ENHANCING MOBILE CONTENT PRIVACY WITH PROXEMICS AWARE NOTIFICATIONS AND PROTECTION

by

Huiyuan Zhou

Submitted in partial fulfilment of the requirements
for the degree of Master of Computer Science

at

Dalhousie University
Halifax, Nova Scotia
November 2015

Dedication

I dedicate this thesis to:

My mother, ***Xiuying Zhang****, a brave and strong woman who sacrificed her own needs to offer me unconditional love and support throughout my life. I wish I could repay her tremendous love and make her happier.*

My father, ***Changsheng Zhou****, a generous and sympathetic man who inspired my motivation for achievement with high expectations and was proud of me all the time. He passed away 8 years ago. I hope every step that I take would make him proud.*

My extended family members, who have witnessed my growth, accompanied me through happy and dark times. The ways you've cared about and supported me, I will never forget.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Given the widespread adoption of mobile devices and the private personal and work information they carry, casual or deliberate shoulder surfing is an increasing concern with these devices. We iteratively designed a tablet interface that detects when people nearby are looking at the screen, providing awareness through glyph notifications, and response through visual protections, and evaluated its use in two experimental simulations. The results indicate that mobile content privacy management systems such as ours could help alleviate the cognitive and social burden of managing mobile device privacy in dynamic settings. We identify physical privacy behaviours, practices and preferences that can inform the design of privacy notification and management protocols on mobile devices. We argue that such systems require *subtlety* so as not to advertise the users' intention for privacy, *flexibility* in addressing dynamic privacy needs, *trustworthiness* to promote adoption, and *socio-cultural awareness* to be socially appropriate for both users and onlookers.

LIST OF ABBREVIATIONS USED

BYOD	Bring Your Own Device
CAD	Computer-Aided Detection
EHR	Electronic Health Record
G	Group
GS	Grayscale
HR	Human Resources
MMC	Markerless Motion Capture
NN	No Notification No Protection
NY	No Notification Yes Protection
P	Participant
PAC	Picture Archiving and Communication
PET	Privacy Enhancement Technologies
SH	Selective Hiding
SMS	Short Message Service
WOz	Wizard of Oz
YN	Yes Notification No Protection
YY	Yes Notification Yes Protection

ACKNOWLEDGEMENTS

I would like to acknowledge and thank several key individuals and institutions without whose assistance and support this research endeavor would not have been possible.

First, I would like to express my utmost gratitude to my supervisor **Dr. Derek Reilly** for being a brilliant supervisor, mentor and partner. I have been impressed by your ability of thinking creatively, working tirelessly, and communicating effectively, as well as your optimistic, approachable, humorous and patient personality. I have also learned from your excellent leadership skills in leading by example, working under pressure, multi-tasking, and motivating team members. Your firm guidance and constructive feedback have been inestimable for my research. Thank you for being so inspiring, generous and supportive for my whole graduate study.

Dr. Kirstie Hawkey, my co-supervisor during my earlier research, has provided me with invaluable knowledge, guidance and feedback. I was fascinated by your diligent research, broad perspective, and initiatives of offering lively and interesting courses to all your students. Thanks for all your support for my research.

I would like to thank my examining committee members **Dr. Bonnie MacKay** and **Dr. Sageev Oore** who were more than generous with their expertise and precious time. Thank you for agreeing to serve on my committee and all the helpful reviews.

I would also like to thank **Dr. Srini Sampalli**, **Dr. Denis Riordan, Dr. Nauzer Kalyaniwalla** and **Dr. Yannick Marchand** for your trust in me as a teaching assistant and providing me opportunities to help students and build my teaching skills. Thanks to **Dr. Stephen Brooks** for your feedback and advice. Thanks to **Dr. Evangelos E. Milios** for supporting the administrative aspects as the graduate coordinator of the Faculty of Computer Science. Thank **Raghav Sampangi** for generously sharing your teaching experiences and materials.

A big thanks to **Vinicius Ferreira** and **Thamara Silva Alves** for developing the prototype used in my research; **Khalid Tearo, Aniruddha Waje** and **Elham Alghamdi** for helping conduct my lab study and data analysis. I would never forget how we worked together until early in the morning and how we made it through the snow during the worst winter weather to not miss a group of participants.

My special thanks go to **Gang Hu** who is an outstanding listener and problem solver with a sincere heart and constructive suggestions, and all members of the GEM lab: **Mohamad Salimian**, **Majid Nasirinejad**, **Mohammed Alnusayri**, **Nabil Hannan, Swapnil Mahajian**, **Aisha Edrah**, **Aaquib Mohammed**, **Karan Sharma**, **Xihe Gao,**

Xiaoting Hong, and **Lingbo Zou**. You guys are an excellent group of people and a big family to work and hang out with. I have been lucky to have you around during my graduate years.

Thanks to **Paul Hardman** from the Writing Center of Dalhousie University for your help, patience and encouragement with the English writing in my paper and thesis. Thanks to **Barbara Borden** for your kindness and smiles.

Thanks to all my roommates, especially **Yue Liu**, **Hankun Zhang** and **Yue Du**. You guys have made my time in Halifax very warm, special and extraordinary. Thanks to all my family and friends for supporting my decisions, being compassionate and caring. I love you all.

Finally, I was fortunate to receive funding from the BRAVA project supported by Boeing and Mitacs, the Boeing Mobile Graphics project, the Faculty of Computer Science and Graduate Studies at Dalhousie University, and the Computing Research Association-Women (CRA-W).

CHAPTER 1 INTRODUCTION

1.1 PROBLEM DEFINITION

Given the explosive growth of the mobile device market and the popularity of large screen smartphones, tablets, and subnotebooks, shoulder surfing has moved off the laptop and onto mobile devices. In the US people spend more time on average using mobile devices than desktop computers [25]. Mobile devices often carry sensitive or personal data, and their mobility means that such data can be accessed in environments that carry a real or indeterminate threat to privacy. Thompson [94] surveyed 800 professionals and found that for organizations, sensitive data such as internal financials (42%), private HR (Human Resources) information (33%) and trade secrets (32%) were the most commonly accessed data outside the office. Surveys indicate growing concern about the privacy of personal information such as passwords, emails and text messages on smartphones [69]. At the same time, 72% of office commuters in the UK admit to looking over their neighbours' shoulders on the bus or train [84]. Similar behaviours occur in queues, at cafes, and in dynamic, semi-public workplaces such as hospital wards.

From a traditional **social and interpersonal** perspective, privacy, defined by Altman as "*selective control of access to the self*", concerns controlling the desired level of one's accessibility to others, or interaction with others [4]. Contemporaneous social research identified interpersonal privacy management behaviours such as verbal and nonverbal communication, and the maintenance of personal space, territory and cultural norms [4]. For example, people may block, turn away, or move in response to intruders in close proximity [73].

From an **information control** perspective, one of the most acknowledged view proposed by Westin defined privacy as "*the claims of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is*

communicated to others" [101]. According to Langheinrich [61], the focus of privacy issues evolve with changes in technology: starting from earlier punishing peeping and eavesdropping behaviour (media privacy), to the advocate of private property (territory privacy), to the invention of telephone (communication privacy) and finally to the electronicized and digitized modern society (information privacy). Lee [63] viewed privacy research as to defend against new opportunities technology has brought for intrusion: solitude against pervasive viruses and spams, anonymity against the Internet's tracking and exposing abilities, autonomy against data mining, sharing etc.

Integrating both perspectives, Ackerman and Mainwaring [2] defined privacy as "*individuals' capabilities in a particular social situation to control what they consider to be personal data*" which highlighted the role of information control, individual subjectivity and social implications in privacy. This research focuses on the shoulder surfing problems (when someone nearby happens to see your information without your permission) on mobile devices. The privacy in this context is also a social concern, but the focus shifts from self-other interaction to self-device-other interaction. It also involves information control, but the focus is on hiding on-screen content of mobile devices. We therefore define ***mobile content privacy*** as "individuals' capabilities in a social situation to control the accessibility of visual information to others on mobile devices."

As with interpersonal privacy, mobile content privacy could be managed by *physical* means. Taking advantage of spatial elements of the built environment is one basic way to do this [70]. For example, in a library mobile content privacy could be managed by moving from a busy foyer to a quiet alcove. However, mobile devices are also physically manipulated relative to the user (e.g., moved, tilted) to preserve privacy. Luff and Heath argue that "*micro-mobility*"—the way artefacts and objects can be subtly placed, mobilized and interwoven into interactions—is critical for collaboration [64]. There is currently little understanding of the role that a device's micro-mobility can play in mobile content privacy.

Mobile content privacy can also be managed through the device itself *digitally*. Possible approaches can be classified and understood using Brunk's privacy framework, in which privacy management is seen as an ongoing process of awareness, prevention, detection, response and recovery [20]. For example, hardware privacy filters that limit screen visibility to a small range from perpendicular [80], and indirect password entry schemes such as Convex Hull Click scheme [102] and gaze-based input methods [59] provide *prevention*, however the user must maintain *awareness* of when it should be used (not when sharing content, for example). When the privacy characteristics of a setting are fluid, or when an individual accesses information across a range of settings, solutions that focus on *awareness, detection* and *response* may be useful. Portnoff et al showed notifications (e.g., on-screen icons, LED lights) could raise users' awareness of privacy-related events such as unexpected webcam recording [78]. Tarasewich et al. designed privacy blinders that could cover specific types of data (e.g., banking numbers) with opaque squares [92] in response to a perceived or real threat to privacy. For mobile content privacy management, a system that detects shoulder surfing could trigger just-in-time notifications or protection mechanisms. Moreover, as the possibility of mobile content privacy breach highly depends on the shoulder surfers' spatial proximity and looking directions relative to the device, proxemic interactions [42] which exploit spatial relationships such as distance, orientation are particularly appropriate for dynamic privacy breach detection and management. While proof of concept prototypes of proxemics-based content privacy interfaces using markers [18] or a fusion of camera and other sensor data [62] have been demonstrated, it is not clear how people respond to and use such systems.

Taking one step further, we wondered how physical privacy management behaviours are used to maintain mobile content privacy, how digital privacy management systems with shoulder-surfing awareness, detection and response could be integrated into existing privacy management mechanisms (e.g. tilting the device, facing another direction), and how mobile content privacy management might differ in individual vs. collaborative tasks [22].

1.2 THESIS CONTRIBUTION

We explored the design space of mobile content privacy management systems by designing notification and protection alternatives and evaluating them with Wizard of Oz (WOz) methodology in the field. By using various privacy-related scenarios, we maximized the stimulus and collected rich qualitative feedback on advantages and disadvantages of each design and user's expectation of how the system works. An informal interview with two healthcare professionals highlighted the implications of system design in work-related contexts.

With the support of a portable motion tracking system, we were able to track the spatial information (i.e., position and orientation) of both mobile devices and potential shoulder surfers. We implemented a working proof-of-concept prototype to instantiate the proposed proxemic-interaction-mediated privacy management system: the prototype monitors the relative distance and orientation between a tablet and a designated onlooker in real time. When the onlooker approaches the tablet and is oriented towards the tablet, a glyph notification will pop up on the tablet to alert the user and / or a protection (e.g., the screen brightness turns down) will be applied to the contents to defend against the shoulder surfing event.

In a follow-up study, we evaluated the prototype in the lab with 26 participants performing both individual tasks and collaborative tasks while experiencing different combinations of notifications and protection techniques. We observed participants' privacy management behaviours without and with the digital system, and compared participants' attitudes toward the proposed digital system and existing physical mechanisms. We further explored the relationship between privacy management elements, between physical and digital privacy management, and between individual and collaborative scenarios.

This thesis work contributes to the fields of content privacy management of ubiquitous systems, proxemic interaction, privacy enhancement technology and personal / collaborative information management. The contributions are as follows:

Theoretical Contribution:

- Explore how digital interfaces could support dynamic mobile content privacy management when prevention privacy strategies are not available
- Provide a classification to understand physical mobile privacy management behaviours and show very obvious privacy behaviours are seldom used in real-life scenarios
- Show digital techniques for mobile content privacy management are useful when physical management is constrained by cognitive capacity and/or social norms
- Explain divergent privacy preferences of digital privacy systems (e.g., notification and protection) from a holistic privacy management perspective
- Examine mobile content privacy management at the small group level and identify the challenges of maintaining task efficiency and accommodating potential conflicting needs of multiple users

Design Exploration:

- Design a number of alternatives of privacy notifications and protection techniques and evaluate them in both personal and work-related contexts
- Implement a proof-of-concept prototype that demonstrates how proxemics behaviours can be mediated for privacy management on mobile devices
- Evaluate the working prototype with plausible real-life privacy scenarios and show that the digital privacy system, although it doesn't alter people's physical privacy behaviours, it does improve perceived awareness, privacy, and satisfaction
- Develop design guidelines for mobile content privacy management systems

1.3 THESIS OVERVIEW

Chapter 2 presents a background of related work. We begin with defining the connotation of mobile content privacy, summarizing end users' mobile privacy concerns and privacy management models. We describe frameworks of how people regulate privacy with physical and behavioural mechanisms. We then list digital privacy notifications and

protection techniques and proxemics interactions that mediate privacy management. In addition, we discuss the pitfalls and solutions of evaluating privacy in a lab setting.

In Chapter 3, we present the design exploration process that motivates our study. We first designed a number of candidates of on-screen glyph notifications as well as protection techniques that leverage visual attributes of content. We then used Wizard of Oz methodology to evaluate the design alternatives with 12 participants. Initial results and discussion about strengths and weaknesses of the design candidates and design implications are explained. We also collected design feedback from two healthcare professionals to further our understanding in an applied context. At the end, a proof-of-concept implementation of the proposed privacy management interface is specified.

In Chapter 4, with informed choices from the outcome of the design exploration, we select one notification design and two protection techniques and present the research questions and study design of a lab evaluation of the proof-of-concept prototype with 26 participants. We explain the study procedure, setting, tasks and data analysis in detail.

Chapter 5 presents the results of the lab evaluation including participants' privacy perceptions, validity of the study design, how participants physically manage mobile content privacy, the impact of our digital privacy system on both privacy perceptions and behaviours of participants, and discuss privacy management at a small-group level.

Chapter 6 discusses a holistic perspective of privacy management, trust issues and cultural implications of digital system designs. We then present design feedback about notification, protection and the whole system and derive design guidelines for mobile content privacy. Finally we justify our lab approach and outline the limitations of the current study as well as recommendations for future work.

Finally, Chapter 7 looks back at this thesis work, summarizes the findings, and highlights the theoretical and applied implications of this research.

CHAPTER 2 REVIEW OF LITERATURE

We present in this chapter related work to the topic of mobile content privacy. We first discuss content privacy in a mobile device context and privacy management models. We then review existing physical and digital privacy management mechanisms, and how proxemic information could be exploited to string together multiple privacy management processes. Finally we examine some pitfalls in evaluating privacy in a lab setting. These reviews server as the foundation of our preliminary design exploration in the next chapter.

2.1 CONTENT PRIVACY IN UBIQUITOUS COMPUTING CONTEXT

2.1.1 Mobile Content Privacy

Shoulder surfing happens in a physical setting by direct observation from other people on information from ATM, desktop computers, or other devices' screens. Defending against shoulder surfing concerns how ephemeral on-screen *visual* information is managed and controlled by the user. Boyle et al. identified two privacy control strategies in media space: *access* control (e.g., authentication, authorization) and *content* control (e.g., directly remove sensitive information from media) [15]. In this sense, the privacy issues discussed in this thesis concern on-screen content privacy. Hawkey et al. explored incidental information privacy (e.g., users' traces of past activities such as search engine queries incidental to current task but visible by casual viewing of collaborators / bystanders) management on web browsers [51]. Incidental information privacy also involves visual information and a second screen viewer, but differs in that the private information at risk is irrelevant to the users' task and users expect others to look at a shared screen in some occasions. The onlookers are passive to the information disclosure. Our work, on the other hand, concerns users dealing with private information as their

primary tasks and are often not aware of their surroundings and the moment shoulder surfing occurs. Onlookers could be intentional (active) or passive to the disclosure.

A traditional line of research concerns defensive mechanisms on password (e.g., graphical password) inputting schemas that are by nature visual and more vulnerable to shoulder surfing attack) [102, 39]. Almaula pinpointed two principal approaches as obfuscating presented information and/or obfuscating user input (e.g., introduce noise into input or output) [3]. However, these approaches focus on short-term inputting process and might not be easily applied to a wider range of contents such as ordinary texts and images.

Moreover, the media that the information is situated in also matters. Physical privacy management with fixed devices (e.g. desktop, large display, projection) is relatively hard because fixation restricts the way people can arrange space to maintain privacy. As the screen size of the devices gets larger, the visibility increases. Thus they are more likely to be used for sharing and collaboration purposes and less for displaying private data. Mobile devices' portability opens possibilities of more diverse physical management. In addition, mobile devices are often used in casual and social situations. Traditional interpersonal privacy could be managed by boundary negotiation (e.g., mutual awareness of both parties to regulate privacy) [4, 18]. It's not clear how the way people manage device privacy would affect social interaction between users and others.

2.1.2 Privacy Concerns for Mobile Devices

Regarding personal information privacy, Chin et al. (2012) investigated 60 smartphone users (age >18, age and gender balanced) and found that security concerns made users less willing to perform financial tasks such as banking and shopping, or to access private data such as social security numbers and health records on their smartphones than on laptops [23]. Moreover, users have more privacy concerns related to personal information such as location, photo sharing and text messaging when using their phone vs. their laptop. Muslukhov et al. (2013) surveyed more than 700 smartphone users (mean age =

25.6, 51% male, average annual income = $43k) [69]. Most were concerned about passwords, email, SMS messages, data in social networking applications, and photos and videos. In relation to friends and family, users are more concerned about unauthorized access to SMS messages, call history, browsing and search history; for strangers, users are more concerned about contact details and progress in games. Tablets are larger than smartphones, making them more visible and more prone to privacy breach. Privacy concerns regarding tablet use have been underexplored. In organizational settings, according to surveys in a white paper for visual data security [98], 45% of companies have adopted a Bring Your Own Device (BYOD) strategy, two thirds of 2010 office workers in UK worked 2 extra hours often while commuting, and 38% US employees claimed it would be impossible to work without mobile access to emails.

For a more general web usage, Radke et al. [83] identified three tiers of information in terms of users' perceived level of security importance: the top level was online finances information; the second level was medical information. Participants in the 45+ age group concerned about traces of searches for medical conditions being recorded and linked back to them; the third level was personal information such as physical address, telephone number, and children's details such as photos, names and schools.

We chose finance scenarios for both our studies for the unanimous high security and privacy concerns from the users. We also used scenarios of social media chat, viewing health records and photos in our first study to explore the effectiveness of our designs in diverse privacy contexts.

2.1.3 Privacy Management Models

Schneier recognized four types of solutions to address network security vulnerabilities and breaches: prevention, detection, response and recovery [88]. Schneier argued that prevention systems were not perfect and risk management should be achieved through better process such as detection and response. Brunk examined 1,241 features of 133 privacy solution software tools with content analysis and expanded Schneier's

categorization by adding one more "awareness" category [19]. According to Brunk, awareness features communicate information about the status which servers the foundation for all other privacy processes (see Figure 1); prevention features took precaution measures; detection features search for potential problems in an active way; response features took action after detecting a problem; and recovery features help restore status to normal. The number of prevention features were prevailing. Brunk also claimed security and privacy features usually intertwined to be separate from each other.

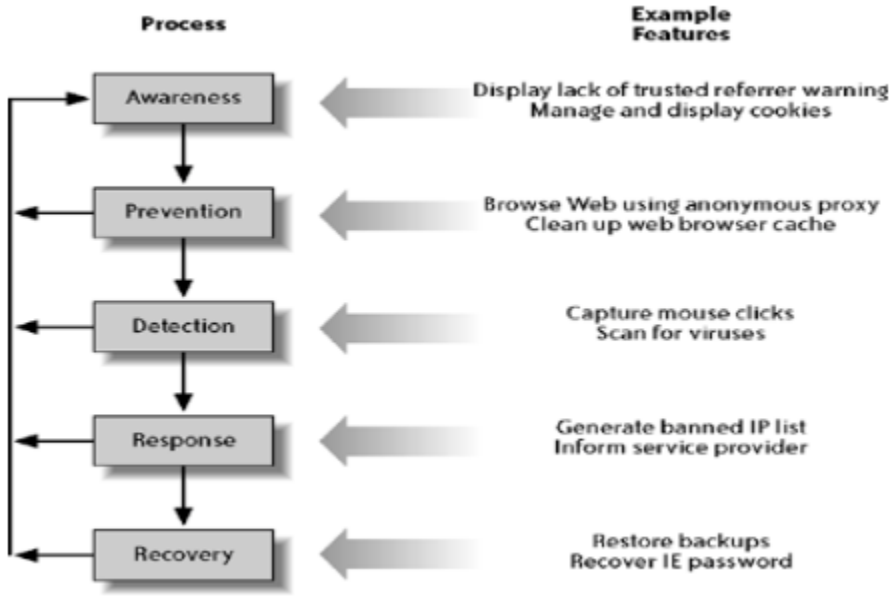


Figure 1 The privacy space framework as a process. Figure from [20]

Tools intended to promote privacy are sometimes called Privacy Enhancement Technologies (PET). In the field of identity management, PET focus on meeting 4 core ISO requirements: anonymity, pseudonymity, unlinkability and unobservability [66]. According to Pfitzmann and Hansen [75], anonymity refers to "not identifiable within a set of subjects"; *pseudonymity* means using an identifier other than subject's real names; *unlinkability* refers to an attacker not being able to relate two or more items of interest; *unobservability* means invisibility of item of interest to uninvolved subjects and anonymity to involved subjects. As our privacy scenarios (e.g., chat, health record) included personal identifiable information (e.g., names, pictures), one of our mechanism designs (Selective Hiding) adopted anonymity by anonymizing sensitive information by

generic pictures, name initials or "x". We should note that content privacy in our work refers to the privacy of the person the content is about. It is not necessarily the device user's privacy (e.g., a doctor's tablet may carry patients' privacy).

