND FORTE, A. 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.
- [210] MENG, W., LEE, W. H., MURALI, S., AND KRISHNAN, S. Charging me and i know your secrets! towards juice filming attacks on smartphones. In *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security* (2015), pp. 89–98.
- [211] MITCHELL, M., WANG, A.-I., AND REIHER, P. Cashtags: Prevent leaking sensitive information through screen display. In *Proceedings of the USENIX Security Symposium* (2015), vol. 1.
- [212] MORGADO, F. F., MEIRELES, J. F., NEVES, C. M., AMARAL, A., AND FERREIRA, M. E. Scale development: ten main limitations and recommendations to improve future research practices. *Psicologia: Reflexão e Crítica* 30 (2017).
- [213] MUSLUKHOV, I., BOSHMAF, Y., KUO, C., LESTER, J., AND BEZNOSOV, K. Understanding users’ requirements for data protection in smartphones. In *2012 IEEE 28th international conference on data engineering workshops* (2012), IEEE, pp. 228–235.

- [214] MUSLUKHOV, I., BOSHMAF, Y., KUO, C., LESTER, J., AND BEZNOSOV, K. 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* (2013), pp. 271–280.
- [215] MYAGMAR, S., LEE, A. J., AND YURCIK, W. Threat modeling as a basis for security requirements. In *Symposium on requirements engineering for information security (SREIS)* (2005), vol. 2005, Citeseer, pp. 1–8.
- [216] NARAIN, S., SANATINIA, A., AND NOUBIR, G. Single-stroke language-agnostic key-logging using stereo-microphones and domain specific machine learning. In *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks* (2014), pp. 201–212.
- [217] NARAIN, S., VO-HUU, T. D., BLOCK, K., AND NOUBIR, G. Inferring user routes and locations using zero-permission mobile sensors. In *2016 IEEE Symposium on Security and Privacy (SP)* (2016), IEEE, pp. 397–413.
- [218] NAVEED, S., NAVEED, H., JAVED, M., AND MUSTAFA, M. ”ask this from the person who has private stuff”: Privacy perceptions, behaviours and beliefs beyond weird. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (2022), pp. 1–17.
- [219] NETEMEYER, R. G., BEARDEN, W. O., AND SHARMA, S. *Scaling procedures: Issues and applications*. sage publications, 2003.
- [220] NIEMIETZ, M., AND SCHWENK, J. Ui redressing attacks on android devices. *Black Hat Abu Dhabi* (2012).
- [221] NUNNALLY, J. C. *Psychometric theory*. McGraw-hill, 1967.
- [222] OATES, M., AHMADULLAH, Y., MARSH, A., SWOOPES, C., ZHANG, S., BALEBAKO, R., AND CRANOR, L. F. Turtles, locks, and bathrooms: Understanding mental models of privacy through illustration. *Proceedings on Privacy Enhancing Technologies* 2018, 4 (2018), 5–32.
- [223] OCR, T. Tesseract ocr, 2022. Retrieved February 20, 2022.
- [224] OKTA. Privacy vs. security: Exploring the differences & relationship, 2024. Retrieved March 23, 2025.
- [225] OMETOV, A., LEVINA, A., BORISENKO, P., MOSTOVOY, R., ORSINO, A., AND ANDREEV, S. Mobile social networking under side-channel attacks: Practical security challenges. *IEEE Access* 5 (2017), 2591–2601.

- [226] OPENCV. Eroding and dilating, 2022. Retrieved February 20, 2022.
- [227] OPENCV. Opencv, 2022. Retrieved February 20, 2022.
- [228] OPENCV. Opencv: Canny edge detection, 2022. Retrieved February 20, 2022.
- [229] OPPENHEIMER, D. M., MEYVIS, T., AND DAVIDENKO, N. Instructional manipulation checks: Detecting satisficing to increase statistical power. *Journal of experimental social psychology* 45, 4 (2009), 867–872.