2.2 PHYSICAL PRIVACY MANAGEMENT

2.2.1 Physical Privacy management in day-to-day life

In Altman's theory, non-verbal behaviours for regulating privacy are exhibited by the facial expression, posture, position, orientation, and movement of people's own body whereas use of personal space (defined as "*area immediately surrounding persons and groups, distance and angle of orientation from others*") and territory behaviour ("*use, possession, and ownership of areas and objects in a geographical locale*") are implemented in relation to their environment (referred to as environmental behaviour in Altman's dialectic model of privacy regulation [6]). Moreover, mix of multiple behavioural mechanisms are possible and varied based on social relationships (e.g., family vs stranger). These physical behaviours are relevant when looking at how people manage the physical privacy of the information revealed from their mobile devices as on-screen privacy could be achieved through regulating self-other privacy (e.g., move away from others, close a door). People could also manipulate mobile devices easily as they move their body parts. Table 1 summarized Altman and Chemers' behavioural mechanisms used to manage privacy [21]:

Table 1 Behavioural mechanisms for privacy management. Table from [21].

Table 1. Behavioral mechanisms used to regulate privacy.

Behavioral Mechanism	Definition	Examples
Verbal	the contents of what a person says	Saying: • "Let's talk" • "Can I raise an issue with you" • "Sorry, I'm too busy now" • "No, I can't make it this evening"
Para Verbal	way of speaking, how someone says something	Speaking in a cool or warm tone
Non Verbal	communication without words including posture, gaze, facial expressions and gestures	• body orientation • turning away • smiling • grimacing • frowning • looking away • fidgeting with own clothing • rubbing own hands together • looking at our watches • assuming rigid, symmetrical body positions

Personal Space	"the space within an invisible boundary around people that is with them everywhere they go." (Altman & Chemers, 1980, p. 102)	• increase or decrease physical distance between self and another person
		  ○ by backing away
		  ○ by moving closer

Territory	control and ownership of a place by a person or group	• invite someone into a territory they occupy • closing a door • use signs saying keep out or welcome • offering a chair • providing refreshments • not inviting in
Culture	customs, rules and norms which communicate availability to other members in the same culture	• not dropping by a friend's house at dinner time • too early in the morning or too late at night avoiding • coming to parties too early and leaving at a reasonable hour • not opening shut doors (at least without knocking) etc.)

(Altman & Chemers, 1980; Altman, 1975)

Caine conducted an archival analysis from previous focus group data and categorized everyday privacy behaviours into three types: **avoidance behaviours** ("*not performing an originally intended action because of privacy concerns and engaging in a behaviour to avoid a situation where privacy would be an issue*", e.g., avoid using device, selective sharing content and recipient), **modification behaviours** ("*performing an action but not*

in the originally intended manner", e.g., being careful, not doing in front of others, being vague, quietly, use code or different language) and **alleviatory behaviours** ("*taking actions to prevent the spread of information, reduce consequences and determine whether further steps needs to be taken*", e.g., limiting distribution, destroying evidence, checking) [21]. Avoidance behaviour was found to be the most common type and modification behaviour was most reported in heath disclosure scenario. This model provided a high-level understanding of behaviours related to different privacy processes. Mobile content privacy could be managed through avoidance (e.g., switch to a non-sensitive window), modification (e.g., move the device out of line of sight of other people), and alleviatory (e.g., change passwords after potential privacy breach) behaviours. However, this classification lacks the detail of how, for example, behaviours could be actually modified to maintain mobile content privacy.

Another body of research emphasized on behaviours concerns behavioural mechanisms against spatial intrusion. For example, Ashcraft et al. found people claimed their territory through defensive behaviours such as maintaining a fixed interpersonal distance, staring/glaring at the intruder, using body parts such as arms, legs and backs to form temporary barrier, using objects such as furniture as barrier, maintaining characteristic posture (e.g., akimbo position with legs spread apart, both hands placed on hips) to block vision and physical access to the inner group), and verbally warn the intruder to regulate intrusion [8]. Patterson et al. also found as the intruder got closer, people demonstrated more nonverbal behaviours such as moving location, glancing, blocking, leaning or turning away etc. [73]. As people use mobile devices in close proximity to their bodies, these behaviours against spatial intrusion could easily be adapted to maintain mobile privacy.

2.2.2 Physical Privacy Management in Organizations

In organizational settings, people strategically manage physical spaces to achieve privacy. For example, Dourish et al. reported how administrative assistants position their computer screens in a way that circumvents the vision of visitors, and how seats and

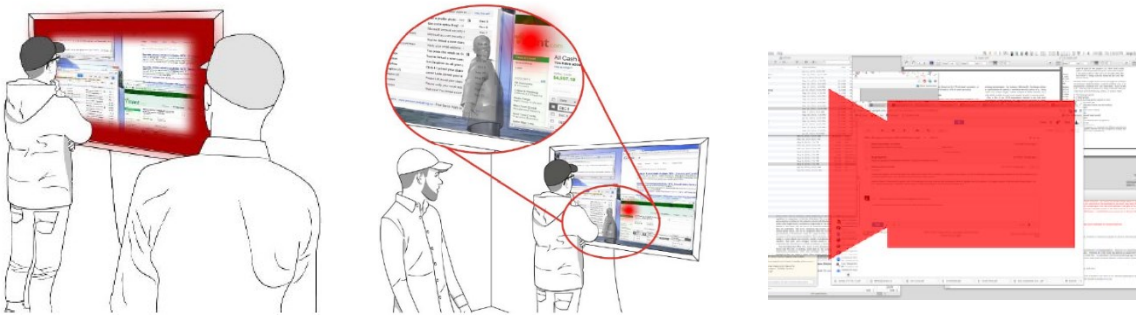
desks were placed as barriers that separate public part and private part of the office, and how managers' offices had clearly demarked zones for visitors and meetings as well as private work area to protect online information security [32]. The healthcare domain faces privacy challenges of health professionals constantly carrying, sharing and discussing sensitive patient data (e.g. Electronic Health Record (EHR)). A survey [37] conducted by Epocrates in 2013 with 1,063 healthcare providers showed 86% professionals use smartphone and 53% use tablet for work. Physician assistants and nurse practitioners showed highest preference for mobile devices, and 50% of professional use of tablets concerns EHR, clinical notes taking and e prescribing. Murphy et al.'s ethnographic study in a hospital setting showed that doctors, nurses and registration assistants used physical proximity (e.g., stay close to logged in and untimeout computer), secure space (e.g., choose private office, close the door, avoid taking in the hallway), and protected verbal communication (e.g., lower voice, lean close to partner, use hand of paper to cover mouth when speaking) as privacy practice [68]. Study from emergency department patients found that patients with curtain partitions reported to have less auditory and visual privacy than with solid wall room and 5% of patients with curtain chose to withhold medical history and decline part of physical examination to maintain privacy [11]. Chen et al. found privacy management in medical context through technical (access control, anonymization, and encryption) and behavioural (training, promoting, and educating medical professionals) safeguards are particularly challenging due to group dynamics (dynamic team members, temporal involvement and different level of patient information sensitivity for different roles) [22]. They argue privacy management studies were more focused on organizational level and called for underexplored small-group level examination. Digital ways to manage privacy in hospitals usually involves access control (e.g., unique logins, inactivity timeouts) over desktop computers and monitors [68]. Mobile devices have similar access control mechanisms, but on-screen content control mechanisms need more attention.

2.3 Digital Privacy Management System

2.3.1 Notification

Visual Notifications

Goucher argued that shoulder surfing mostly happens when involvement in the task that takes up cognitive load reduces awareness of the dynamic change in the environment [43]. Ware identified visual attributes that might be used in glyph design: spatial position, color, shape, orientation, surface texture, motion coding and blink coding [99]. Brudy et al. designed visual cues to provide awareness to large display users when detecting shoulder surfing moments. The cues included both abstract ones (e.g., flashing border in red color to indicate someone was nearby and looking, see Figure 2, A), or literal ones (e.g., a 3D model of a passerby, with the passerby's relative position and orientation to the display, and a red dot representing his/her gaze point, see Figure 2, B) [18]. Portnoff et al. explored the effectiveness of webcam LED indicator lights (blinking at 0.5Hz) and onscreen glyphs (a large red transparent camera which blinked in the center first and shrunk into the upper right corner and blinked for some time) as privacy indicator to notify user when the webcam is unexpectedly recording without user's consent (see Figure 2, C) [78]. The on-screen glyph was found more noticeable than the LED lights in both computer based tasks (93% versus 45% participants) and paper-based tasks in proximity to the computer (59% versus 5%). However, most unprompted participants did not interpret the glyph as a camera or its purpose being indicating webcam recording. The authors called for designing more noticeable and understandable indicators.



A. flashing border B. 3-D model and gaze C. glyph

Figure 2 Designs of awareness visual cues and indicators. Figure from [18, 78]

In a more general sense, Bartram et al. highlighted the role of icons in simple motion (moticons) in communicating awareness to the user [12]. They found moticons outshone color and shape-based icons in terms of detection error rate and detection time, especially in the periphery. The study also compared four types of motion cues: linear (move smoothly up and back to the origin), zoom (zoom twice the starting size and back to the original size), blink (traditional on-off) and travel (move across the screen right to left or top to bottom). The results showed blink and linear moticons were rated less distracting and slow linear motion was thought to strike a good balance between minimal distraction and good detection. Anderson et al. found evidence of security warnings habituation at neurological level with functional magnetic resonance imaging (fMRI) [7]. Polymorphic warnings (e.g., jiggle, zoom, change color of window and add pictorial symbol were the four most effective variations) were found to significantly withstand habituation than traditional warnings. McCrickard et al. examined effect of notifications in the form of text animation (ticker, fading, blast) in a secondary display besides the primary browsing window on communicating awareness of important information [65]. None of the three forms were found interruptive to primary task, and in-place displays such as fade (fine-grained) and blast (on-and-off) could better facilitate rapid identification than moving text.

Multi-modal Notifications

Another group of studies investigated the effectiveness of different modalities (visual, auditory, tactile) of privacy indicators at the moment the user's private information was being accessed or even shared. Auditory notifications are more intrusive and public while tactile notifications are more subtle and private [46]. These indicators serve similar purpose of providing awareness for content privacy, and the evaluation results could be exploited to inform the design of privacy indicators. For example, Balebako et al. designed just-in-time notification in the form of combination of icon and text in mobile phone's status bar and notification drawer area as well as sound and vibration to inform the user that sensitive data was being sent [9]. Vibration was suspected to be distinguishable from those caused by other applications. Sounds were found more distracting than vibrations and participants tried to figure out what information was sent

and why when they were notified. Cranor et al. evaluated how persistent indicator such as Privacy Bird, a bird icon with song bubble in the top right corner of the browser title bar together with optional sound (earcon), communicated whether the web page privacy matched user preference [27]. The results showed the green-yellow-red color scheme was interpreted as the level of goodness of the site. It also suggested that literal meaning of the icon design should avoid ambiguity to prevent confusion: symbols without obvious meaning were more distracting than helping; a happy bird singing or an angry bird talking might be unintendedly interpreted as playing music or using foul language. The sound effect was found to increase perceptibility but was annoying for high frequency appearance and thus modified to play once per day for each site.

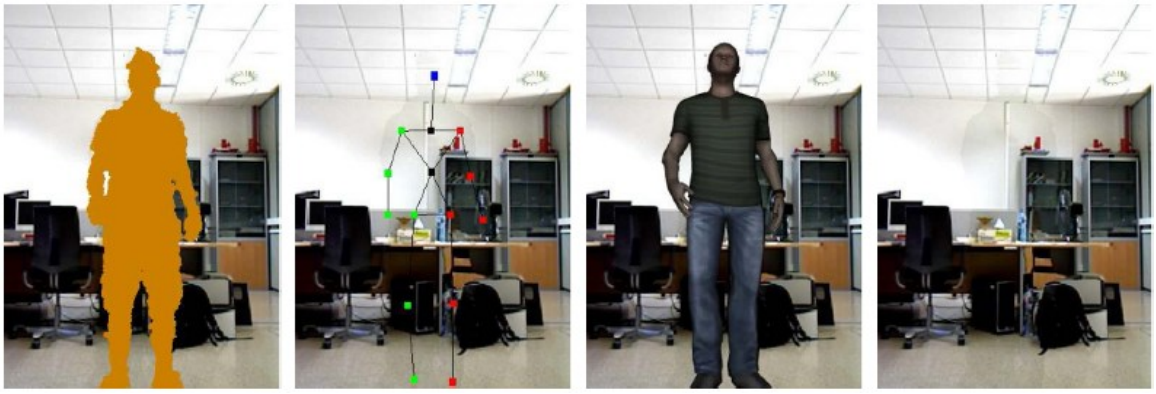
As glyph notifications were commonly used for awareness and the effect of sound and vibration is somewhat mixed, we chose glyph designs to explore in our study.

2.3.2 Protection

Tarasewich et al. conducted some of the early work to directly address protecting privacy and security information in public places [92]. They designed privacy blinders for web browsers that could automatically cover customizable types of data (e.g., money amounts, email addresses, phrases) with opaque squares (see Figure 3, A). Blinders could be removed to retrieve information by moving stylus or drawing stylus gestures (e.g. a letter) on mobile devices (Tablet PC, PDA). Participants reported positive feedback on the usefulness of privacy blinders. However, the task completion time was longer with the blinder on and too much information being covered was annoying. Brudy et al. distinguished two types of protection: explicit protection which requires user to take actions (e.g., hand-wave gesture, or turning away from the display) and implicit protection that is triggered by the system [18]. One example of protection techniques was identifying public and private window (by marking types of application or searching sensitive keywords such as “bank”, “mail”, “https”) and change the transparency of private window with the severity of privacy breach (see Figure 3, B). The silhouette

protection took the user body's role as a physical barrier into consideration and only blacked out the parts of screen not shielded by the user (see Figure 3, C).

A. privacy blinders B. black out window C. silhouette



D. visual abstraction examples of solid silhouette, skeleton, 3D avatar, invisibility

Figure 3 Designs of protection techniques for visual information. Figure from [18, 92, 57]

For specific types of information protection, a body of research focused on image and video processing techniques to preserve image privacy. For example, Padilla-López et al. summarized protection methods for imagery data into five categories: intervention, blind vision, secure processing, redaction and data hiding [57]. *Intervention* which prevents visual data being captured from the environment by interfering with camera lens concerns with privacy breach caused by devices recording whereas *redaction* methods which modify sensitive area of an image are closely related to privacy breach caused by human observing. Common redaction methods include image filtering (e.g., blur, pixelation), image/video encryption (encrypt or scramble original data to be unintelligible), face de-

identification (prevent face from being recognized), object/people removal, and visual abstraction/object replacement (e.g., replace people with solid silhouette, skeleton, 3D avatar or completely remove, see Figure 3, D). Similarly, Boyle et al. categorized content control methods in video media into distortion filter (e.g., blur that hides detail fidelity but maintain overall fidelity), publication filter (e.g., background subtraction that remove noncrucial detail) [15]. They argued both fine-grained control (being adjusted at personal, occasional level) and lightweight control (requiring little mental and physical effort) were important but hard to balance. Another potential way is to utilize hybrid images which could be interpreted as two different images based on viewing distance to maintain privacy: the user near the display sees the true meaning whereas the onlooker further away only see the decoy image [3].

Technologies that are used to support multi views on a single display could also be exploited to support privacy [31]. For example, Harrison and Hudson described how LCD displays' color distortion at different viewing angles could be exploited to generate dual-output such that sensitive information (e.g, digit password on a ATM keypad) could be masked with watermarks that is invisible for the primary user who views straight-on but shown to a secondary user viewing at an oblique angle [48]. These approaches use glasses or specialized (e.g., TN) display hardware, which might not be a realistic requirement.

Regarding exploiting text attributes to preserve privacy, Hasegawa et al. investigated visibility of graphic Japanese text displayed on LCDs of mobile phones and found the size of characters significantly affected user's reading performance [50]. This result indicated altering text size might be used as a privacy protection method. Another study of Hasegawa et al. revealed readability could also be affected by (Japanese) font [49]. Other attributes of text (e.g. brightness, foreground/background color, position, and orientation), relationship between texts (e.g., spacing between characters, words and sentences, hierarchies, pattern) and the relationship between text and the context (contrast, layout) could also be further explored.

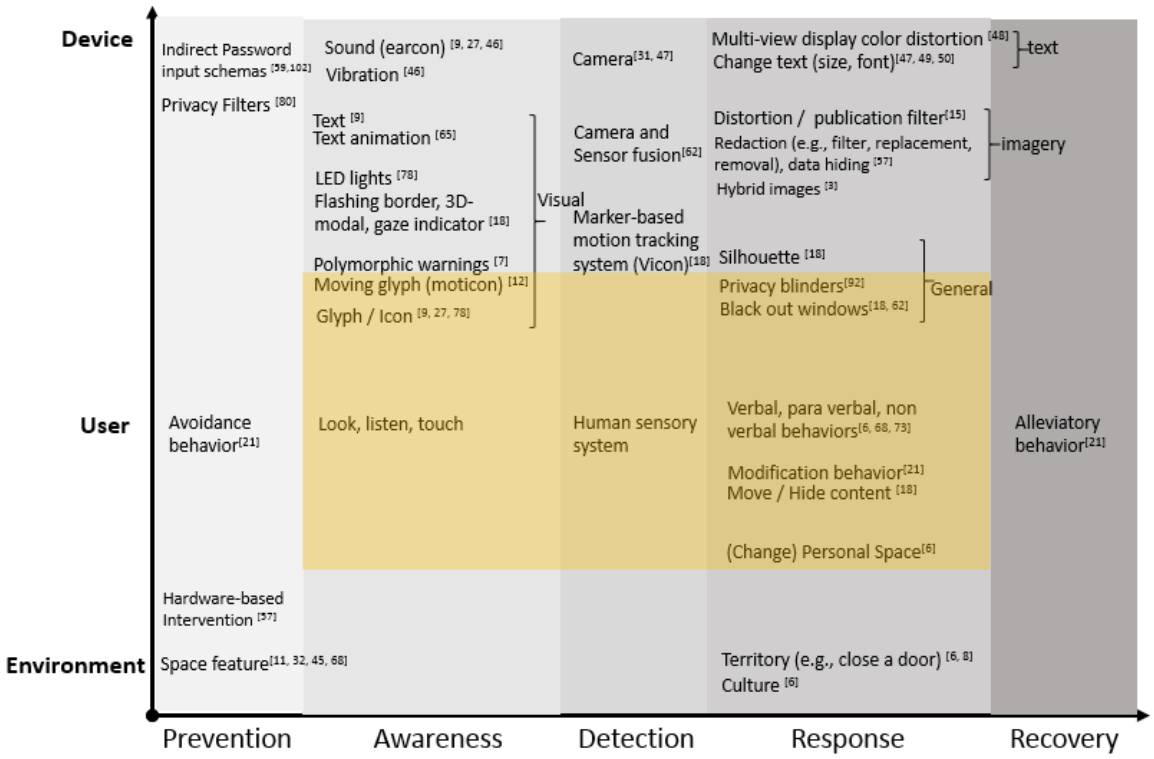


Figure 4 Content privacy management mechanisms. The x axis is divided by the 5 privacy processes. The y axis indicates the media through which content privacy is managed (device, the users themselves, or the environment). The light yellow highlights this thesis's research focus.

2.4 PROXEMICS AND PRIVACY

2.4.1 Proxemics Interaction

In the field of nonverbal communication, Hall [44] first coined the term "proxemics" in the 1960s, which specified four interpersonal zones by distance: intimate zone (less than 1.5 feet), personal zone (1.5-4 feet), social zone (4-12) and public zone (12-25 feet), see Figure 5. Altman emphasized that Hall's physical distance per se was not important but the milieus that personal space provided to various communication cues and behavioural /interactional possibilities were critical [4]. For example, within intimate zone people could touch each other whereas within public zone people might not be able to see each other's facial expressions clearly. The type and granularity of social interaction behaviours possible were different based on distance.