- [230] OWUSU, E., HAN, J., DAS, S., PERRIG, A., AND ZHANG, J. Accessory: password inference using accelerometers on smartphones. In *proceedings of the twelfth workshop on mobile computing systems & applications* (2012), pp. 1–6.
- [231] PHAM, A., DACOSTA, I., LOSIOUK, E., STEPHAN, J., HUGUENIN, K., AND HUBAUX, J.-P. {HideMyApp}: Hiding the presence of sensitive apps on android. In *28th USENIX Security Symposium (USENIX Security 19)* (2019), pp. 711–728.
- [232] PING, D., SUN, X., AND MAO, B. Textlogger: inferring longer inputs on touch screen using motion sensors. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks* (2015), pp. 1–12.
- [233] POR, L. Y., NG, I. O., CHEN, Y.-L., YANG, J., AND KU, C. S. A systematic literature review on the security attacks and countermeasures used in graphical passwords. *IEEE Access* (2024).
- [234] POSSEMATO, A., LANZI, A., CHUNG, S. P. H., LEE, W., AND FRATANTONIO, Y. Clickshield: Are you hiding something? towards eradicating clickjacking on android. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (2018), pp. 1120–1136.
- [235] PROBST, G. 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, 2000.
- [236] PROLIFIC. Prolific | online participant recruitment for surveys and market research, 2021. Retrieved September 01, 2021.
- [237] QUALTRICS. Qualtrics - leading experience management and survey software, 2021. Retrieved February 11, 2021.
- [238] RAGOZIN, K., MARKY, K., LU, J., AND KUNZE, K. Eyemove-towards mobile authentication using eog glasses. In *Augmented Humans 2022*. 2022, pp. 10–14.

- [239] RAGOZIN, K., PAI, Y. S., AUGEREAU, O., KISE, K., KERDELS, J., AND KUNZE, K. 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* (2019), pp. 1–6.
- [240] RAGURAM, R., WHITE, A. M., GOSWAMI, D., MONROSE, F., AND FRAHM, J.-M. ispy: automatic reconstruction of typed input from compromising reflections. In *Proceedings of the 18th ACM conference on Computer and communications security* (2011), pp. 527–536.
- [241] RAYKOV, T. Estimation of composite reliability for congeneric measures. *Applied Psychological Measurement* 21, 2 (1997), 173–184.
- [242] REIPS, U.-D. Standards for internet-based experimenting. *Experimental psychology* 49, 4 (2002), 243.
- [243] RESCORLA, E., AND KORVER, B. Guidelines for writing rfc text on security considerations. Tech. rep., BCP 72, RFC 3552, July, 2003.
- [244] RICKER, T. J., VERGAUWE, E., AND COWAN, N. Decay theory of immediate memory: From brown (1958) to today (2014). *Quarterly Journal of Experimental Psychology* 69, 10 (2016), 1969–1995.
- [245] RIEMAN, J. 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* (1993), pp. 321–326.
- [246] SAAD, A., CHUKWU, M., AND SCHNEEGASS, S. Communicating shoulder surfing attacks to users. In *Proceedings of the 17th International Conference on Mobile and Ubiquitous Multimedia* (2018), pp. 147–152.
- [247] SAAD, A., ELKAFAWY, D. H., ABDENNADHER, S., AND SCHNEEGASS, S. Are they actually looking? identifying smartphones shoulder surfing through gaze estimation. In *ACM Symposium on Eye Tracking Research and Applications* (2020), pp. 1–3.
- [248] SAAD, A., LIEBERS, J., GRUENEFELD, U., ALT, F., AND SCHNEEGASS, S. Understanding bystanders’ tendency to shoulder surf smartphones using 360-degree videos in virtual reality. 1–8.
- [249] SAAD, A., LIEBERS, J., GRUENEFELD, U., ALT, F., AND SCHNEEGASS, S. Understanding bystanders’ tendency to shoulder surf smartphones using 360-degree videos in virtual reality. In *Proceedings of the 23rd International Conference on Mobile Human-Computer Interaction* (2021), pp. 1–8.