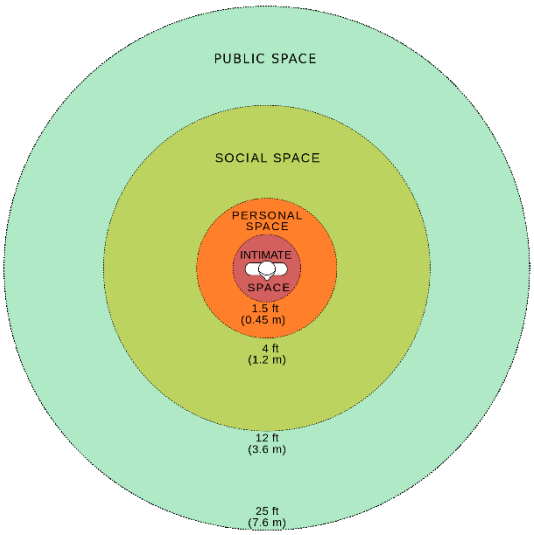


Figure 5 Hall's interpersonal zones. Figure from [74]

Hall also identified three fundamental types of space setting/layout/arrangement in the environment that could affect social interaction: fixed-feature space (permanent and immovable features such as floor, wall, building, or even invisible physical partition of (e.g. men and women area), semi-fixed feature space (movable parts or objects that are arranged in an area such as furniture), and informal space (perceptual and dynamic space maintained between interactants such as distance that varies with the mobility of interactant and are usually unaware of by interactants) [45].

Hall further categorized proxemics behaviour into 8 dimensions [100]: 1) postural-sex identifiers (sex and postures such as sitting, standing or prone) 2) socio-fugal-sociopetal axis (orientation of shoulder in relation to others such as face to face, at a certain angle, back to back) 3) Kinesthetic factors (distances between people that provides the potentiality for holding, grasping or touching each other) 4) Touch code (amount of touching contact such as accidental touching, holding, caressing) 5) Visual code (amount of visual contact present) 6) Thermal code (detection of human body heat) 7) Olfaction code (detection of odor or smell of breath and body) 8) Voice loudness (volume of voice in interaction). Thirumalai summarized Hall's series of study as how people exploited different types of distance and space features for proxemics behaviour [93]. Although

distance and space features are important aspects pertaining to proxemics behaviours, other spatial characteristics such as orientation, objects and barriers embedded in the space could also be exploited for interactions. Dostal et al. (2013) summarized the evolvement of proxemics dimensions from distance to Vogel et al.'s (2004) four interaction zones (personal, subtle, implicit interaction and ambient display), to Ballendat et al.'s (2010) incorporation of objects/digital devices and continuous distance, and Wang et al.'s extension of attention (visual focus) towards the display [31]. Greenberg et al. (2011) operationalized proxemics into five dimensions (distance, orientation, movement, identity, location) which highlighted contextual dimensions such as time (e.g. movement reflects the relationship or distance and orientation over time), identity (uniqueness of people, digital devices, non-digital objects) and conducted a series of work of using proximity to conciliate interactions such as video communication (person-to-person), media surface control (person-to-surface, device-to-surface) etc. [42, 10].

2.4.2 Proxemics as mediator for privacy

In the privacy field, Greenberg et al. leveraged the distance between people and screen in always-on video connection to infer interaction intention and alter video and audio fidelity to preserve privacy [42].

With content privacy, Brudy et al. exploited proxemics information to both providing visual cues of potential privacy intrusion and protecting large public displays against shoulder surfing [18]. An informal evaluation with 8 participants from onlookers perspectives showed as the onlooker got closer to the large display (2.7m~1.1m), the average angle of field of view is larger for looking with corner of eye (86°~ 106°) than for looking with straight head (57°~ 73°) [17]. However, it didn't evaluated the system from a user-centric perspective. Also large display is fundamentally different from mobile devices in terms of magnitude of visibility (large vs small), type of information intended to display (public vs personal) and the amount of physical ways possible to manage privacy (scarce vs rich).

Lian et al. proposed a scheme that combines screen peeping detection (eye detection and person counting), user distance and environmental brightness with video camera, ultrasonic distance and light sensor module to dynamically adjust computer screen brightness to protect privacy [62]. They implemented the scheme with a 4.2-inch screen smartphone (which includes a front-facing camera), a light sensor and an ultrasonic distance module in Android OS. The evaluation of the system performance showed the detection decreased with capturing distance and camera's resolution, especially with a distance greater than 0.4m under natural outdoor light and weak indoor light. Subjective ratings about the screen protection effect also showed the screen details were protected when the view distance is bigger than 0.3m and view angle is bigger than 40 degree. The system also contained a screen protection alert part and a user confirmation process for the protection to be triggered. Although how the alert was implemented was not specified, it was suggested to be in the form of a text, voice or animation message. This work explored more practical implementation with mobile devices and evaluated the system from more objective perspective (accuracy, observer visibility). It did not address the impact of different protection technique design or how user might use the system or their attitudes toward the system.

In addition, Harrison et al. exploited the level of leaning posture with laptop camera to magnify the screen content at discrete level [47]. The lean and zoom system was evaluated with 10 participants by an experiment with pre-task, post-task survey. The results showed that leaning was an intuitive and stable input for screen content control and 80% participants thought this technology would be applicable for mobile devices. This research didn't directly address privacy issue, but it could potentially be appropriated to mediate privacy management. For example, when a user leans forward, the system shrank the size of screen content to make the shoulder surfer harder to read.

2.5 Challenges of Privacy Evaluation in the Lab

Designing experimentally sound study to impose plausible privacy threat and elicit realistic privacy responses in the lab is difficult. On the one hand, requiring users to use real data (e.g. bank information) in the lab could bias the results by precluding privacy fundamentalists and only recruiting people who didn't have real concerns about banking privacy [72]. On the other hand, in an experimental simulation, participants will hardly invest themselves to value fake task data or be responsible for their demonstrated behaviour in the manner they do in the real world because those actions won't result in real consequences. Moreover, the perceived reputation of the research institution, consent form could affect participants' trust toward the study and result in disparity between observed behaviour in the lab and their self-reported behaviour in everyday life [89]. Nonetheless, researchers have developed various paradigms to evaluate privacy and security in the lab setting. For example, Tan et.al evaluated the effectiveness of a spy-resistant keyboard with pairs of participants where one participant typed in given password with the interface on a large screen and the other participant acted as the observer to watch and reconstruct the passwords [90]. Preibusch described an experimental procedure how privacy concern could be measured by observing how much compensation is needed for users to accept privacy invasion or how much they wish to pay for privacy [79]. Role playing has been found to be helpful in engaging participants in study tasks and develop a sense of responsibility [86, 96, 33, 36]. Iachello and Hong suggested making the tasks used as realistic as possible, properly motivate participants to protect their information, or putting them in the setting that matched expected usage [54]. Concealing the study purpose and use unrelated primary task is also useful for the secondary nature of privacy and security goal [72].

We applied some of the practices from the literature to our study design. In the design exploration evaluation, we chose the location of the Wizard of Oz study in a busy library to put participants in the setting where the designs/techniques are intended to be used; we used high-fidelity prototypes (with made-up data) of Facebook chat, online banking to simulate real life privacy scenarios; we also used a memory match game or unrelated primary tasks (e.g., retrieve a piece of information) to accommodate the secondary nature of privacy purpose. Moreover, in the lab evaluation, we adopted the pairwise user-

observer idea and designed a hide-and-seek game played by a user and an onlooker to observe privacy management behaviours; we also applied the role-playing technique to increase the sense of responsibility towards the fake data. In addition, we measured participants' privacy concerns, motivation for preserving privacy during the tasks, the realness of the tasks and the role-playing to verify the effects of these study design decisions.

Content privacy on mobile devices is far from fully explored. Given the existing physical and digital privacy techniques (summarized in Figure 4), we identified a gap in how visibility of content on mobile devices is managed physically, how well these digital techniques would work for mobile devices, how a comprehensive solution which combines both physical and digital mechanisms and integrates multiple privacy processes could be designed from a user-centric perspective.

CHAPTER 3 DESIGN EXPLORATION

In this chapter, we first present several visual forms of notification and protection technique designs. With the Wizard of Oz methodology, we then use typical privacy sensitive scenarios (e.g., banking, chatting) to collect feedback on the understandability and effectiveness of the notifications, and the strengths and weaknesses of various privacy enhancement mechanism designs. We present the results and design implications of such content privacy management system. We further evaluated the design candidates in a healthcare context with an interview. Lastly, we show the implementation of a proof-of-concept prototype that mediate notifications and protections with proxemics data. Section 3.1-3.4 have been published in [106].

3.1 PROTOTYPE DESIGN

We designed several glyph privacy notifications that were meant to notify the tablet user of potential privacy threats, as well as four privacy protection mechanisms that could adapt screen content dynamically to protect privacy.

3.1.1 Notification Design

A notification pops up on a tablet as a warning that informs tablet users when someone in close proximity is looking. Similar to Edworthy's [35] division of warnings into iconic and informational, we designed two types of representations to denote proximity information: metaphorical and literal. We use an eye to metaphorically indicate that somebody could see your screen. Different statuses of the eye represent the level of risk (determined based on a combination of relative distance and relative viewing angle). We designed 3 notifications with different granularity (see Figure 6 A, B, C). For the literal representation we used a radar view to represent the relative position and orientation (field of view) of the potential intruder(s) in real time (see Figure 6, D). The dot in the

center represents the tablet, with the bottom half of the circle representing the screen, and the top half the back of the tablet. We assume the tablet is held approximately vertically; tablet height, pitch and yaw are not represented.

A. Simple B. Coarse C. Fine-grained D. Radar

Figure 6 Notification mechanisms. A. Metaphorical notification with 2 levels (on or off). B. Metaphorical notification with 3 coarse levels. C. Metaphorical notification with fine-grained opacity levels. D. Literal notification with intruder's relative position and field of view mapped on a radar animation.

We aimed to explore the impact of notification granularity on users' perception of privacy threats. We also aimed to understand the strength and weakness of metaphorical vs. literal representations.

B1 B B2 B3

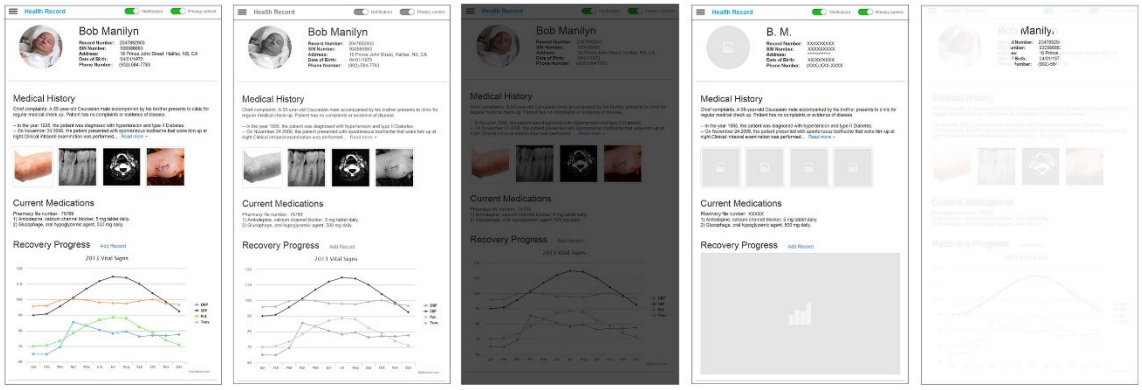
Figure 7 Alternative designs of metaphorical notification with 3 coarse levels. B was used in the tasks whereas the other three were asked for comparison during the post-task interview.

In addition, we designed coarse-level notifications with different visual representation (see Figure 7). For example, B1, B and B2 are redundant-coded designs: both color and

area of color/number of color arcs/extent that eye is opened illustrate the severity of potential privacy breach. B3 is single-coded design with an icon of a spy to imply that somebody is peeking. For all the designs, as the level of privacy risk increases the color of the icon changes from yellow to orange then to red. We wanted to understand among these metaphorical designs which are effective designs and which are not, and what the factors that might affect people's preference are.

3.1.2 Privacy Protection Mechanisms Design

In addition to or instead of notifications, privacy control mechanisms can be triggered as a potential intruder is getting closer to the tablet (implicit control) or as the tablet user takes explicit actions (e.g. tilts the tablet, uses the body to shield the screen) to protect screen privacy (explicit control) [18]. Four privacy controls have been designed and are under study: Grayscale, Dim, Selective hiding, and Mask (see Figure 8).



A. No control B. Grayscale C. Dim D. Selective hiding E. Mask

Figure 8 Privacy protection mechanisms. A. A normal electronic health record with no privacy control. B. grayscale. C. Dim. D. selective hiding. E. Mask.

- **Grayscale**: This mechanism gradually removes hue from screen content, from full colour to grayscale. Green et al. and others discuss how visual variables like colour facilitate human cognition during analytics activities (e.g., information discovery, search, creation and analysis of hypotheses) [41]. Since colour is preattentively processed and distinguishable by peripheral vision, removing it may protect privacy

for certain visualizations and possibly other images by not calling attention, and reducing the immediacy of visual data representations.

- **Dim**: This mechanism changes the screen's brightness in a fine-grained manner. As the risk of privacy intrusion increases, the screen is darkened gradually to almost complete black. This mechanism has been used by previous researchers for privacy protection [53, 18, 62].
- **Selective Hiding**: When activated (automatically or with a single click), selective hiding shortens or anonymizes all sensitive information on the screen. Here the type of sensitive information is highly scenario-specific. For example, photos in a photo album could be sensitive but pictures in a bank webpage are usually not sensitive. The types could be user-defined or machine-defined. In our content samples, we used consistent machine-defined types for evaluation purposes: names were shortened to initials and other identifying textual data was replaced with "xxxxx"; pictures in a photo album, health record or chat profile, and charts in a health record and financial pages were replaced with default pictures; balance numbers in financial pages were replaced with "xxxxx" (similar effect to Tarasewich et al.'s privacy blinder [92]).
- **Mask**: This mechanism uses a white and partially transparent layer to mask the whole screen except a small circle-shaped viewport. Selective hiding is different from the other three in the sense that a user actively controls it by dragging the viewport to see information. It looks similar to Brudy's silhouette protection [18], but the visible area is chosen by the user instead of determined by intruder's relative position. This is intended to give the user more flexibility and allow the user to continue working.

We examined how varying certain visual attributes of the content might facilitate privacy enhancement and explored the tradeoffs of different mechanisms.

3.2 Design Evaluation Study

We used typical privacy sensitive scenarios (e.g., banking, chatting) to collect feedback on the understandability and effectiveness of the notifications, and the strengths and weaknesses of various privacy enhancement mechanism designs.

3.2.1 Goals and Overview

The study aimed to elicit design feedback. We planned to explore whether notification mechanisms are interpreted by the users in the manner intended and to assess the strengths and weaknesses of each. For the privacy control mechanisms, we intended to investigate their generalizability by testing them across a number of scenarios and eliciting participant feedback after each scenario. We also wanted to validate whether the notification-protection concept as a whole fits users' mental model of managing privacy. We ran the study in a busy public space (a library lobby) instead of the laboratory, so participants could be put into a context where privacy might be compromised and offer more valuable feedback. Considering the purpose of the study and the difficulty of deploying the tracking system in the field, we applied a Wizard of Oz (WOz) methodology to evaluate the interface. .

3.2.2 Study Procedure

We recruited participants from Dalhousie University via email lists. Participants were required to use a Tablet PC on at least a monthly basis, and to "*have experienced privacy concerns about others viewing [their] screen as [they] conduct activities on the tablet*". We offered participants $15 to participate, and the study lasted approximately 90 minutes. The study was conducted in the atrium of a university library where faculty, staff, and students could take a break, study and socialize (see Figure 9). This high-traffic area is chosen to motivate participants to think about privacy in real life and to elicit better judgment and feedback.

Prior to the study, participants gave consent and filled in a background questionnaire. One researcher then met the participants at the atrium. We provided participants with a Windows Surface Pro 2 tablet PC and seated participants in front of a table. The

researcher sat beside participants, used a second tablet PC (Google Nexus 7) to control the content displayed on participants' screen, and could observe the details on the screen while participants completed study tasks. The study started with a few pre-task questions regarding participants' occupation, tablet usage, and privacy concerns of other people viewing their tablet screen. Participants then completed two major sessions in turn: notification evaluation and privacy control mechanism evaluation. In each session, participants performed a set of tasks and reflected on different designs. Participants were encouraged to think out loud during the task and to provide honest feedback. At the end of the study, we performed a semi-structured interview, asking them to reflect on their physical mechanisms to manage tablet screen privacy, their expectations of how notifications and privacy protection mechanisms might work together, their concerns about using the system and suggestions for improvement. We videotaped the participants and took handwritten notes.

Figure 9 Wizard of Oz study location: a university library. Figure from [29].

3.2.3 Study Tasks and Materials

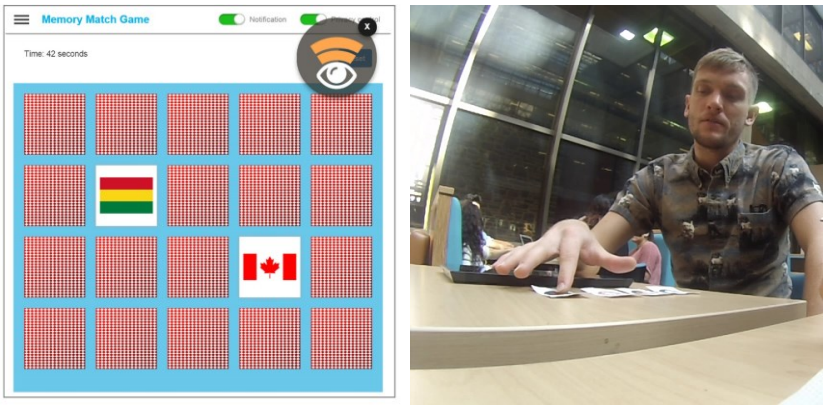
Notification Evaluation

For the notification evaluation session, participants were given a general scenario (See Table 2):

Table 2 Notification evaluation scenario.

You're sitting in a public library using your tablet. From time to time, people may be able to view the content on your display. Imagine there is an application that can provide some kind of notification that your display might be visible.

Four notification designs were evaluated one by one; their order was counterbalanced across participants. To test participants' level of awareness and distraction for each notification, we used a memory match game as the primary task (see Figure 10, A). The game required players to tap on two cards to reveal the pictures underneath. If the pictures match, both of them disappear. Otherwise, both cards flip over. Participants were asked to clear all the cards as quickly as possible, thus requiring their attention. All participants were trained with an easier version of the game beforehand. During the game, the researcher made one of the notification designs appear at random times (between 2-6 times per round). After each round, participants were asked how many times somebody could see their screen as well as their understanding of the notification. After all the notifications were presented, participants were asked to rank the designs in terms of awareness, distraction, usefulness and preference and to provide reasons for their rankings.

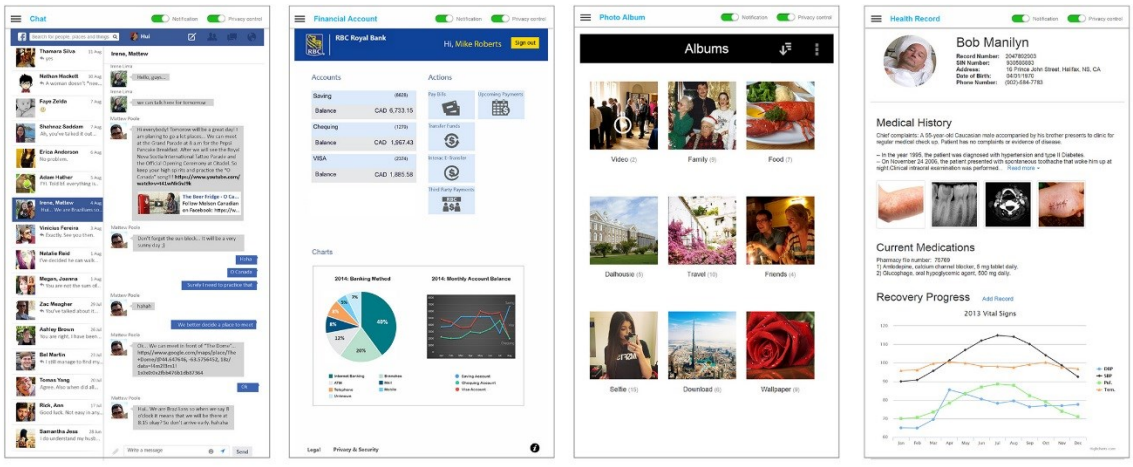


A B

Figure 10 Notification evaluation setting. A. Memory match game interface with a notification. B. One participant ranking different notification designs while reflecting his choices.

Protection Mechanisms Evaluation

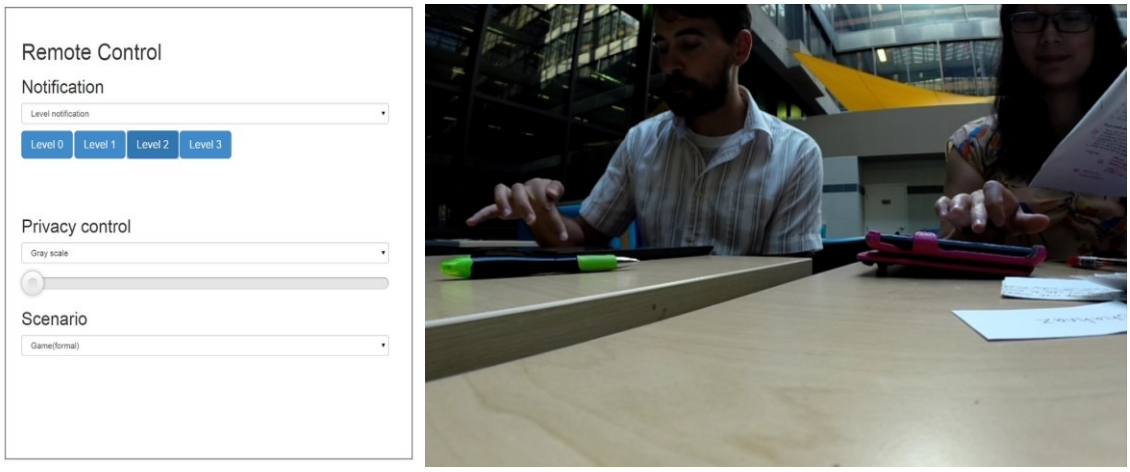
For the privacy control mechanism evaluation session, we used four scenarios that may be considered to be sensitive: Facebook chat, online banking, viewing photo albums and viewing online health records (see Figure 11). After piloting the study, we administered 2 tasks per scenario due to time constraints. In each scenario, two different privacy control mechanisms were tested and rated in terms of protection, interference and satisfaction, one for each task. The other two mechanisms were only showed without performing tasks. Half of the tasks contained potential sensitive information to highlight the difference between a normal scenario and a private scenario. The task type included retrieving information from Facebook chat (e.g., find what's the advice given to a friend cheating on her boyfriend in a message dialogue), inputting text (e.g., login into an online bank account), viewing photos (e.g., find the photo you would be concerned about other people viewing such as awkward family photos, drunken stupors), or reading charts (e.g., find health problems such as bad teeth and the prescriptions given). After each scenario, participants were asked to rank all four mechanisms in terms of protection, interference and usefulness, and reflect on their rankings. Each participant completed 8 tasks (2 tasks per mechanism). The order of privacy control mechanisms, scenarios, and tasks were counterbalanced across participants.



A. Chat B. Finance C. Photo D. Health Record

Figure 11 Screenshots of prototype illustrating 4 privacy sensitive scenarios. A. Facebook Chat. B. Online banking. C. Viewing photo albums. D. Viewing a health record.

All the study materials were developed in HTML5, CSS and JavaScript. Node.js was used to host the server on a lab computer, providing access to the matching game and privacy scenario content. The client was connected to the server with a Google Chrome browser through the university's wireless network. For the study, we developed a remote control (WOz) page to manually switch scenarios, trigger different types and levels of notification and privacy control mechanisms, and turn on/off each notification or mechanism (See Figure 12, A).



A B

Figure 12 Wizard of Oz study setup. A. Remote control interface. B. One participant performing the tasks while a researcher user the remote control interface on another tablet to trigger a notification or protection.

3.2.4 Participants

We recruited 12 participants (6 male, 6 female) who regularly use tablets. Participants averaged 28 years in age (range 21-44, SD=7.7). No participants were color blind. 8 participants were graduate students from Computer Science, Engineering, Economics and Information Management. The remaining 4 participants worked as a business analyst, administrator, dentist, and system analyst in a hospital. 10 participants used iPads (including 2, 3, mini, air) and 2 used Android tablets. 9 participants used tablets for more

than 1 year, 3 for more than half a year. 5 participants used their tablet on a daily basis, 4 about twice weekly and 3 on a weekly basis. On average participants used tablets 9 hours per week, 64% for personal use and the remainder for work or school. 9 out of 12 participants chose home as the primary location to use the tablet, and while at home it was used mostly for entertainment. The secondary locations are workspaces such as an office, study area, or lab (7 participants). Participants also use tablets in cafés (3), on the bus (3) and on the plane (2).5 participants used passcodes to protect their tablet. Among the 7 participants who do not use passcodes, 4 of them share their tablet with family or classmates. We asked participants to rate their privacy concern level for accessing the following information while being viewed by others on a 7 point Likert scale: social network chat, email, calendar, document, finance, shopping, photo, game, and health data. Using Friedman's ANOVA, we found participants are more concerned about financial information and less concerned about game progress/score. On average, participants were least concerned about family viewing their screen (M=3.5), followed by close friends (M=4.1), colleagues (M=5.1), and then acquaintances (M=6) and strangers (M=6). Participants had experienced tablet privacy concerns when doing banking, chatting on Facebook, reading email/documents and taking minutes that may contain negative feedback about colleagues. Participants rated the privacy levels of the scenarios we used in the study (on a 7 point Likert scale) as finance (6.8), health (6.3), chat (5.4) and photo (4.9).

3.3 RESULTS

3.3.1 Notification Design

Notification A (All or None)

Among the 3 metaphorical designs, A (all or none) was ranked the lowest. Participants ranked it as less understandable ($p<.05$), less noticeable ($p<.01$) and less useful ($p<.05$) than the other two. The gray color made it hard for nearly half of participants to understand its meaning. P4 commented: "*It doesn't mean much to me… It doesn't suggest someone is looking, doesn't suggest a threat to me*." Two participants described it as a

more generic symbol associated with eye detection or tracking. Participants thought A was the least noticeable. For example, P12 said "*I might be invaded but not notice*". However, they made fewer errors in reporting the number of appearances of the notification during the game than the radar (D). P5 echoed other participants concerns about lack of granularity: "*I felt it doesn't tell me as much information. There are variability in my concerns for people being able to see depending on how far they are. This [A] doesn't give me the variability. I feel like I would be protecting the screen a lot more with this one on and off*".

Notification B (Coarse)

We didn't find significant differences in rankings between mechanisms B (coarse) and C (fine-grained). Most of participants interpreted the 3 different "*gradations*" or "*signal strengths*" as level of "*risk*", "*severity*", "*vulnerability*", "*alert*" or "*invasion*", but two participants thought it represented how crowded the surroundings were. The colour coding from yellow to red made it easy to understand, while the redundant "*signal strength*" coding "*give[s] information in two forms*". Most of participants associated color with distance, 2 with looking direction. For example, P2 stated "*I believe red means somebody is really watching you, standing beside you, and curious about what you are doing. Orange could be 50-50 for most of the time... Yellow is like little, but he is mostly looking somewhere*". 6 participants also mentioned that yellow or orange would not make them concerned enough to take action, and they will ignore them after using the system for some time. In terms of awareness, 4 participants thought the changing color is "*drastic difference*" and the changing bars is like "*a movement going on in your screen*". 6 participants claimed with this design, they paid less attention. For example, P9 said: "*It is there and you know it is there. You don't tend to look at it again. You can see the lines going up and down*". But P12 thought "*more things appearing, that's annoying*". Overall, participants thought this design was straightforward, easy to grab attention, and a good indicator of severity. Aesthetically, they felt it was "*simple*", "*easy on the eyes*", "*professional*" and "*modern*".

Regarding the alternative designs of coarse level notifications (see Figure 7), we found significant differences in rankings among the three redundant-coded designs with mean rank of B1=2.92, B=1.92, B2=2.25 ($p=0.039<0.05$). The design used in the study (B) was ranked as the highest among all the alternative designs, its similarity to a Wi-Fi signal making it easier to "*denote the range where people might be*" (P3) or "*show the distance*" (P2). The shape change across levels is also more noticeable than color change (P7, P12). Using post hoc paired comparison, we found participants prefer design B to B1. B1 was thought to be hard to understand (P1 and P6), less noticeable (P5 and P7) or simply disliked with no reason (P2 & P12). Design B2 generally got positive ratings and was described as "*professional*", "*appealing*". Two issues were identified with the large color block: either too bright thus distractive or the difference between different colors were not obvious enough to be notices. 7 participants interpreted B3 as a person with secret identity ("*spy*", "*bad person*", "*Carmen Sandiego*", "*criminal*"). 4 participants liked the spy design, but the majority disliked it because of poorer understandability, unfriendliness, and clutter (mean rank of B3=2.92).

Notification C (Fine-grained)

C is also a metaphorical design, but uses transparency to indicate severity of risk instead of color. The red color was perceived as "*serious alert*", "*danger*", "*urgent*" and "*stop*". The "*degree*" or "*intensity*" of the eye was interpreted as distance and looking direction. P3 said "*When they [people] are closer and appearing right over my shoulder, it would be dark, when it's faint, maybe they were just passing by*". P8 thought *"[it means] a person is coming near and going far from the screen*". P12 said "*Somebody might be looking at the tablet. Darker means definitely someone is looking, lighter means not certain*". Participants thought the big area of red color caught their attention, but only when it was fully red. 8 participants ranked it less noticeable than B overall. In terms of distraction, it was similar to B; in this case the red color is distracting. P3 stated "*It seems to distract me more. It was something I found like 'oh my god I have to do something to stop it'*". Another factor is the fine-grained way the color changes. P6 commented: "*The color is changing continuously, I need to check whether the color is dark enough*". Overall, design C was found to be easy to understand. While it easily catches people's

attention when fully red, a disadvantage is it is hard to judge the exact risk level for action. Design B was ranked higher than C in all the dimensions: easier to understand, more noticeable, less distractive, more useful and more preferable, but these differences in ranking were not significant.

Notification D (Radar)

D is a *literal* design. Participants see themselves as the black dot in the center and the moving triangle as someone passing by or approaching them, therefore providing relative position and distance information. Half of participants explicitly used the term "radar" to describe the design. 5 participants comprehended the meaning of the triangle, which is the vision of potential onlooker, exactly as the design intention. The remaining participants either did not understand the triangle or interpreted it as the head, face or body of the person, facing the opposite direction. For those who understood correctly, they still needed explanation to validate their understanding. P12 said "*It doesn't have an eye. It doesn't necessarily indicate someone is looking*". In terms of awareness, 5 participants did not notice it at all. We found that this design did not pop out as much for participants as the other designs. The background always stays on the screen, and only the red triangle changes. Secondly, the contrast of red foreground and gray background may not be strong enough. Interestingly, if we exclude the 5 people who didn't notice it at all, 5 participants thought it was the most distracting. P6 said "…*The direction of the red button, and the distance between triangle and the center, this would cost a lot of time*". P9 also commented "*I think you can do your work or look at the symbol. You cannot do it together. It needs more of your attention, but your first preference would be doing work*". Nonetheless, most participants thought the design is quite useful because it provides detailed information about the surroundings: where a person is and his looking direction. The main drawbacks according to participants were that it's more complicated, and interferes with work. P12 said "*I don't want something I need to think a lot about*". P4 said "*If it only pick[ed] up the immediate area, it could be pretty useful. But if running [in a] larger area and there are too many people, I don't know how effective it would be*".

General Design Aspects

Proximity perception: We asked participants to estimate how far they think the potential onlookers were when notification B appeared as red, orange and yellow. We calculated the median of all estimations and found that when a potential intruder is less than 2 feet, 2-5 feet, and 5-10 feet away, participants expected the system to notify as red, orange and yellow. It is interesting that participants' perceived risk distance roughly corresponds to the four interpersonal zones Hall (1966) [45] specified: intimate zone (less than 1.5 feet), personal zone (1.5-4 feet), social zone (4-12 feet), and public zone (12-25 feet).

Location: Before the notification evaluation, we let participants drag the notification to their preferred location. It turned out that the locations were dispersed on the corners or in the middle of edges. Although participants had diverse habits, the principle behind choice of location was identical: keep it out of the way but still in line of sight.

Size: The 150*150 pixel notifications were presented on a 1080*1920 pixel screen. An equal number of participants thought the size should be bigger, smaller or stay the same. Two participants suggested the size should be customizable to accommodate different users and variable task sensitivity. Perhaps, for example, the size could increase for highly private tasks (e.g., banking, video chat) to become more noticeable. Two participants suggested the size of the notification could change with proximity.

Suggestion for designs: For the coarse notification (B), P4 suggested that it could rotate to point to the direction of the threat so that the user could look and make sure the person is not looking at the tablet. For the radar notification (D), two participants suggested changing the color of the triangle to indicate different risk. P5 suggested allowing customization for everything including the notification icon, size, color, transparency etc.

3.3.2 Privacy Protection Mechanisms Design

Grayscale

Grayscale was ranked in almost every circumstance the least protective mechanism (See Figure 13). Participants generally did not trust that grayscale can be effective or helpful in protecting information. P3's comment is representative: "*This [grayscale] didn't interfere whatsoever cause it really didn't do anything*". However, P3 added "*I guess I'd have to have some proof, like from distance, does that actually stop people from seeing it? My guess is it probably doesn't. But if it does, that would be phenomenal to use…totally the one to go with. Because this was less intrusive, it is very easy and you can still see everything. But if it is not actually useful for what you intended for, why have it*? " The key strength of grayscale is related to color. In the Photo scenario grayscale received its highest satisfaction score (although still in the middle range). For example, P6 explained "*For photos, colors are very important. Sometimes colors can attract people's eyes. If it is black and white, in my mind, most of the people can't be attracted*". Nonetheless, most participants still thought it was not effective to use. Another problem is the reduced contrast could be difficult for users with reduced vision. It decreased the legibility of text in the chat scenario, and interfered with tasks involving colorful photos and charts. P2 thought grayscale could be useful in health setting because "*black and white won't affect images. If you are an experienced physician, even with black and white you can tell what that is*". P5 thought graphic designers might use it to protect color choices and ideas.

Dim

Dim seemed to provide a good balance between efficiency and privacy, but was also controversial. Participants were more certain that Dim did protect privacy because it made themselves harder to see. At the same time, it still allows some onlookers to see content. Participants who liked it said: "*It will not affect work efficiency but still be protective. It is equally friendly, it uses less power. I like to set my screen brightness to very low level. It's good to the eyes, and consumes less power*" (P7). P9 described it as "*average*", "*medium*", "*helping in all senses*" and "*quite user friendly and practical*". Participants who disliked Dim struggled to see the content, saying: "*I can't read it. I won't use it. I don't like less bright screen in general. I usually make it brighter. If I increase the brightness, the technique itself is of no use*" (P8). P10 thought it could be

useful in a health setting because "*I'm thinking about usability, [it's] good and protective. You [healthcare providers] don't want to slow down*". P2 disagreed: "*If you make it black, I can't see the contrast here, and as a physician, I need to be careful for what I'm observing here, so I can reach my diagnostic conclusion*". While many participants agreed that it might be useful for photos or personal use like chatting, its usefulness seems to be more dependent on personal preference, fitness to the current context, and task sensitivity. Participants suggested it would be useful if the brightness could be easily controlled or adjusted.

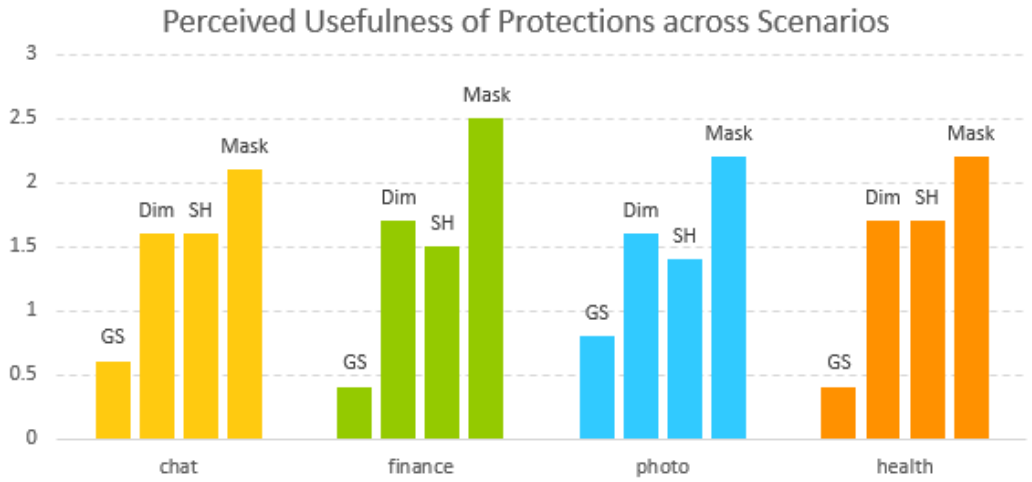


Figure 13 Perceived usefulness ranking of protection techniques across scenarios (GS for Grayscale and SH for Selective Hiding).

Selective Hiding

Selective hiding can be very protective, ensuring that all sensitive information is hidden or obfuscated (e.g., all financial numbers). At the same time, it can interfere with a task so much as to stop the user from doing work. Its usefulness is highly dependent on task information and whether the type of hidden information suits the level of protection users need. For example, in the chatting scenario, P4 said "*I'm not too private [about chat]. This [selective hiding] would make it just hard enough to make it more private but not interfere with what I'm doing*" while P3 thought "*Although it takes the name out here, but you still have something written here [conversation history], you can still identify people*". Similarly, in financial scenario, P3 commented "*I do enjoy how it takes out the*

numbers and name, so it's kind of useful…If someone is right beside me, I'd be happy it was done. If someone is quite a few feet back, and it did that, Ok I have to use this".

Participants had different opinions about what kind of information should be hidden. For example, P10 thought for healthcare professionals, the pictures of X-rays, body parts and even graphs may not be that sensitive. P12 thought that for a dentist, teeth photos and charts are not something major, but for major diseases such as cancer, or pictures that show parts of the body other than mouth, photos and charts may be more sensitive. P8 thought as a patient, "*I don't want anybody to see the pictures of my body part*". One thing special we learned about health records is that they are sensitive in a global sense. P10 stated "*Depending on knowledge. Like medication, I won't be able to figure out because I'm not a health profession, but someone will be…Everything really is sensitive. That's how we treat it. Just the initials can reveal a lot*". P12 was concerned about only covering identifiable information, pictures and graphs, as there still may be sensitive information in the text: "*Because not everything is hidden, maybe patients won't be comfortable with it showing everything in it*". Perhaps partial protection will not suffice in some healthcare use cases. For general usage, allowing configuration of the type of information to hide might be useful.

Mask

Mask provides protection but could be difficult to use in certain situations. The screen is covered in white, but s not completely opaque, allowing the user to vaguely see underneath. It also gives the user control of what screen region they want to view unobstructed. Mask was rated overall most preferred protection (for mean rank Mask=2.4, SH=1.6, Dim=1.5, GS=0.5). A benefit that mechanisms like Mask have is that in extremely sensitive situations, it not only protects sensitive information, but also protects the activity itself. For example, P8 stated "*[selective hiding] does protect the data. But if somebody looks at it, he can see I'm working on my financial account. If anybody knows I'm working on my financial data, I would be more prone to attack*". Similarly, P11 suggested that cartoons and pictures kicks in to hide the whole screen when doing very sensitive activities such as banking or viewing photo albums.

Participants though it is "a bit like art" and "cool". Overall, Mask was the most well-accepted mechanism (7 participants ranked it as most preferred mechanism). The drawback is it was sometimes difficult to use. In the chatting scenario, P3 said "*It's literally I have to go one [line] by one, it interfered quite a bit*". For tasks that require large amounts of scanning or where information is dispersed across the screen, it could be very frustrating and tedious. For unfamiliar pages, it could be difficult to locate information.

Some participants expected Mask to be something that could be turned on in public places like on trains or busses, and when doing really private tasks (e.g. banking). However, it might not be suitable for healthcare settings. P10 commented "*It's [Mask] good to turn it on when you feel unsafe, but then to work like this, it's impossible…You want to see the whole table. Looking at graphs or tables, this little thing is not going to help you…It's very disruptive. You cannot ask people to do this when they are taking care of patient*". Participants wanted to be able to adjust the size of the circle depending on task sensitivity, preferably with pinch gestures. A rectangular visible area could be more useful for texts and documents. .

3.3.3 Concerns about the System

Participants expressed various concerns about using the system. First of all, 6 participants were worried about the system being overly protective. For example, P11 stated "*How sensitive it is to the surroundings? Like this scenario [library], everybody can pass by. If they don't look at you, they don't affect your work, it's OK…The system shouldn't hide the information. The system should be smart enough to recognize whether they are passersby or dangerous strangers*". Secondly, identity recognition. P4 noted *"[I wonder] if it could tell the difference between my eyes and your eyes… it has to somehow recognize you as individual*". P10 highlighted the importance of identity recognition in clinical settings: "*But again be careful. Most people walking around hospitals, like in wards, and entering patients' room are professionals. If it notifies every person approaching, they [health professionals] would turn it off. It would be just too many false*

notifications that it won't be useful". P2 and P5 considered system learnability. P5 says "*It might be annoying or take some time to get used to it*". P6 and P7 mentioned concerns about power consumption (e.g., change the brightness of the screen). Other concerns include interference with work, missing the notification because of not looking at the screen, or the system failing to function properly.

3.4 Discussion

3.4.1 Physical and Digital Privacy Management

Participants used different physical mechanisms to manage tablet screen privacy. P3 was actively using the system: whenever she saw that a notification appeared, she tried to lean backwards, change the orientation of the tablet, or set it on her lap and use her body to block the potential viewer. P5 was thinking aloud during the game: "*So I think there is no one, so I'm ok to leave the tablet on the table… [notification appeared] So someone must be getting closer, so I will pull the tablet close to me to protect the screen and I'm blocking the tablet a little bit with this hand…They're very close to me, so I hold it against me so that they can't see anything.*" When doing the banking login task, he used the "bank card" (a piece of paper in this exercise) to shield the login box. Other participants talked about having a physical barrier behind you (e.g., a wall), quitting the current work, turning off the screen, flipping the tablet, or even getting up and moving to a more secure location.

Despite such a wide variety of physical privacy mechanisms, almost all participants thought the system would be useful. With notification, "*you might not look around as much to see if anybody is watching*", said P3. P4 said "*If you're very much into your work, you might not be paying attention to your immediate surrounding*". P5 also described notification as "*add an eye in your back*". Participants thought that digital privacy control mechanisms could protect privacy better than just using hands, quitting the application or closing the tablet, while allowing people to continue their work in a normal pose. The system can also be used in circumstances where human senses are

muted. For example, P2 told a story of doing a budget while listening to music with earphones, not realizing other people were standing right behind him, and thought the notification would be useful at that moment.