- [250] SAENZ, D. Using computer, 2024. Retrieved August 11, 2024.
- [251] SALAZAR, S. Abstract, 2024. Retrieved August 11, 2024.
- [252] SALEH, M., KHAMIS, M., AND STURM, C. What about my privacy, habibi? In *IFIP Conference on Human-Computer Interaction* (2019), Springer, pp. 67–87.
- [253] SAMBASIVAN, N., CHECKLEY, G., BATOOL, A., AHMED, N., NEMER, D., GAYTÁN-LUGO, L. S., MATTHEWS, T., CONSOLVO, S., AND CHURCHILL, E. "privacy is not for me, it's for those rich women": Performative privacy practices on mobile phones by women in south asia. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (2018), pp. 127–142.
- [254] SANNON, S., AND FORTE, A. Privacy research with marginalized groups: what we know, what's needed, and what's next. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–33.
- [255] SCHINKA, J. A., AND VELICER, W. F. *Handbook of Psychology, Developmental Psychology*, vol. 6. John Wiley & Sons, 2003.
- [256] SCHNEEGASS, S., STEIMLE, F., BULLING, A., ALT, F., AND SCHMIDT, A. Smudge-safe: Geometric image transformations for smudge-resistant user authentication. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (2014), pp. 775–786.
- [257] SCHOLAR, G. Shoulder surfing, 2024.
- [258] SCIENCEDIRECT. Side channel - an overview, 2020. Retrieved March 23, 2025.
- [259] SECURITY, H. Android permissions can be dangerous: Full guide to managing them, 2022. Retrieved February 20, 2022.
- [260] SECURITY, N. E. Uniqpass v15 – large password list, 2022. Retrieved February 20, 2022.
- [261] SHI, D., DISTEFANO, C., MCDANIEL, H. L., AND JIANG, Z. Examining chi-square test statistics under conditions of large model size and ordinal data. *Structural Equation Modeling: A Multidisciplinary Journal* 25, 6 (2018), 924–945.
- [262] SHI, E., NIU, Y., JAKOBSSON, M., AND CHOW, R. Implicit authentication through learning user behavior. In *International Conference on Information Security* (2010), Springer, pp. 99–113.
- [263] SHIN, H., SIM, S., KWON, H., HWANG, S., AND LEE, Y. A new smart smudge attack using cnn. *International Journal of Information Security* 21, 1 (2022), 25–36.

- [264] SHUKLA, D., AND PHOHA, V. V. Stealing passwords by observing hands movement. *IEEE Transactions on Information Forensics and Security* 14, 12 (2019), 3086–3101.
- [265] SIMON, L., AND ANDERSON, R. Pin skimmer: inferring pins through the camera and microphone. In *Proceedings of the Third ACM workshop on Security and privacy in smartphones & mobile devices* (2013), pp. 67–78.
- [266] SIMON, L., XU, W., AND ANDERSON, R. Don't interrupt me while i type: Inferring text entered through gesture typing on android keyboards. In *Proceedings of Privacy Enhancing Technologies* (2016), vol. 2016, p. 136–154.
- [267] SLOBOGIN, C. Public privacy: camera surveillance of public places and the right to anonymity. *Miss. LJ* 72 (2002), 213.
- [268] SMITH, G., CARSON, S., VENGURLEKAR, R. G., MORALES, S., TSAI, Y.-C., GEORGE, R., BEDWELL, J., JONES, T., MONDAL, M., SMITH, B., ET AL. "i know i'm being observed:" video interventions to educate users about targeted advertising on facebook. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (2024), pp. 1–27.
- [269] SMITH, H. J., MILBERG, S. J., AND BURKE, S. J. Information privacy: Measuring individuals' concerns about organizational practices. *MIS quarterly* (1996), 167–196.