Generally participants considered that the system could complement existing physical privacy mechanisms. For example, 7 participants pointed out that when the notification shows, "*the person is behind me, looking towards me*". Because "*I see [when] a person is in front of me. What we [are] really worried [about] is over the shoulder*" (P10). When asked to guess a potential intruder's gaze direction, participants estimated that they must not be viewing from directly behind because they considered their back as a natural obstacle that would block intruder's sight.

3.4.2 Workflow and Protection Model

When asked about how notification and privacy control mechanism might work together, participants' responses were divergent. Nearly half of the participants liked to use both notification and privacy protection. For example, P2 expected protection to follow notification: "*If the red code [notification] shows up, then you have to practice those techniques immediately*". P6 expected that protection would be enabled by direct user interaction after a notification: "*When I see the sign [notification], I just tap a button or something, and then the screen changed to one of the four [mechanisms]*". The way protection is triggered may be dependent on the user's level of trust of the system, or task sensitivity. P3 thought "*People might be lazy and just rely on the tool, let's be honest, if the tool was reliable*", while P8 thought "*In every situation, I don't rely on machines*". For task sensitivity, P11 stated "*If not that private, rely on the system; if it is extremely private, I want to control it myself*", while P2 said "*auto comes first when it's extremely private…manual when I believe it's not that really private*".

The remaining participants felt that either notification or control was needed, but not both. People that prefer notification may be annoyed by the interference protection mechanisms bring. P10 said "*It can be notification only… I would be very reluctant to*

introduce this [privacy protection] automatically for anyone, just stuff, you know, disappearing, I'd rather have notification, and maybe on demand." P6 also said "*When I'm checking my bank account, suddenly it changes to this way, I cannot see anything, it will make me angry*". By contrast, P5 felt that privacy protection could stand on its own: "*I feel that I'm being notified when it [privacy protection] turns itself on*" (P5). In this case, providing the option for the user to override the system's response was regarded as essential.

3.4.3 Design Implications

In this section we highlight five design guidelines that have emerged from the study. They are designing notification mechanisms to capture attention, being careful about superfluous notifications, tailoring designs for specific contexts, and allowing user control and customization of notification and privacy control mechanisms:

- **Design notification for attention**: Salience is considered as the first requirement of an effective warning [103]. Coarse and fine-grained notifications are better candidates by this standard. Our results corroborate with previous research [16] in that colour coding not only enhanced the saliency of warnings, but was also better in communicating risk than black-and-white designs (simple notification). Using other modalities such as sound and vibration in parallel with visual notifications might enhance attention. As Edworthy [35] suggested, in addition to grabbing attention, another role of notification is to "convey information the user needs". One important reason that radar design was considered useful is that the user could locate the potential threat from the literal representation of position and gaze direction. This information might be incorporated into metaphorical designs to increase their usefulness.
- **Design notification against "crying wolf":** Frequent notifications are likely to be ignored and could also disrupt the user's work. The system should only notify when there is a real threat that privacy might be compromised. All proxemic dimensions should be considered. For example, even if the distance between the user and potential onlooker is very close, if the onlooker is not looking towards the device, or

the onlooker is in a position of trust, or there is a physical barrier between the device and the onlooker's line of sight (e.g., back, wall), this situation shouldn't be considered as a threat.

- **Design for work context:** Participants chose distinct notifications or privacy control mechanisms based on the needs of a specific context. If it is for personal use, participants were more tolerant of interference. If it is for work, they valued productivity. For example, although P5 rated the radar design as the most useful, he added "*It is more distracting if you are trying to work. I probably wouldn't use this one on my work*". P12 rated Mask as her favorite mechanism. But when it comes to work, she said "*No I don't like it. I need to see the whole thing [X-ray picture]. I need to see it while working even though somebody might pass by and see it*".
- **Design for control:** Although participants had distinct perceptions of privacy, their choices for a specific mechanism in a specific task were to reach "a good balance of convenience and control" [61]. Grayscale, Dim and Mask are all fine-grained controls. However, they could achieve all-or-none control by immediately removing all hue, blacking out the screen or eliminating visible areas. Selective hiding could also become a fine-grained control by allowing the user to specify the type of information to be hidden. In case of emergency or for extremely sensitive data, coarse-grained control might be employed for short periods of time, while fine-grained control has better support for variable and less drastic privacy needs.
- **Design for customization:** For notification, different individuals may react differently to the same level of risk. As a result, the user might determine the desired frequency of notification based on their tolerance to mild or severe risk. The use of privacy control mechanisms may also vary depending on perceived task sensitivity and user preference. Users should also be able to select the protection model (implicit/automatic or explicit/user-driven protection).

3.4.4 Social Implications

In our study, participants took social appropriateness into consideration when trying to manage privacy. One benefit of the proposed privacy protection mechanisms was noted

by P4: "*Say a friend came over and want to talk. It's kind of rude maybe to shield it [tablet]. But if something like this [privacy protection mechanisms] kicked in, then it could be good and effective*". Another example of social considerations occurred when we asked participants to evaluate a set of notification designs similar to coarse notification (B). One of them (B3) had an icon that was interpreted as "*spy*", "*thief*", or "*criminal*" by participants. P6 explained the reason he didn't like it is because "*It means you don't respect a person. If I put it here, then suddenly this person comes to me and asks 'what's this? Am I a spy?' how could I tell him? Although it looks cool*". P7 also described this design as "*not friendly*" and that "*People will think you regard them as enemies and bad person*". Kindberg et al. categorized users' rationale for ranking different designs of technology as "trust-oriented", "convenience-oriented" and "socially-oriented" [58]. They suggested that features that enforce social protocols should be considered as important as other features. Patil and Kobsa also discussed the social perspective of privacy, the violation of which might cause potential embarrassment or breakdown in relationships [71]. Our results are in line with their theory.

3.5 Design Evaluation in Healthcare Context

Privacy issues in the hospital context are a topic of great interest in practice. To gather feedback on our proposed privacy management system in a more applied domain, we conducted a semi-structured interview with two healthcare professionals in a local hospital.

Figure 14 Interview setting: a hospital reading room.

Specifically, the goals of the interview were to 1) understand a context where the digital privacy management system might be used, 2) extract scenarios grounded in reality for evaluation and further study, and 3) collect feedback for notification and privacy protection mechanism designs from a practical perspective.

The interview was conducted in a reading room in the hospital where healthcare professionals open patient charts, check X-ray/ CT/ MRI images or radiology modalities and so on. Both participants were female between 40~55 years old and employees from the hospital. One of them was a radiologist (P1) and the other was an epidemiologist (P2). When one question was asked, two participants answered it in turn. To collect feedback about privacy system designs, color-printed pictures with a sample notification showing on the top right corner of an electronic health record and with different privacy protection mechanisms applied to the same health record (see Figure 8) were shown to the participants and the concepts of how the designs work were briefly explained. The interview was audio-recorded and fully transcribed. We are aware that this interview is

limited in its small sample size and the location where the interview was conducted: the medical specialty of the two healthcare professionals were not representative enough to cover a wider range of mobile devices users in the healthcare domain. It would be better to further collect feedback from nurses, physicians whose jobs require more dynamic use of mobile devices with potential privacy threats; also the location of the evaluation was in an enclosed room which didn't match the real usage environment. In addition, we used paper prototypes which lacked the interactivity that the tablet prototype had that the professionals could only evaluate based on imagination. However, we believe some qualitative feedback from workers in their working environment would still help uncover differences of a work context and a personal context in terms of privacy system designs. Several themes emerged from the transcription:

Potential Privacy Scenarios

- **Patient privacy among healthcare colleagues**: P2 described a scenario where paper based charts or stacks of films were dispersed "*here and there and everywhere*" in the consultation room that co-workers who were not on the care team might see patient's information. She said: "*So the privacy wasn't so much about someone from the public seeing something. It's about that if you have this stack with images or whatever and I work here, I could go and look at somebody else' stuff which I really shouldn't*". P1 echoed the similar issue in the reporting room due to the nature of group care environment among physicians, technologists, nurses etc.: "*we have five techs running in and out, and you're reporting 50 cases a day, and they see everything coming in. They may not be names or anything like that, but they can see stuff.*" Nonetheless, P1 pointed out that in order to improve quality by getting second opinions as well as avoiding making mistakes, consulting colleagues who are not listed as a provider and revealing patient information are acceptable practice in the hospital.
- **Patient privacy in emergency room during rounds**: P1 mentioned another scenario in the ER wards with multiple beds with curtains between. According to P1, it is possible to overhear a doctor's talking but seeing paper/charts are unlikely. P2 added in some situations doctors have a cart and they carry the charts as they do

rounds or they do rounds at nurse site. The cart is usually supervised by nurses as charts come off and go back on.

Notification Design

Participants were concerned that frequency of notifications in a crowded environment like hospital would disrupt work a lot. For example, P2 commented: *"Say you had your tablet, and Shawn walks by and it warns you, and another technologist walks by and it warns you. Oh my gosh, the doctors are going to throw the tablet on the floor. Because it pops up all the time… No no no, it disrupts.*" When informed of the possibility of identity recognition (e.g., the system only alerts tablet user when the identity of the onlooker is not authorized), P1 noted: "*that would have to be the way*".

Privacy Protection Mechanisms

- **Grayscale**: P2 thought removing color would lose essential information embedded in the figures: "*For the clinician, you have just removed information. The reason of having the color is the information. Now I have to figure out the legend. Forget it.*"
- **Dim**: Although participants understood the principle behind this design, they thought protecting privacy at the cost that the user can't see is not acceptable. For example, P2 stated: "*I can see it would be a terrible nuisance if you were trying to review it. If you're working, you need to see it… Whether people are coming and going or whatever. You're either using it or you're not. It's not useful the epidemiologist just looks at the data. You have to work now to get the data… Physicians want everything to be as easy as possible.*"
- **Selective hiding**: This seemed to be the only design that might be applied to the health contexts of our participants. As P2 said: "***You need to keep the clinical data. You can't compromise that****. What you need to mask is the personal data, not everything.*" Selective hiding allows for hiding the personal identifying information while preserving clinical information that professionals requires continuous access.
- **Mask**: As this design covers most of the screen content, it was also considered not useful for their work environment.

Implications for Healthcare Scenarios

- **Privacy/security practice interrupts workflow**: P1 talked about how the system time out which serves to protect data security and privacy would affect her work. "*Everything is timed out… Oh it's so annoying. You get a patient half done and you ran and then you come back, login again…I got a memo viewer, I got my PAC [picture archiving and communication] system, and I got my CAD [Computer-aided Detection], and as you can see they all timed. So I have my chair on rollers to run around and hit the mouse 'cause I don't want them to time out. It's nuisance. It really is.*" P1 also noted how access control in a collaborative environment hinders workflow: "*the hospital cracked down a while ago that when you sign in with your credentials …for audit purposes, they know who did what. So it created problem of workflow in areas where people would use the same work station because you've got people who has to login and logout for the next person to come in… When it's a collaborative environment, it's a pain.*"
- **Workflow takes precedence over privacy**: In a work-related context, getting the work done is the first priority. Duffy described the life of nurses as "people who structure our professional lives around efficiency and timeliness" [34]. Our participants repeatedly mentioned that working information can't be compromised for privacy requirements and disruption to the existing workflow would negatively impact or even prevent the technology adoption in workplace.
- **Be sensitive to the users' cognitive burden**: If privacy controls work on top of existing interfaces, users' cognitive load should be taken into consideration, in a manner that is sensitive to the context of use. For example, P1 commented: "*It would be how often it disrupted you. Even for this [protection mechanisms] coming on and off would be disrupting, visually. If you only see a few patients a day, then you're going to remember. But if you are seeing 200… that's craziness. Then if you get that [the system] in addition… We do a big volume here.*"

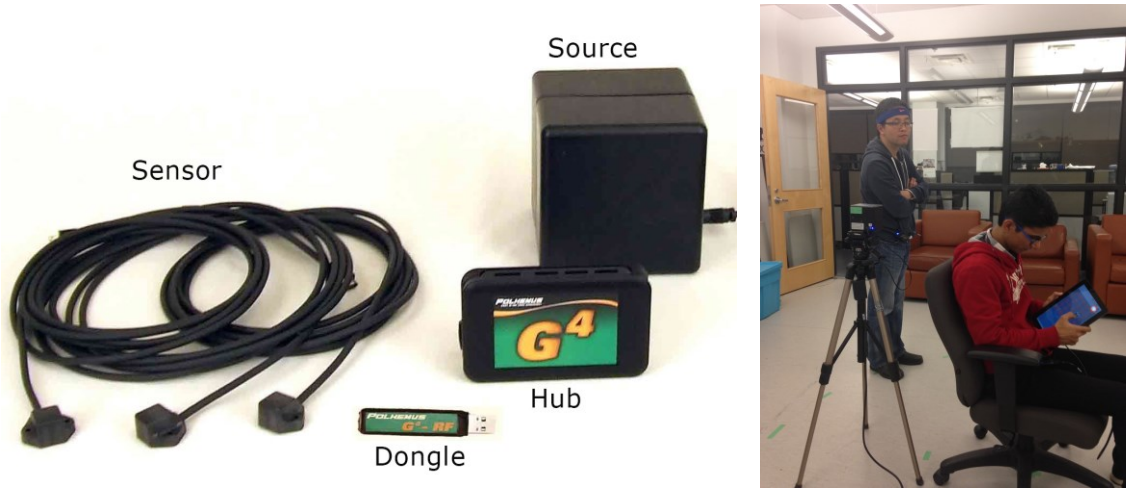
These implications echoed the inherent privacy-utility tradeoff recognized in previous work [15, 67], especially in a collaborative environment. It also supported the general design guideline we identified earlier that productivity is preferred over privacy in work

contexts. Moreover, it enriches our design guidelines by noting the impact of cognitive burden in work contexts which could have been overlooked in personal contexts.

3.6 Proof-of-concept Prototype Development

With the feedback from the WOz study and the healthcare professionals, we implemented a working prototype for the purposes of the study that monitors potential shoulder surfing events around a tablet computer. The prototype calculates the relative distance and orientation between the device and a designated onlooker to monitor potential privacy breaches in real time (see also in [105]). When the onlooker is approaching the personal zone (<5 feet) of the user, and is oriented toward the tablet (within a 60° field of view, at which shapes and icons become recognizable [56]), a shoulder surfing event is triggered.

3.6.1 Tracking Technology



A B

Figure 15 Proof-of-concept prototype demo. A. Polhemus G4 motion tracking system. Figure adapted from [77]. B. Test Polhemus G4 setup with one sensor attached to the tablet and one attached to the back of the onlooker's head.

We used Polhemus G4 (see Figure 15, A) to keep track of proxemics data. G4 is a 6 degree-of-freedom electromagnetic motion tracking system which features an update rate of 120 Hz per sensor, less than 10 milliseconds optimal RF communication latency, a

recommended range of 6 feet away from the source, and tracking accuracy of 0.5 degrees RMS for orientation and 0.08 inches (0.20 cm) RMS for position in 3.3 feet (1 meter)'s range [76]. The basic G4 system is comprised of a source, a System Electronics Unit (Hub), a sensor and a RF/USB module (RF dongle). The source generates magnetic field within a recommended range of 6 feet away from the source. The sensor's position and orientation is measured and computed by the hub that it is connected to. The hub then transmits the data wirelessly to the USB dongle which is attached to a host computer and delivered to a Polhemus native software (G4mfcTCP, see Figure 16).

The sensor data received from Polhemus G4 includes hub ID, sensor ID, frame number, position data represented in Cartesian 3D coordinates X, Y, Z with centimeter as unit, and orientation data represented in w, x, y, z as a quaternion. The parameters in a quaternion represent both the axis around which a rotation will occurs and the angle of the rotation. With the X, Y, Z readings from two sensors, we can calculate the relative position (distance) of the two sensors. Similarly, with the w, x, y, z readings, we can calculate the relative orientation (degree) in real time.

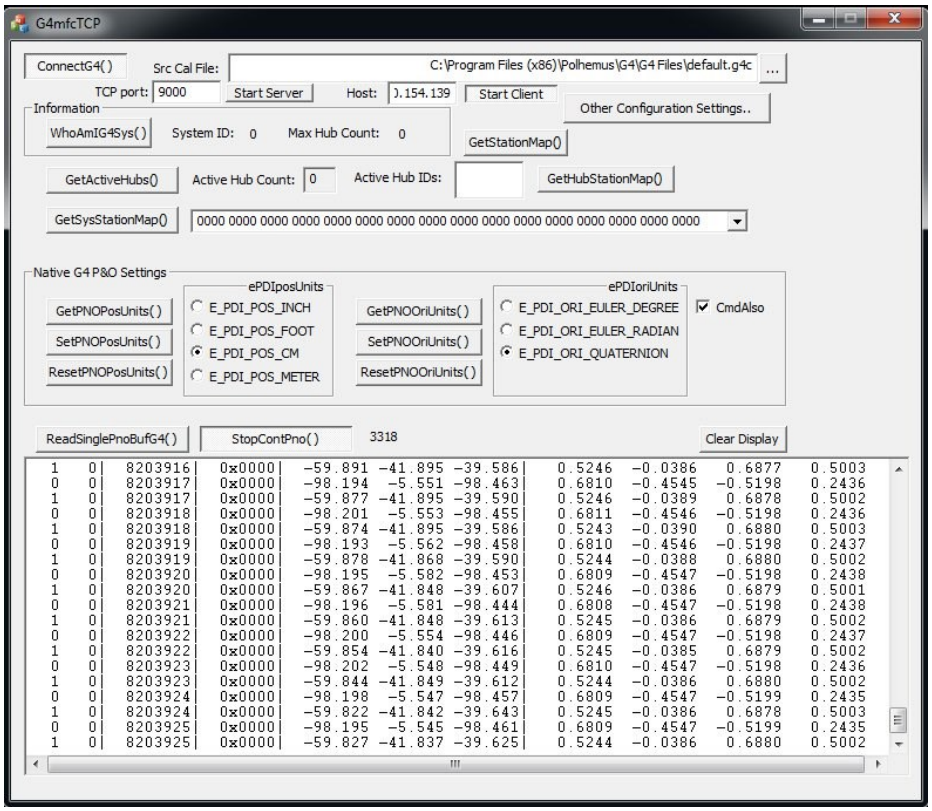


Figure 16 Screenshots of user interface of Polhemus G4 native data streaming application G4mfcTCP.

3.6.2 System Architecture

Two Polhemus G4 sensors tracked the tablet and the onlooker respectively (while this configuration is not proper for real world deployment, it is useful for controlled evaluation). Sensor data is transmitted through a portable hub wirelessly to a central server that logs the data (through the G4mfcTCP program) and forwards it to a custom application that calculates the distance and relative orientation between the sensors and determines whether the proximity conditions are met. The central server was implemented in C# with the .Net framework. Once a shoulder surfing event is detected, a Node.js server communicates the event to a client (on the tablet) using the WebSocket protocol (see Figure 17). The prototype does not consider occlusion by the person using the device in this calculation.

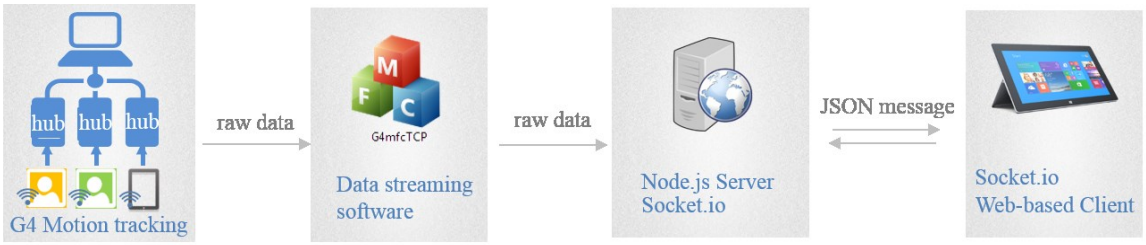


Figure 17 Proof-of-concept prototype system architecture.

On the tablet (Windows Surface Pro 2), two task-specific applications were developed using HTML5, CSS, and JavaScript, with variants supporting each experimental condition. Depending on the condition, a notification may pop up and/or a protection may be applied to the contents on the tablet. Aside from automatic protection, a manual protection mode allowed tablet users to decide when and for how long to use a protection by clicking a button. System behaviours could be overridden via toggle buttons for enabling/disabling notification and protection.

We explored the design space of glyph privacy notifications and visual content control mechanisms in this chapter. The WOz methodology allowed us to understand the tradeoffs of each design and derive design guidelines without having to develop a fully functional prototype for every design. We arrive at a proof-of-concept prototype in the end. In the next chapter, we will present the study design for evaluating how this prototype works in actual usage.

CHAPTER 4 METHODOLOGY

In the preliminary design exploration, we learned that privacy notifications favoured an iconic rather than literal representation, and that the most suitable protection technique varies with both context and content attributes. These results help make informed choices when evaluating dynamic proxemic-aware mobile content privacy management systems in a more controlled and focused context. However, the design exploration is limited in several ways: first, people's predictions about their 'would-be' behaviours are not always reliable. We would like to further explore people's behaviours and feedback about the system in actual usage. Secondly, with a relatively small sample, the relationship between notification and protection and how it might impact people's privacy decisions is not yet clear. Lastly, a system that works for individual privacy management might not necessarily support collaborative tasks. In this chapter, we present the methodologies used in a second controlled study investigating how proxemics might mediate privacy management interactions in actual usage for both individual and collaborative tasks.

4.1 Research Questions

In this study, we consider the following research questions:

1. How do people physically manage mobile content privacy on their mobile devices?
2. How could a digital privacy management system (privacy notifications and protection techniques) be designed to work with physical privacy management mechanisms?
3. What are the roles of privacy notification and protection techniques respectively and how could they work together to best support mobile content privacy management?
4. How might a digital privacy management system be designed differently to support individual tasks versus collaborative tasks?

4.2 General Study Design

We chose a controlled lab study for two reasons: first, our proximity and privacy-aware prototype is not feasible to deploy in a field setting due to the motion tracking system we used, and implementing a mobile approach (relying on a mobile device's camera and onboard sensors, for example) is beyond the scope of this work. Second, in the lab we can observe a range of behaviours within a reasonably short time frame in response to consistent privacy scenarios; this experimental control allows us to isolate the impact of different design choices.

To motivate participants to manifest diverse privacy management behaviours, we designed a game scenario with successive privacy breaches for participants to handle while doing a primary task (playing the game). It was intended that the competitive nature of the game would elicit realistic privacy-related behaviour, albeit not directly comparable to more subtle behaviours we might see outside a game context. The game also allowed for repeated and consistent privacy breaches over a short period, permitting an analysis of emergent behaviour patterns. We also used an everyday online banking scenario that most people can relate to, to understand how the system might support more real-life tasks. To explore the system's use in collaborative tasks, we designed a third collaborative banking scenario. All three categories of task are described in detail below.

To explore the different roles of privacy notification and protection techniques and how they might be used together to support privacy management, we vary the use of notification and protection in four conditions: no notification and no protection (NN), only notification with no protection (YN), no notification with protection (NY), and having both notification and protection (YY). The general study design is a 2 (task type: individual versus collaborative) * 4 (privacy mechanism type: NN, YN, NY, YY) within subjects design. Due to time constraints, each participant only experienced a subset of conditions and the condition order was counterbalanced across participants (See Table 3 and 4). For both individual and collaborative tasks, we used the NN condition (no digital privacy mechanism support at all) as a baseline to understand the effect of the digital privacy management system on the existing physical privacy management behaviours

people have. There are potential issues with this study design: for example, the 4 conditions for solo tasks are distributed across two different activities (the game and the individual banking), which makes participants' comparisons and our ability to attribute any differences in attitudes and behaviours to different configurations somewhat problematic. For collaborative tasks, each participants only experienced 3 out of 4 conditions but were asked to rank and reflect on all the conditions, which is also somewhat unreliable. We mitigate the issues with counterbalancing the treatment orders across two activities for attitude analysis, and comparing aggregate behaviour patterns for each condition only for a given activity. Considering the effect of learning and fatigue, we believe our study design is a reasonable compromise between feasible timeframe and sufficient stimulus.

4.3 PARTICIPANTS

We recruited participants by inviting members of the Dalhousie University community who subscribed for the university daily digest via email (notice.digest@dal.ca). Members of this mailing list constitute a diverse group of faculty, staff and students.

Table 3 Sample study order for game and individual tasks counterbalanced across 26 participants. Each participant experienced all 4 privacy mechanism configurations across two activities. Light blue highlights the 'NN' baseline.

Participants				Game (simulated) Activity		Individual (real-life) Activity	
				Task1	Task2	Task3	Task4
P1	P9	P17	P25	NN	NY	YN	YY
P2	P10	P18	P26	YN	YY	NN	NY
P3	P11	P19		NY	YY	NN	YN
P4	P12	P20		NN	YN	NY	YY
P5	P13	P21		YN	NN	YY	NY
P6	P14	P22		YY	NY	YN	NN
P7	P15	P23		YY	YN	NY	NN
P8	P16	P24		NY	NN	YY	YN

Participants were required to use tablet on a monthly basis, have normal or corrected-to-normal eyesight, and sign up together with a partner they are familiar with. Piloting suggested that familiar pairs would be more comfortable and engage more fully in our competitive and collaborative tasks. Each participant was compensated $20 (See Appendix **M** for participant payment receipt).

Table 4 Sample study order for collaborative tasks counterbalanced across 13 groups. Each group experienced 3 out of 4 privacy mechanism configurations.

Groups			Collaborative Activity		
			Task1	Task2	Task3
G1	G7	G13	NN	YN	NY
G2	G8		YN	NN	YY
G3	G9		NY	YN	NN
G4	G10		NN	NY	YY
G5	G11		YY	NN	YN
G6	G12		YY	NY	NN

We recruited 26 participants (14 female, 12 male). Participants averaged 28 years in age (range 18-46) with 10 undergraduate students, 9 graduate students, and 7 were faculty or staff. 12 participants were from Computer Science, the rest were from across the campus (e.g., art, social science, engineering, medicine and biology). 9 pairs were friends, 3 pairs were family (husband and wife), and 1 pair were colleagues. 19 participants used iPads, 6 used Android tablets and 1 used a Windows Surface. 15 participants had used tablets for more than 1 year. 19 of 26 participants used tablets on a daily basis. On average participants used tablets 10 hours a week, 64% for personal use, 24% for study and 12% for work use. The main locations to use tablets are home, workspace (office, school, lab) and public places (buses, airplanes, coffee shops, libraries, and restaurants).

4.4 Study Methodology Details

4.4.1 Study Procedure

The study was conducted in the middle of an open lab where other researchers might be quietly working and occasionally passing by. The total study was designed to take about 2 hours. Participants first gave consent to the study (Appendix A) and filled out an online background questionnaire prior to the study (Appendix B). Two researchers greeted participants, provided them with a Windows Surface Pro 2 tablet PC (10.6 inch sized screen) and seated them on a couch. Each participant pair then performed 3 activities in turn: a competitive game, a personal banking and a collaborative finance scenario. Participants completed a short questionnaire (Appendix D, F and H) and interview (Appendix E, G and I) after each activity. At the end of the study, they participated a final semi-structured interview (Appendix L). Specifically, the post-game questionnaire asked participants to rate the system used in each condition as a player in terms of awareness, protection, balance of efficiency and privacy, and overall satisfaction on a 7 point Likert scale. It also asked participants to rate the easiness of seeing the screen content as an onlooker. In individual and collaborative tasks, they also rated task realism, role play realism, and ranked their preferences over the 4 interface conditions and over Dim and Mask. The follow-up interview asked participants to explain their choices, reflect on privacy strategies used and differences from real-world experience. The final interview collected feedback on various design aspects (e.g., notification versus protection, automatic versus manual protection, individual versus collaborative scenarios), potential usage scenarios of the system, concerns, and suggestions for improvement. All the questionnaires and interviews were done independently in separate rooms except the interview after the collaborative activity, for which both participants reflected on their experience together. See Figure 18 for the overall study procedure. We videotaped the study, captured the tablet screen and took hand written notes.

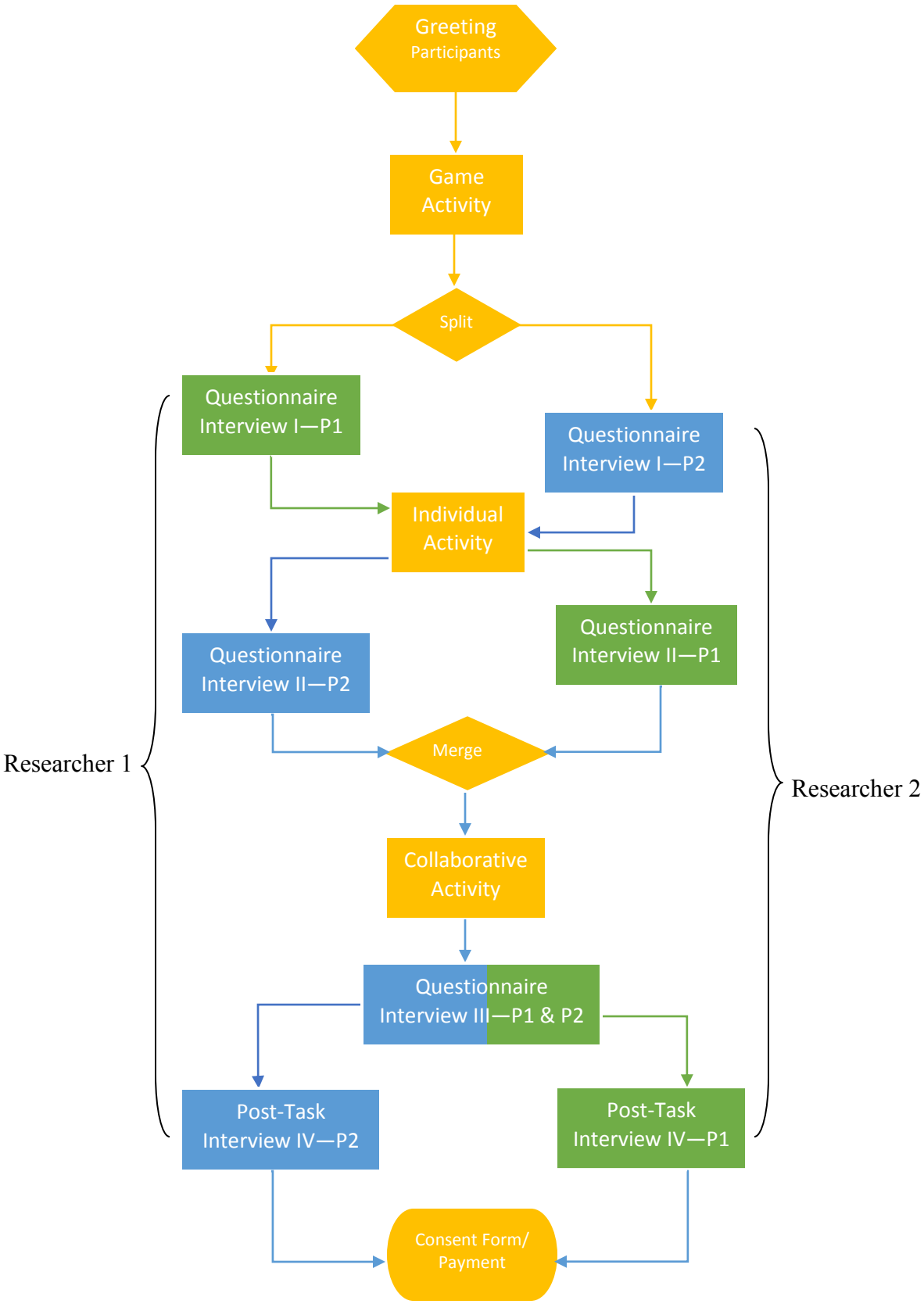

Greeting
Participants
Game
Activity
Split
Questionnaire
Interview I—P1
Questionnaire
Interview I—P2
Individual
Activity
Questionnaire
Interview II—P1
Questionnaire
Interview II—P2
Merge
Collaborative
Activity
Questionnaire
Interview III—P1 & P2
Post-Task
Interview IV—P2
Post-Task
Interview IV—P1
Consent Form/
Payment
Researcher 1
Researcher 2

Figure 18 Flow chart of the study procedure.

In order to study privacy management behaviour, we introduced a potential onlooker for each task to trigger privacy intrusion. In the game activity, we asked two participants to play the role of each other's onlooker who tries to explicitly observe tablet user's screen. We expected the motivation to win a game against a familiar partner would encourage the onlooker's looking behaviours thus activate the tablet user's privacy preserving behaviour. In both individual and collaborative tasks, a research confederate who was never introduced to the participants and whose identity was not revealed until the end of the study acted as the onlooker (although he was made conspicuous by the headband he wore). The research confederate walked around the couch area pretending to do lab work (e.g., measurement, making coffee, working on the computer, making phone calls etc.). When participants didn't pay attention, he looked over participants' shoulders casually to trigger privacy invasion 3-5 times during each task. After the task, the research confederate took notes for observed privacy management behaviour and rated easiness to see the screen (Appendix J and K). With a confederate, we ensured the privacy threats were controllable and consistent across all tasks. By not introducing the confederate, we created a 'stranger' in a traditionally 'safe' lab setting to pose plausible threats in real-life scenarios and stimulate participants' privacy responses.

Table 5 Tablet user and onlooker configuration for all study activities.

	Game Activity		**Individual Activity**		**Collaborative Activity**
Tablet User	P1	P2	P1	P2	P1+P2
Onlooker	P2	P1	Confederate		Confederate
Notification	Simple		Simple		Simple
Protection	Dim		Mask		Dim

As shown in Table 5, we used the same notification design across all tasks. From the design exploration, participants preferred notifications that would capture attention when necessary and not distract from the primary task with subtle changes or movement. We combined attributes of A (simple, not too distracting, see Figure 6) and C (highly

noticeable when opaque, see Figure 6) into a new on/off notification (see Figure 19, A). We chose the privacy protection techniques (Dim or Mask) based on the nature of the task and feedback from the design exploration so that the techniques used could potentially best support each task (see details in 4.4.3). The instructions given to the participants before each task varied based on different study conditions (Table 6):

Table 6 Instructions for 4 different study conditions. NN (no notification and no protection), YN (notification with no protection), NY (no notification with protection), and YY (both notification and protection).

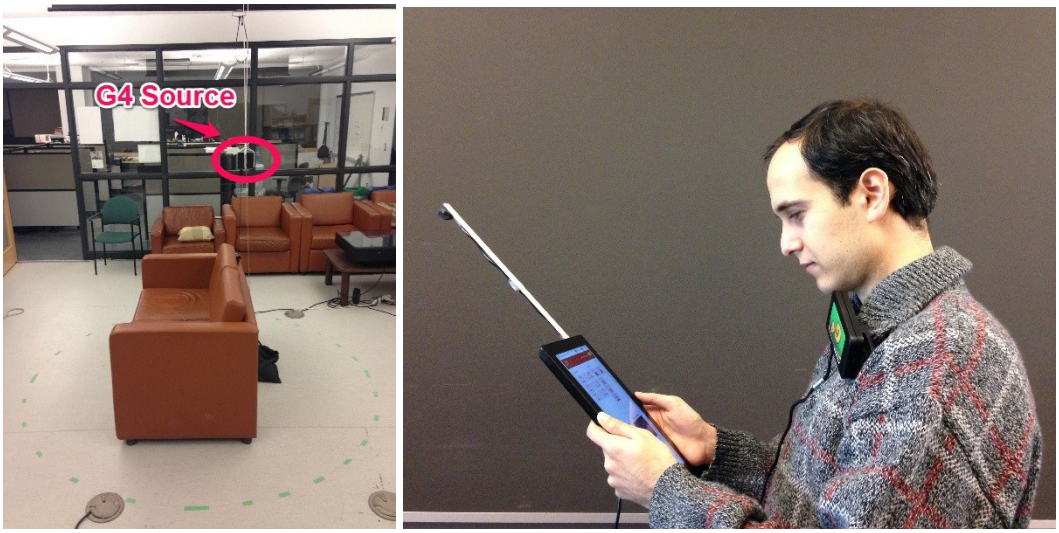
Condition	Instructions
NN	You have to rely on your own to guard your information.
YN	Every time the observer is able to see your screen, a notification (icon) will pop up and notify you that your screen might be visible. When the potential threat is gone, the notification will disappear.
NY	Every time the observer is able to see your screen, the screen will automatically[1] dim / be masked except a circle-shaped area that you can drag to where you want to see to protect the screen content. When the potential threat is gone, the screen will recover to normal state.
YY	Every time the observer is able to see your screen, a notification (icon) will pop up and notify you that your screen might be visible. Meanwhile, if you want to protect your screen, we suggest you click this button [*on top right corner of the tablet*] to turn on[2] the protection and make the screen dim /be masked. You can turn it off by clicking the same button.

4.4.2 Study Setting

A single Polhemus G4 source was hung from the ceiling with a plastic rope and secured with a sandbag on the floor. It was positioned slightly behind and 2ft (61cm) above the couch (See Figure 19, A) to cover a sensing area to a diameter of about 10 feet (3 m). The camera was attached to a tripod and placed in front of the couch with a slight angle to best videotape the whole study setting and participants' behaviours. One sensor was attached to a plank 12 inches (30 cm) from the right top corner of the tablet to mitigate magnetic field distortion caused by the tablet (See Figure 19, B). The position and

[1] Protection in the NY condition was triggered automatically
[2] Protection in the YY condition was turned on manually (automatic notification and protection were considered redundant in the previous study)

orientation readings were mapped to the center of the tablet. A second sensor was attached to the back of the onlooker's head with a headband. Hubs were attached to the collar or belt of the user and the onlooker respectively. Sensor data is transmitted through a portable hub wirelessly to a central server. All the interfaces were high fidelity prototypes developed with HTML/CSS/JavaScript.



A B

Figure 19 Lab study setting. A. The couch where participants were seated and the Polhemus G4 source deployment. B. Polhemus G4 hub was attached to the participant and the sensor attached to user's tablet.

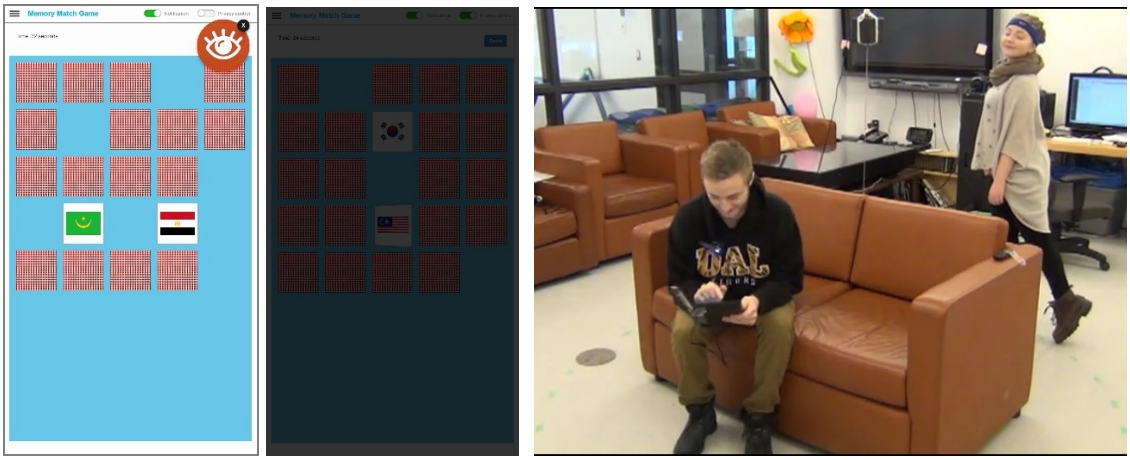
4.4.3 Task Design

Activity 1: Hide-and-Seek Game

Two participants played a game described as "competition" against each other. In each round, one participant played a memory match game (See Figure 20, A) on the tablet while hiding the screen from the other participant (onlooker). The game scenario was as Table 7. The matching game required the player to tap on two cards at a time to reveal pictures of national flags (see Appendix C for a complete set of cards). Matching pieces will disappear. The matching game is cognitively challenging and it was chosen to simulate a primary task taking up most attentional resources.

Table 7 Game scenario.

Now two of you will play a game against each other. This is a competition and you will play for two rounds in turn. In each round of game, one will be the player and the other one will be the observer. To win the game, player should try to finish a memory match game as quickly as possible while hiding the content on the screen from the observer. If you finish the game quickly but didn't protect the screen well, you will lose points for all the flags your opponent correctly recognize. If you protect the screen extremely well but the game time is very slow, you will also lose points for that. Observer will try to see your screen as much as possible and record the result. The player who gets a better score between you two will receive a $1 bonus reward.



A B C

Figure 20 Game activity setting. A. Screenshots of the game interface with a notification. B. Screenshots of the game interface with Dim protection. C. One participant (the user) hid tablet information while performing a primary task. The other participant (the onlooker) tried to see the information.

The player was encouraged to use any technique to hide the information with the constraint of remaining in the couch area. The onlooker was encouraged to use any technique to look with the constraint of observing only at specified intervals and staying outside a green-dashed circle with a radius of 4 feet to simulate the personal zone around the couch. A 'Ding' sound signaled the onlooker to observe for 10 seconds and in the following 10 seconds they recognized and circled the flags seen on a recording sheet. The process was repeated until the player finished the game. While the environment setup precludes certain privacy behaviours (e.g. stop sensitive task and move to a secure location), we argue it allows us to evaluate the efficacy of the technique when there is a real and present threat. The spatial and temporal constraints for the observer was designed to highlight shoulder surfing moments given the privacy regulation of social protocols.

After two rounds, the player and the onlooker switched roles and played for another two rounds. The player would lose points for either playing slowly or when their opponent correctly identified information (flags), and the winner of the game got a $1 compensation bonus. We used *Dim* in conditions where a protection mechanism was used, as our design evaluation suggested it would provide reasonable protection without interfering too much with the time-sensitive primary task (See Figure 20, B). The game completion time and the number of correctly/wrongly observed flags were recorded.

Activity 2: Individual online banking

Participants were asked to role play a person ("Casey" or "Jessie") who works at Dalhousie University. The scenario was shown in Table 8. This activity was done individually. Participants were given an authentic looking bank card (see Figure 21, A) with password and asked to perform two information retrieval tasks using an online banking site: to log in to the account and retrieve the last two digits of the amount paid on a particular account on a particular day or for a particular item. After finishing each task, participants told the researcher the values they found.