- [270] SMITH, W., WADLEY, G., WEBBER, S., TAG, B., KOSTAKOS, V., KOVAL, P., AND GROSS, J. J. Digital emotion regulation in everyday life. In *CHI Conference on Human Factors in Computing Systems* (2022), pp. 1–15.
- [271] SNEDECOR, G. W., AND COCHRAN, W. G. Statistical methods, 8th edn. *Ames: Iowa State Univ. Press Iowa* 54 (1989), 71–82.
- [272] SON, S., KIM, D., AND SHMATIKOV, V. What mobile ads know about mobile users. In *NDSS* (2016), Citeseer.
- [273] SONG, C., LIN, F., BA, Z., REN, K., ZHOU, C., AND XU, W. My smartphone knows what you print: Exploring smartphone-based side-channel attacks against 3d printers. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (2016), pp. 895–907.
- [274] SPREITZER, R. Pin skimming: exploiting the ambient-light sensor in mobile devices. In *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices* (2014), pp. 51–62.
- [275] SPREITZER, R., GRIESMAYR, S., KORAK, T., AND MANGARD, S. Exploiting data-usage statistics for website fingerprinting attacks on android. In *Proceedings of the 9th*

- ACM Conference on Security & Privacy in Wireless and Mobile Networks* (2016), pp. 49–60.
- [276] SPREITZER, R., KIRCHENGAST, F., GRUSS, D., AND MANGARD, S. Procharvester: Fully automated analysis of proofs side-channel leaks on android. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security* (2018), pp. 749–763.
- [277] SPREITZER, R., PALFINGER, G., AND MANGARD, S. Scandroid: Automated side-channel analysis of android apis. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks* (2018), pp. 224–235.
- [278] SRSRAN. srsran - your own mobile network, 2022. Retrieved February 20, 2022.
- [279] STANGOR, C., AND WALINGA, J. *Introduction to psychology*. BCcampus, 2014.
- [280] STATISTA. Global smartphone penetration rate as share of population from 2016 to 2023, 2024.
- [281] STATISTA. Number of smartphone users in the uk 2020-2029, 2024.
- [282] STATISTA. Smartphones in the uk, 2024.
- [283] TAJIK, K., GUNASEKARAN, A., DUTTA, R., ELLIS, B., BOBBA, R. B., ROSULEK, M., WRIGHT, C. V., AND FENG, W.-C. Balancing image privacy and usability with thumbnail-preserving encryption. *IACR Cryptol. ePrint Arch. 2019* (2019), 295.
- [284] TANG, B., WANG, Z., WANG, R., ZHAO, L., AND WANG, L. Niffler: A context-aware and user-independent side-channel attack system for password inference. *Wireless Communications and Mobile Computing 2018* (2018).
- [285] TANG, B. J., AND SHIN, K. G. {Eye-Shield}:{Real-Time} protection of mobile device screen information from shoulder surfing. In *32nd USENIX Security Symposium (USENIX Security 23)* (2023), pp. 5449–5466.
- [286] TIEFENAU, C., HÄRING, M., GERLITZ, E., AND VON ZEZSCHWITZ, E. Making privacy graspable: Can we nudge users to use privacy enhancing techniques? *arXiv preprint arXiv:1911.07701* (2019).
- [287] TOURANGEAU, R., AND YAN, T. Sensitive questions in surveys. *Psychological bulletin* 133, 5 (2007), 859.
- [288] TRULL, T. J., AND EBNER-PRIEMER, U. W. Using experience sampling methods/e-ecological momentary assessment (esm/ema) in clinical assessment and clinical research: introduction to the special section.

- [289] TSALIS, N., VASILELLIS, E., MENTZELIOTI, D., AND APOSTOLOPOULOS, T. A taxonomy of side channel attacks on critical infrastructures and relevant systems. In *Critical Infrastructure Security and Resilience*. Springer, 2019, pp. 283–313.