Table 8 Individual online banking scenario.

You graduated from Dalhousie University and are now working at Dalhousie University. You have a tablet and a RBC/CIBC account. Occasionally during lunch time you use your tablet to do online banking at your desk. Normally you wouldn't do that but today you have a couple of transactions to do. Your office is not enclosed so colleagues may pass-by in your vicinity. Financial information is sensitive to you and you don't want anybody to see it.

As we described, a research confederate acted as the potential onlooker to trigger privacy response. We used *Mask* as a protection mechanism for this activity, as it was the most preferred technique for a similar scenario in the design evaluation.

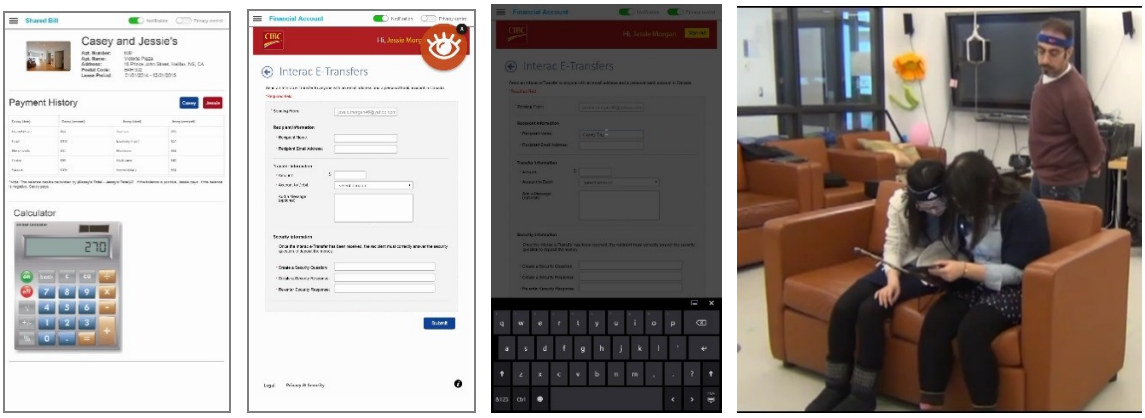
Figure 21 The individual banking activity setup. A. The bank cards for Jessie and Casey. B) Screenshots of Jessie's online bank login page. C. Screenshots of Casey's online bank login page. D. Online banking login interface with a notification and Mask protection. E. One participant performing banking tasks and a research confederate looking over his shoulder.

Activity 3: Collaborative splitting bill scenario

Using the same roles as Activity 2, participants acted as roommates sharing a bill in a coffee shop together. The scenario is shown in Table 9. In each task, participants were shown a webpage with "Casey and Jessie's" apartment information, shared bills (e.g. electricity, internet, furniture), and an embedded calculator (see Figure 22, A). They were asked to first calculate the balance with a suggested way. Then the person who owes their roommate money logged in to their bank account and paid the money using email transfer. Participants were asked to calculate and fill in the transfer information together, and to discuss realistic security questions.

Table 9 Collaborative splitting bill scenario.

You two are friends and you rent a 2-bedroom apartment together since 2014. You share a lot of bills in your daily life: for example, internet, electricity, furniture and appliances for the apartment, or restaurant, movie etc. You usually record your shared bill in an online document. After a while, you sit together to calculate the balance and pay back through online banking email transfer. Today when you are having coffee in a coffee shop, you find it a good time to split your recent shared bills with your tablet. Coffee shop are quite busy. From time to time, there are people passing by. Financial information is sensitive to you and you don't want anybody to see it.



A B C D

Figure 22 The collaborative activity setup. A. Screenshots of the bill calculation page. B. Jessie's email transfer page with a notification. C. Jessie's email transfer page with Dim protection. D. Two participants performing shared tasks and a research confederate looking over their shoulders.

The same confederate acted as the onlooker. Each pair completed 3 similar tasks with different bill values and different payers. (e.g., Casey pays for the 1st and 3rd task, Jessie pays for the 2nd task). To control the calculation procedure, a suggested way to calculate the balance was given on the calculation page and demoed to both participants in the task instructions. To keep participants engaged in the collaborative tasks, participants were instructed to: 1) calculate together. If one person does the calculation, he/she will have to explain to their roommate how they arrive at the number. 2) fill in the transfer information together and discuss a realistic security question. 3) enter their credit card information themselves rather than passing their bank card with personal data (e.g. email address) to collaborator. We used *Dim* as a protection technique in this activity in order not to interfere with collaboration.

4.5 DATA PROCESSING

4.5.1 Data Collection

We collected data before, during and after the activities using the methods outlined in Table 10.

Table 10 Data collection methods.

Phase	Instrument	Description
Pre Study	Background Questionnaire	Demographics, tablet usage habits, privacy concerns about data type/potential viewer, collaborative work experience
Lab Study	Observation Notes	Hand-writtern notes about the participants' behaviours by researcher
	Observation Questionnaire	Questions about participants' behaviours answered by the research confederate 'onlooker' during individual/collaborative tasks
	Tablet Screen Capture	Screen recordings of all actions performed by the participants on the tablet with Camtasia Relay (without cursor movement)
	Video	Video recordings of participants' behaviours performing the tasks
	Logging Data	Interaction logs (selected flags, typed bank information etc.) on the tablet; real-time tablet and onlooker proxemics data (position, orientation) captured by the Polhemus G4, intrusion events detected
	Post-activity Questionnaire	General information about participant motivation, perceived task realism, task information sensitivity in all activities; attitudes towards notification and/or protection techniques used in each task; preference over different protection techniques or combinations,
	Post-activity Interview	participants' explanations about their choices in the questionnaire; experience during the activity; feedback about the techniques used in each task, any other comments
Post Study	Semi-structured Interview	General feedback; participant perception of the relationship between physical and digital privacy management mechanisms, preferences and reasons; reflection on techniques that haven't been tested in the study; suggestions for improvement

.

4.5.2 Data Coding

Responses from the background questionnaire were summarized and tabulated. Observation questionnaires and post-task questionnaires used 7 point Likert scales. All interviews were fully transcribed.

Video and screen capture were synchronized in Adobe Premiere and placed side by side for coding. Video coding of physical privacy management behaviour was done using an iterative process: two researchers first watched all the videos independently, identified privacy-related behaviours and assigned a unique code to each behaviour. The same two researchers then compared the code lists, discussed discrepancies and resolved the differences to create a single code list. This list was then checked with privacy behaviours identified in the literature to add any missed behavioural code (e.g., be vague, facial expression). Code such as "remind partner", "help partner hide" (collaborative privacy management), and "move tablet position", "turn tablet angle" (device privacy management) were not found in the literature we reviewed. We then summarized all the participants' reported privacy strategies from the transcribed post-activity interviews, and compared the strategies with the code list. Any code in the list that was not reported by participants (e.g., facial expression) was deleted as non-verbal behaviours are often ambiguous, especially in relation to privacy intentions [6]. We settled on 5 verbal codes and 13 non-verbal codes. The final code list is shown in Table 11. One researcher rewatched the videos and coded all the behaviours using the Vcode Vdata software. It was possible that some non-privacy driven behaviours (e.g., natural body leaning) were counted. Counts of each behaviour were aggregated for each task and each participant.

Table 11 Coding for physical privacy management behaviours across the three activities.

Type	Code	Example
Verbal	Ask to leave	Saying: "*get out of here*", "this is a private discussion, I have to ask you to leave"
	Lower voice	Whisper when discussing
	Speak a different language	Use native language such as Chinese to communicate
	Remind partner	Telling partner: "*I think somebody is watching us*", "*Oops, there is a guy next to you*."
	Be vague	Saying: "*do you want to use our **regular** security question?*"
Non-Verbal	Look around	Look around to check whether there is somebody
	Eye contact/glare	Glare at the observer to deter them
	Body leaning	Lean over the tablet or lean away
	Move body position	Change sitting position to increase the distance from the observer
	Turn body angle	Change body orientation to face toward or away from the observer
	Move tablet position	Move tablet closer to the body
	Turn tablet angle	Change tablet orientation to the side
	Use body to cover	Use parts of body such as chest, arm, hand, head to block the vision of the observer
	Use objects to cover	Use objects at hand such as clothes, hair, bank card to block the vision of the observer
	User barrier to cover	Use natural barriers in the environment such as couch's seat, back and handle to block vision
	Stop working	Temporarily stop the current task to look around or whistle
	Help partner hide tablet	Help partner to draw in the tablet, or use own body to cover the tablet
	Sit close to each other	Sit close to the partner to leave the tablet less open

4.5.3 Data Cleaning

We assigned participants to different conditions (NN, YN, NY, YY) in the study design, and tried to keep activities and tasks consistent. However, the actual participant experience may be different due to the researcher's accidental mistakes (e.g., input condition NY instead of assigned YN) or the tracking technology's objective error. To mitigate the impact of these factors, we watched all the screen captures to validate whether the assigned condition was the same as the actual condition. If not, we adjusted the condition for each task. For example, if a task with YN (notification) condition ended up showing no notification on the screen at all throughout the task, we change it to NN condition for all the related data such as behaviours observed in the task. We also counted the number of times notification or protection techniques appeared.

4.5.4 Data Analysis

Video Data Analysis

Behavioural counts in the game activity were used as a major source for behaviour categorization as the number of occurrences was more frequent and the magnitude of the behaviour is more explicit than in the more real-life scenarios. Privacy behaviours were categorized both by variable (behaviour coding) to identify behavioural patterns and by case (participant) to identify individual privacy management style with Hierarchical Cluster Analysis using SPSS. Hierarchical clustering joins pairs of behaviours that are most similar based on distance calculations, and repeats the process until all behaviours are joined hierarchically. The basic steps are calculating the distances, linking the clusters and selecting a solution based on choosing the number of clusters [26]. R-analysis uses the correlation between variables to find the association among variables / attributes [85]. Q-analysis is used to cluster subjects / cases with inter-subject proximities [24].

Questionnaire Data Analysis

All the questionnaire data was entered into SPSS. For overall experience about the task or motivation, we mainly used descriptive statistics to summarize. For ratings of attitudes or rankings of preferences of different conditions, we used non-parametric statistical tests

(e.g., Wilcoxon signed rank test, Friedman test) to compare means due to the small sample sizes in our analysis.

Interview Data Analysis

One researcher reviewed all the observation notes, video annotations and interview transcriptions to capture interesting details on more than 1,000 individual notes and organized them into several themes for each activity. In the second round of review, notes from each theme were counted, compared, and summarized into results. Related themes were combined into higher-level themes.

Tracking Technology Performance Evaluation

We used logging data from the Polhemus G4 tracking to evaluate system performance, and to determine the reliability of the data for analysis purposes, as there were indications during the study that the system did not behave entirely as expected. We first corrected misinput of participant ID, task ID etc. from the researcher. Secondly, we reviewed the video files to identify the starting and ending timestamp for each task in each activity for all participants. For the first 4 groups of participants (G2, G3, G4, G5), clocks on the host computer and on the video camera were not synchronized to the second. Therefore we looked for unique synchronization points in the video (e.g., points where we can see there was privacy breach and notification popping up on the tablet screen), and compared them with privacy breach data recorded in the logging file (through several tests we found the offset to be 1m13s). We then synchronized host computer time and video camera time by applying the offset and use the time frame as a filter to extract logging data that were related to task behaviour from the raw data. We observed that raw data files from G12 were all under 20 KB, while files from other groups averaged 2 MB. Participants from G12 reported that the system didn't work well. Thus we discarded G12's logging data. We merged the filtered data set into 3 larger files corresponding to the game, individual and collaborative activities.

By looking at the dataset, we observed obvious noise pattern. We found for the tracked onlooker's position and orientation data, there were a number of occurrences with the

pattern 0 (X), 0 (Y), 0 (Z), w (0.5), x (0.5), y (0.5), z (0.5) which suggested that the onlooker was standing exactly at the position of the origin of the system's reference frame (the location of the source) and it was highly unlikely to be the case. Nonetheless, this inaccuracy will only affect the calculation of distance and relative orientation thus the system response of notification and/or privacy protection mechanisms. It doesn't necessarily mean the system responses were completely wrong. In some of the cases, the system could still respond correctly in spite of inaccurate calculation. Regarding the zero-pattern data, we counted the number of error frames in each activity, and calculated overall error rate, the percentage of tasks with a proportion of error frames greater than 50%, and the percentage of tasks with no error frames (see Table 12):

Table 12 Zero-pattern data distribution in game, individual, collaborative tasks.

	Data Type	Game	Individual	Collaborative	Total
Overall zero-frame ratio	Error frame	160415	136390	255070	551875
	Total frame	542808	390281	857274	1790363
	Percentage	30%	35%	30%	31%
High zero-frame ratio	Error rate >=50% task	14	12	6	28
	Total task	47	48	36	128
	Percentage	30%	25%	17%	24%
Non zero-frame ratio	Error rate =0 task	18	12	8	39
	Total task	47	48	36	128
	Percentage	38%	25%	22%	29%

As shown in the Table 12, overall 31% of the frames have inaccurate data.

We also corroborated the issue from participants reported data. During nine participant interviews, they explicitly mentioned that the system didn't work well for at least one of the tasks. Sometimes false positives were reported: for example P18 reported "*it [notification] is flashing all the time. Sometimes it flashes while nobody is around.*"

Similarly, P9 reported: "*I check, for example, when it gets dim, then I saw there is no one around*." Sometimes, the system missed detecting privacy breaches (false negative): P4 commented: "*sometimes… it won't tell you someone is looking at your device*." P26 also commented: "*It wasn't picking up as much. Like if there was someone around, like I only have the mask thing come up for twice for a second, and then it went away.*"

We believe the issue of tracking system accuracy was caused by the following reasons:

- **Distortion**: Real-time Polhemus G4 tracking data might be subject to magnetic field distortion due to metal in the environment (although we tried to keep the source away from metal by setting it with a rope from the ceiling, we are not able to eliminate the effect from the other metal, electronic devices in the lab).
- **Limited range**: Polhemus G4 only has limited tracking range whereas the study tasks require participants (e.g., observer in the game activity) or research confederate (e.g., in the individual and collaborative task) to leave the recommended tracking range of Polhemus (around 1.5 meters away from the source) for certain amount of time. By not allowing the potential onlooker to stay in the closest vicinity of the tablet user all the time, we hope to capture essential aspects of the real-world regarding privacy as the social protocol regulates the distance that potential onlookers need to keep from the tablet user. However, the tradeoff of this setting is that it might impact on the tracking accuracy of the device. The competitive nature of the game activity required participants to enter and leave the best tracking range frequently which may also contribute to the high error frame rate.
- **Software brittleness and testing**: the software was written for ideal operating conditions (precise sensor data), and while the implementation does try to accommodate noise in code, robustness could have been increased with further testing, more sophisticated filtering, redundant sensor data, and task-specific heuristics. Also, while we took precautions to avoid magnetic interference and range issues (hanging the source mid-air, attaching the sensor to a stick some distance from the tablet), and conducted testing to assess the system's response prior to the study, more systematic testing may have identified sources of distortion that could have been removed from the setting, and identified the need for additional sources.

This result suggests we should be careful about the potential impact of inaccurate system response on participants' behaviour and perception. On the one hand, participants might demonstrate excessive or insufficient privacy preserving behaviours than they would have done because of the false positives and false negatives. Participants might also underrate the usefulness of the system because it didn't always function as expected. On the other hand, if the system facilitated people's privacy management behaviour or participants liked the system even when it didn't work perfectly, we would expect it would be more useful if it functioned better. Also, a system that works some of the time may in fact be a welcome addition to the privacy arsenal at the user's disposal. Scrutinizing the reasoning behind participants' behaviour and rating would help us attribute the impact to the conceptual system or the real system more precisely. In conclusion, despite the imperfect system we used in the evaluation, we believe our approach is still reasonable and valid.

CHAPTER 5 RESULTS

We present results of the lab evaluation in this chapter. Firstly, we show participants' privacy concerns regarding different information types, viewers, and media measured from demographic questionnaires. Secondly, we examine the validity of our study design through feedback on motivation stimulation, role play, task design etc. Thirdly, we present physical privacy management behaviours observed and reported from the study and provide a classification of those behaviours. We then discuss how our proposed digital privacy management system might affect participants' privacy perceptions and behaviours, and feedback on the relationship between notifications of protections as well as different mechanisms of protection. Finally, we compare the difference of managing mobile content privacy at a small-group level.

5.1 PRIVACY PERCEPTIONS

As a background information, our participants were most concerned about financial and health information, and strangers as the potential viewers. They shared private data more frequently on mobile phones. They also reported that if the study were to use their real bank accounts, half of them wouldn't have participated in the first place.

Type of Information: Participants rated the level of concerns if somebody were to be viewing their tablets while accessing different types of information on a **7** point Likert scale. As shown in Figure 23, participants considered the most sensitive information as financial information ($M = 5.7$, $SD = 2.2$), followed by health information ($M=5.4$, $SD=1.4$) and email ($M=5.0$, $SD=2.1$). Participants cared least about the game data ($M =3.2$) being seen by others. With Friedman's test we found financial data has higher sensitivity than almost all the data types (e.g., email, social network chat, photo, $p<.05$) except for health data. This results show that it is a consensus across participants that financial scenario will be more likely to raise privacy concerns than other scenarios.

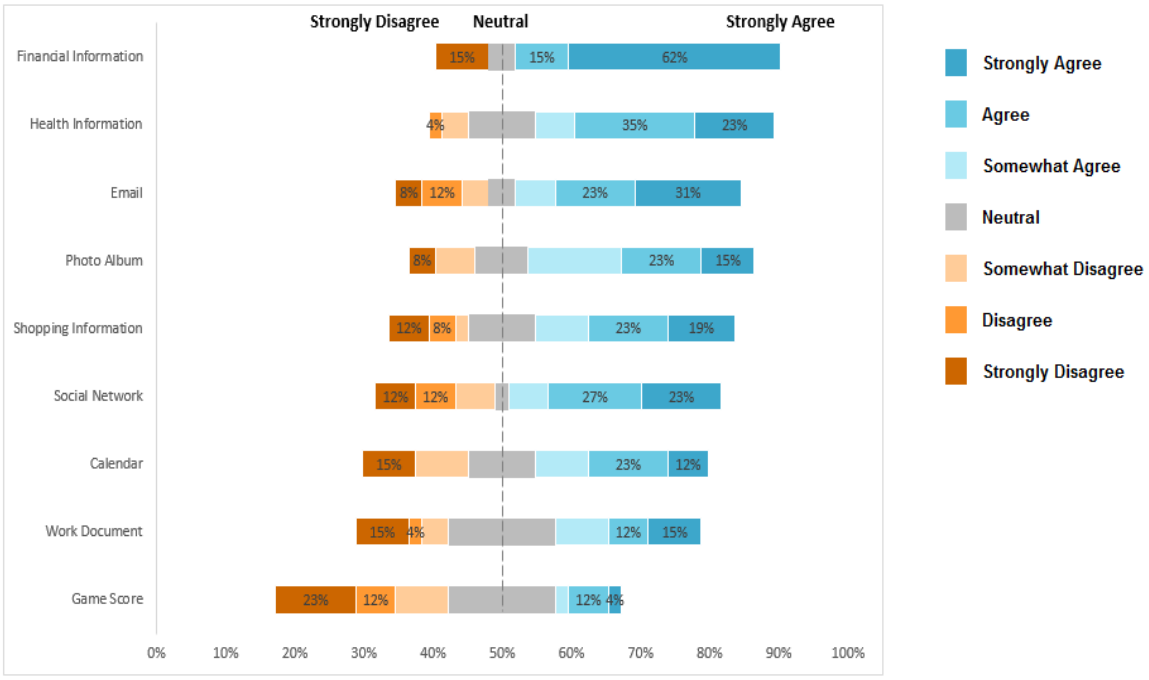


Figure 23 Privacy concern level for different types of information when accessing sensitive information on the tablet.

On the other hand, when asked about the chances of these types of information actually being seen by other people on a **5** point Likert scale (from 1 never to 5 always), game (M =2.9, SD=1.1) and photo (M=2.9, SD=1) were more frequently exposed whereas financial (M=2.2) and health (M=1.9) information were less likely to be viewed by others. This result indicates that as the sensitivity of information increases, people tend not to reveal them when others are around.

Type of viewers: Participants were more concerned about strangers (M=5.2), colleagues (5.0), and acquaintances (4.9), and less concerned about family (4.0) and close friends (3.9). Participants made clear distinctions between family members and strangers ($\chi^2(1) =5.5$, $p<.019$), and close friends and colleagues ($\chi^2(1) =6.5$, $p<.011$). Similarly, close friends and family were more likely to see participants' tablets whereas colleagues, acquaintances and strangers were less likely to see.

Type of media: When asked about the frequency to share what the participants considered as private or sensitive data via the following media, we can see in Figure 24

that most of the private data were shared via mobile phones, desktop computers and tablets. As a traditional communication media, paper is still in use. Large displays and whiteboards were designed for sharing by nature, and private information was rarely shared using these media by our participants.