- [290] ULQINAKU, E., MALISA, L., STEFA, J., MEI, A., AND ČAPKUN, S. Using hover to compromise the confidentiality of user input on android. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (2017), pp. 12–22.
- [291] VERGÉS, A. On the desirability of social desirability measures in substance use research. *Journal of Studies on Alcohol and Drugs* 83, 4 (2022), 582–587.
- [292] VISHWAMITRA, N., KNIJNENBURG, B., HU, H., KELLY CAINE, Y. P., ET AL. Blur vs. block: Investigating the effectiveness of privacy-enhancing obfuscation for images. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops* (2017), pp. 39–47.
- [293] VON GIOI, R. G., JAKUBOWICZ, J., MOREL, J.-M., AND RANDALL, G. Lsd: A fast line segment detector with a false detection control. *IEEE transactions on pattern analysis and machine intelligence* 32, 4 (2008), 722–732.
- [294] VON ZEZSCHWITZ, E., DE LUCA, A., BRUNKOW, B., AND HUSSMANN, H. Swipin: Fast and secure pin-entry on smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (2015), pp. 1403–1406.
- [295] VON ZEZSCHWITZ, E., EBBINGHAUS, S., HUSSMANN, H., AND DE LUCA, A. You can’t watch this! privacy-respectful photo browsing on smartphones. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (2016), pp. 4320–4324.
- [296] WANG, G., ZHAO, J., KOLLNIG, K., ZIER, A., DURON, B., ZHANG, Z., VAN KLEEK, M., AND SHADBOLT, N. Koala hero toolkit: A new approach to inform families of mobile datafication risks. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (2024), pp. 1–18.
- [297] WANG, G., ZHAO, J., VAN KLEEK, M., AND SHADBOLT, N. Informing age-appropriate ai: Examining principles and practices of ai for children. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (2022), pp. 1–29.
- [298] WANG, J., GAO, B., TU, H., LIANG, H.-N., LIU, Z., LUO, W., AND WENG, J. Secure and memorable authentication using dynamic combinations of 3d objects in virtual reality. *International Journal of Human–Computer Interaction* (2023), 1–19.

- [299] WATANABE, T., AKIYAMA, M., AND MORI, T. {RouteDetector}: Sensor-based positioning system that exploits {Spatio-Temporal} regularity of human mobility. In *9th USENIX Workshop on Offensive Technologies (WOOT 15)* (2015).
- [300] WERMKE, D., WÖHLER, N., KLEMMER, J. H., FOURNÉ, M., ACAR, Y., AND FAHL, S. Committed to trust: A qualitative study on security & trust in open source software projects. In *2022 IEEE symposium on Security and Privacy (SP)* (2022), IEEE, pp. 1880–1896.
- [301] WESTIN, A. F. Privacy and freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.
- [302] WILLIAMSON, J. R. *User experience, performance, and social acceptability: usable multimodal mobile interaction*. PhD thesis, University of Glasgow, 2012.
- [303] WISNIEWSKI, P. J., KNIJNENBURG, B. P., AND LIPFORD, H. R. Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of human-computer studies* 98 (2017), 95–108.
- [304] WOODRUFF, A., PIHUR, V., CONSOLVO, S., BRANDIMARTE, L., AND ACQUISTI, A. Would a privacy fundamentalist sell their dna for \$1000 nothing bad happened as a result? the westin categories, behavioral intentions, and consequences. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)* (2014), pp. 1–18.
- [305] WORTHINGTON, R. L., AND WHITTAKER, T. A. Scale development research: A content analysis and recommendations for best practices. *The counseling psychologist* 34, 6 (2006), 806–838.
- [306] WU, C., HE, K., CHEN, J., AND DU, R. Icauth: Implicit and continuous authentication when the screen is awake. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)* (2019), IEEE, pp. 1–6.
- [307] YAN, L., GUO, Y., CHEN, X., AND MEI, H. A study on power side channels on mobile devices. In *Proceedings of the 7th Asia-Pacific Symposium on Internetwork* (2015), pp. 30–38.
- [308] YANG, L., ZHI, Y., WEI, T., YU, S., AND MA, J. Inference attack in android activity based on program fingerprint. *Journal of Network and Computer Applications* 127 (2019), 92–106.
- [309] YE, G., TANG, Z., FANG, D., CHEN, X., KIM, K. I., TAYLOR, B., AND WANG, Z. Cracking android pattern lock in five attempts. In *Proceedings of the 2017 Network and Distributed System Security Symposium 2017 (NDSS 17)* (2017), Internet Society.

- [310] YONG, A. G., PEARCE, S., ET AL. A beginner's guide to factor analysis: Focusing on exploratory factor analysis. *Tutorials in quantitative methods for psychology* 9, 2 (2013), 79–94.
- [311] YU, X., WANG, Z., LI, Y., LI, L., ZHU, W. T., AND SONG, L. Evopass: Evolvable graphical password against shoulder-surfing attacks. *Computers & Security* 70 (2017), 179–198.
- [312] YUE, Q., LING, Z., FU, X., LIU, B., REN, K., AND ZHAO, W. Blind recognition of touched keys on mobile devices. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (2014), pp. 1403–1414.
- [313] ZHANG, J., TANG, Z., LI, M., FANG, D., CHEN, X., AND WANG, Z. Find me a safe zone: A countermeasure for channel state information based attacks. *Computers & Security* 80 (2019), 273–290.
- [314] ZHANG, J., ZHENG, X., TANG, Z., XING, T., CHEN, X., FANG, D., LI, R., GONG, X., AND CHEN, F. Privacy leakage in mobile sensing: Your unlock passwords can be leaked through wireless hotspot functionality. *Mobile Information Systems 2016* (2016).
- [315] ZHANG, N., SUN, K., SHANDS, D., LOU, W., AND HOU, Y. T. Truspy: Cache side-channel information leakage from the secure world on arm devices. *Cryptology ePrint Archive* (2016).
- [316] ZHANG, S., MA, D., AND WANG, Y. Don't peek at my chart: Privacy-preserving visualization for mobile devices. In *Computer Graphics Forum* (2023), vol. 42, Wiley Online Library, pp. 137–148.
- [317] ZHANG, X., WANG, X., BAI, X., ZHANG, Y., AND WANG, X. Os-level side channels without procfs: Exploring cross-app information leakage on ios. In *Proceedings of the Symposium on Network and Distributed System Security* (2018).
- [318] ZHANG, X., XIAO, Y., AND ZHANG, Y. Return-oriented flush-reload side channels on arm and their implications for android devices. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (2016), pp. 858–870.
- [319] ZHENG, H., AND HU, H. Missile: A system of mobile inertial sensor-based sensitive indoor location eavesdropping. *IEEE Transactions on Information Forensics and Security* 15 (2019), 3137–3151.
- [320] ZHOU, H., TEARO, K., WAJE, A., ALGHAMDI, E., ALVES, T., FERREIRA, V., HAWKEY, K., AND REILLY, D. Enhancing mobile content privacy with proxemics aware notifications and protection. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (2016), pp. 1362–1373.

- [321] ZHOU, W., ZHANG, X., AND JIANG, X. Appink: watermarking android apps for repackaging deterrence. In *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security* (2013), pp. 1–12.
- [322] ZHOU, W., ZHOU, Y., JIANG, X., AND NING, P. Detecting repackaged smartphone applications in third-party android marketplaces. In *Proceedings of the second ACM conference on Data and Application Security and Privacy* (2012), pp. 317–326.
- [323] ZISSERMAN, A. The svm classifier, 2015. Retrieved February 20, 2022.
- [324] ZOU, Y., ROUNDY, K., TAMERSOY, A., SHINTRE, S., ROTURIER, J., AND SCHAUB, F. Examining the adoption and abandonment of security, privacy, and identity theft protection practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020), pp. 1–15.