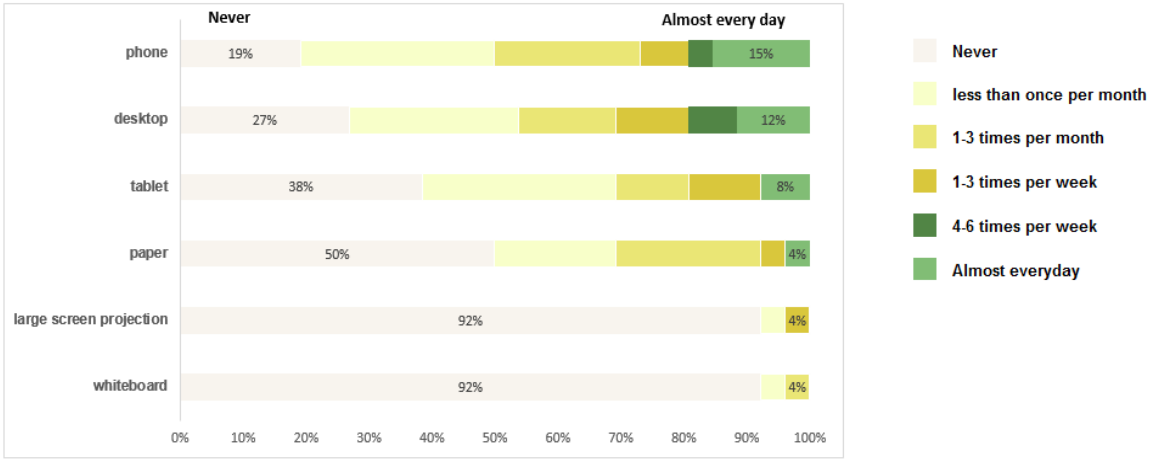


Figure 24 Frequency of sharing private information on different types of media.

Concerns about real data: When asked if the participants were willing to participate if the study were to use their real bank account, 12 said no, 11 said hard to say, only 3 said yes. While participants were of course aware that the financial scenario in our study is artificial, this suggests that it was more likely to motivate privacy behaviours than other scenarios, and verifies that the study didn't preclude participants with high financial privacy concerns.

5.2 Validity of Study Design

Self-report data indicated that participants maintained a high motivation for preserving privacy across tasks. Participants agreed that the financial tasks involved highly sensitive information. They also reported a high degree of realism: participants indicated that the financial role playing scenarios were similar to events that would occur in their own lives, and that they behaved accordingly. While we acknowledge the difficulty in eliciting

realistic privacy-related behaviour using artificial tasks, this suggests our study design is valid for evaluating privacy behaviours and perceptions.

5.2.1 Motivation for Efficiency versus Privacy

To investigate privacy management behaviours, it is essential to motivate participants to care about the data even though it is not critical data (e.g., game play) or their own data (e.g. bank account). After each activity, we asked participants to rate the motivation to complete the task as soon as possible versus the motivation to protect tablet screen as much as they can on a 7 point Likert scale (see Table 13). The privacy motivation for the three tasks was similar and strong (5.7/7 at least). The motivation to complete the tasks quickly was higher in the game than both individual ($Z = -2.84$, $p<.012$) and collaborative tasks ($Z = -3.12$, $p=.006$).

Table 13 Mean rating and standard deviation of motivation for task efficiency and privacy for three activities on a 7 point Likert scale.

Motivation	Game		Individual		Collaborative	
	M	SD	M	SD	M	SD
Efficiency	**6.62**	0.64	5.81	1.65	5.77	1.37
Privacy	6.08	1.35	5.73	1.37	5.77	1.28

The results suggested that participants maintained a high level of motivation to win the game. When it comes to realistic tasks, participants didn't rush to finish the task, but held balanced motivation for both task efficiency and protection of privacy.

5.2.2 Task Design

Quantitative rating: In the post-activity questionnaire for both individual and collaborative tasks, participants were asked to rate the realism of the task, whether they treated the role play similar to their own online banking behaviours and whether the task contains sensitive information on 7 point Likert scale. As shown in Table 14, participants thought the data used in the tasks was very sensitive, the tasks themselves realistic, and

they treated the role play similar to their own. We didn't observe any significant difference in rankings between the two activities.

Table 14 Mean rating of task realism, role play similarity with real life and data sensitivity for individual and collaborative activities on a 7 point Likert scale.

Type of Task	Realism		Role Play		Data Sensitivity	
	M	SD	M	SD	M	SD
Individual	6.38	0.90	5.77	1.39	6.58	0.70
Collaborative	5.92	1.41	6.00	1.33	6.27	1.12

Qualitative feedback: In the follow-up interviews (conducted after each of the three activities), we asked participants to elaborate on what aspects of the task were natural or familiar, which seemed different from their own experience, and whether they felt they behaved differently from how they would in their everyday lives.

Task Realism

For the **individual** online banking scenario, 21 participants considered it as "*natural*", "*normal*", "*very real-life scenario*" in the sense that the task activity (e.g., check account information), the location (e.g., do banking at work places) and privacy concerns are similar. Regarding the difference with reality, 11 participants emphasized the importance of *prevention*: they wouldn't do online banking in public unless absolutely necessary or they would strategically choose private space in public (e.g., washroom, a corner, back against wall) so that nobody could possibly be around or behind them. 8 participants talked about task detail differences: for example, passwords would have been remembered, or a different media (phone or desktop computer) used to perform the task (7 participants). For the **collaborative** roommates-splitting-bill scenario, 15 participants considered the task activity (e.g., share bill, calculate money, Interact-E transfer money) realistic because they currently or formerly split bills with friends/colleagues or roommates. 3 participants said the task location (coffee shop) was similar to where they would do this in their everyday lives, while 12 participants claimed they wouldn't conduct the activity in public places but rather at home or in the workplace. 8 participants

thought the calculations would have been done collaboratively, but the money transfer would be done alone. 3 participants reported that information such as address and calculated result was not as sensitive as passwords, email, and security questions thus they didn't care about protecting this data as much.

Role Playing

Role play did work to some extent in probing realistic responses. P15's comments exemplified the effect of role playing on participants' perceived responsibility on privacy: "*one guy was walking around. I'm not sure whether I should protect or not. I was not instructed to do so. But I feel like I should. I just felt not so comfortable with this kind of private information while someone was there*". 5 participants in the **individual** tasks reported they didn't treat the role play differently from real life, 3 of them even signed out their role's bank account after finishing the task voluntarily. In the **collaborative** tasks, participants were required to discuss a realistic security question. With the log data from the tablet, we found 10 out of 13 groups used realistic questions such as "*what is Hag's old dog name*", "*where are we going tomorrow*", "*what is my favourite thing about you*", "*what is catdog*" with answers that were shared knowledge between participants but were difficult to guess for an outsider. 1 of these 10 groups even used their real life security questions for transferring money. The remaining 3 groups used nonsense numbers (e.g., "*1111*") or very simple questions (e.g., "*who*", "*hello*"). 1 participant commented that both security questions and answers will be longer (at least 6 characters) in real life, in the task they just inputted "*1*" to finish the task quickly.

The main difference between the role play and real-life experience is the frequency of protection behaviours elicited by the study. In the **individual** tasks, 13 participants reported their behaviours were more protective in the study than real life. The major reason is being in a study primed participants to be more aware of the environment and consciously think and act in a safer manner. (e.g., "*I was very cognizant of the person behind me, and I kept it [the tablet] really close*" (P23). "*I think that* ***being in a study about privacy inherently makes you more aware of it****, like definitely more aware of here than I would be in a coffee shop*" (P24)). Other reasons include being primed by the game

task and continued to use strategies in the game (e.g., blocking with hoodie or lying against the couch), becoming suspicious about the identity of the research confederate, and considering the study environment to be less trustworthy than real work places. Only 2 participants were less protective than real life because the data wasn't real or they considered the study setting to be safe. For example, P8 said: "*Cause this is actually not mine, so I don't actually care. It made me less concerned. In real life I might be probably protecting more and trying harder*". In the **collaborative** tasks, 6 participants reported behaving overly protective. 3 again mentioned the impact of being in a study (e.g., "*we knew the point was to provide protection or privacy*", P21). 3 attributed their behaviour to the research confederate (e.g., "*he is wearing a headband*" (P21), P17 and P18 thought he was more persistent and obvious in looking instead of casually glancing).

5.3 PHYSICAL PRIVACY MANAGEMENT

One research question we had was to understand how people physically manage mobile content privacy. We observed 18 types of privacy management behaviours. We classified the main non-verbal behaviours into 5 categories and found privacy behaviours were both less in quantity and magnitude in more realistic scenarios. Reported behaviours corroborated our observation and we discovered the phenomenon of physical mechanisms dominance in the game. Reflections from onlookers' perspectives emphasized the role of awareness in privacy management and supported the usefulness of both physical and digital mechanisms. We further identified greater danger and insufficiency of pure physical privacy management.

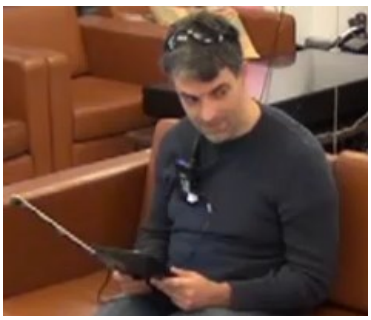
5.3.1 Observed Behaviours

Summary of Observations

We observed both verbal (5 types) and non-verbal (13 types) privacy management behaviours across the three activities (see Figure 25). **Verbal behaviours** (overall 54 occurrences, 90% of which were in collaborative tasks) included explicitly asking the onlooker to leave, lowering one's voice in discussion, speaking a different language,

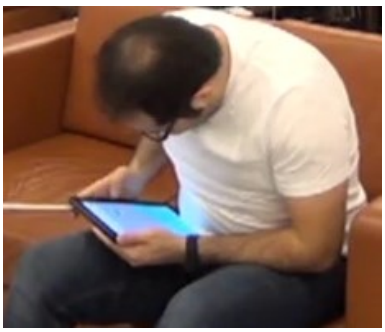
being vague when talking about sensitive information (e.g., security questions), and reminding their partner to be careful. There were also a range of **non-verbal behaviours** (overall 542 occurrences, 76% of these in the game tasks, involving frequent repeated threats and for which we explicitly instructed participants to protect the tablet from their opponents). Participants looked around to check the vicinity, leaned their bodies over the tablet, brought the tablet closer to them, tilted the tablet, changed location, and turned their body angle to face towards or away from the onlooker. To block the view of the tablet they used parts of their body (e.g., arms, hands, long hair), objects (e.g., clothes, bank card), or the environment (e.g., lie on the couch or use the back of the couch as a barrier). They also glared at the onlooker or temporarily stopped working. In the collaborative task, participants sat close together or blocked the screen while their partner worked.

Look around



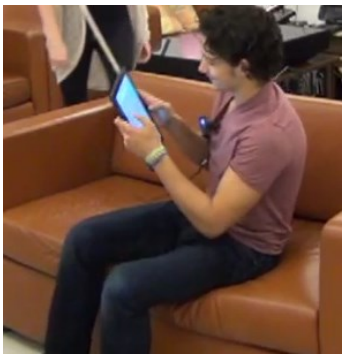
Eye contact/Glare

Body Leaning

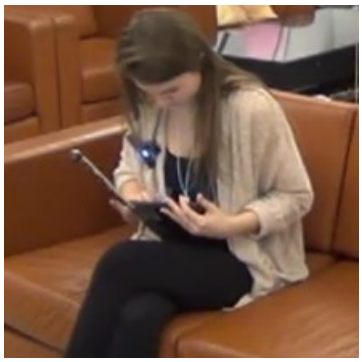


Move Body Position

Turn Body Angle



Move Tablet Position



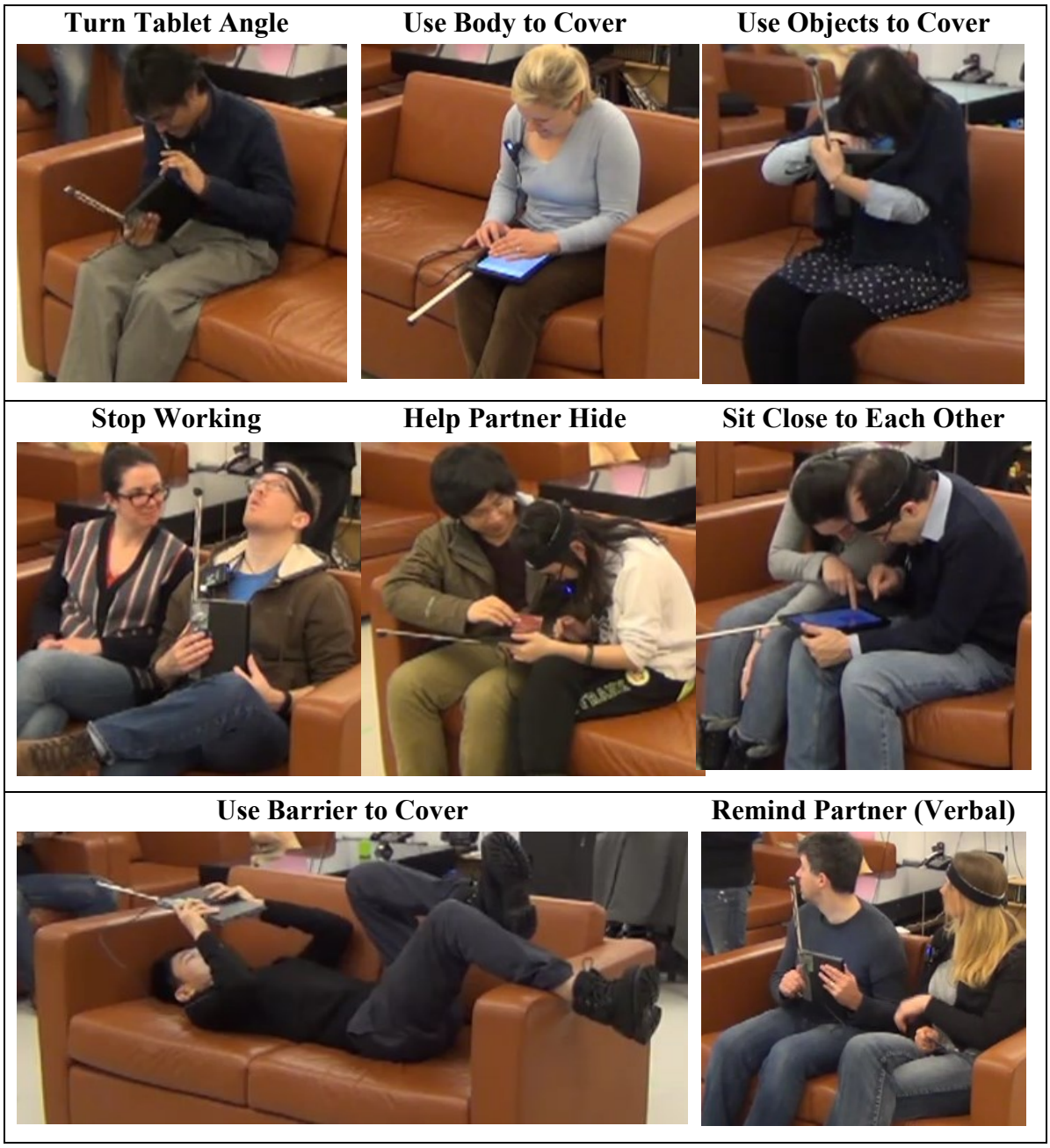


Figure 25 Screenshots of the all 13 nonverbal and 1 sample verbal privacy management behaviours observed across three activities.

Categorization of Behaviours

As discussed, the game scenario was designed to elicit rapid and frequent privacy management behaviour. We recorded the most frequent and most obvious privacy management behaviours during the game. We focused on 9 types of non-verbal

behaviours (verbal behaviours were rare in the game) to categorize. The 9 types of behaviours are: look around, body leaning, move body position, turn body angle, move tablet position, turn tablet angle, use body to cover, use objects to cover, and use barriers to cover. We used Hierarchical Clustering Analysis (R-type) with Between-groups Linkage as the cluster method and Pearson correlation as the distance measure. This distance measure calculates the Pearson correlation coefficient for each behaviour pair across all participants. Higher coefficient indicates stronger relationship between two behaviours (e.g., as one increases the other also increases), and these two behaviours will be joined first (e.g., move body position and move turn body angle in Figure 26). We chose the cluster threshold of 15 to yield clusters that best correspond with privacy processes: cluster 2 as awareness, cluster 1, 3, 4 as response, and cluster 5 as prevention. The dendrogram (see Figure 26) illustrates that behaviours seem to cluster by nature of body movement: moving body position and angle (cluster 1, we name it **macro protection**) and looking around (cluster 2, **awareness)** are large-scale behaviours; body leaning, using objects or body parts (cluster 3, **micro blocking**) require less movement and manage the immediate surroundings of the device; moving the tablet position and angle (cluster 4, **device maneuver**) merely manipulates the device itself; using barriers to block vision (cluster 5, **environment utilization**) doesn't require movement once a spot is chosen and is more preventative in nature.

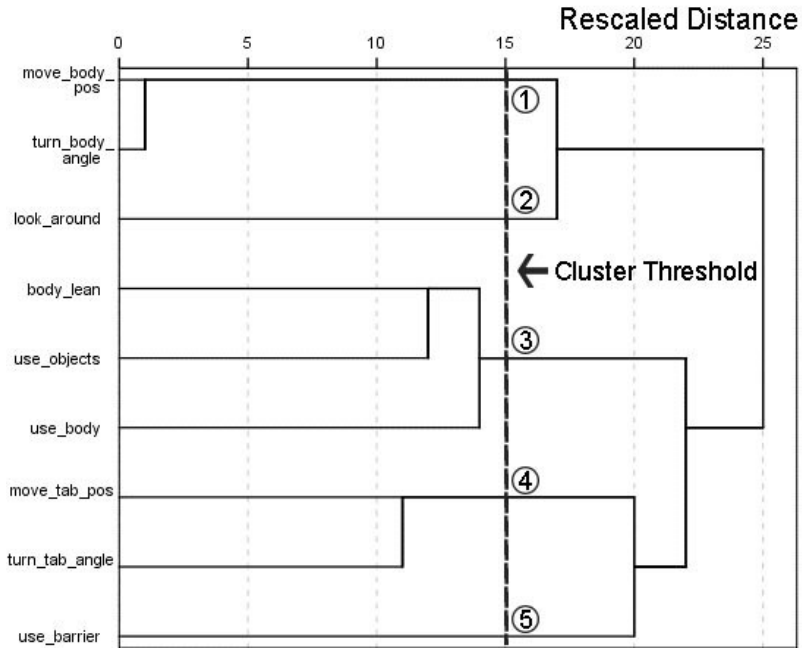


Figure 26 Dendrogram showing clusters of physical privacy management behaviours in the game tasks.

Using the 5 behaviour categories, we compared physical privacy management patterns across the 3 scenarios regardless of condition (see Figure 27). We excluded P6's data from the individual activity (as P6 misunderstood the individual task as another game, behaved "*unnaturally*", and her turning body angle frequency accounts for one third of the total counts) and G12's data from the collaborative activity (as G12 was super primed and they exhibited significantly more protective behaviours than all the other groups that would bias the total counts).

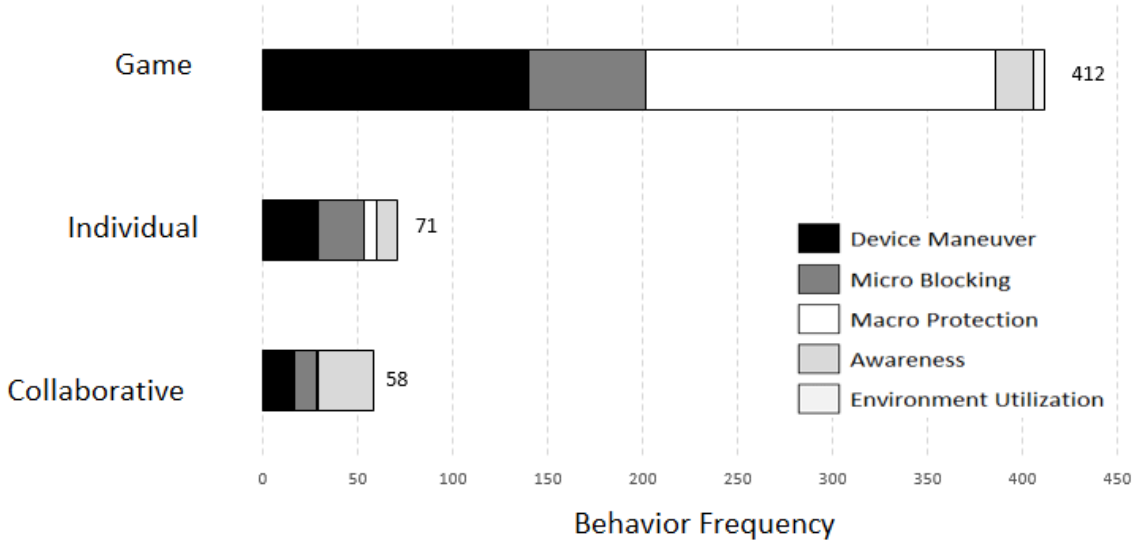


Figure 27 Total non-verbal physical privacy behaviours observed by activity.

Pattern: The Figure 26 shows that device maneuver and micro blocking behaviors were consistently used across three activities. In the more realistic financial tasks, macro protection behaviour (large-scale movement), which was heavily used in the game and very effective, almost disappeared. Instead, participants mainly relied on less conspicuous behaviours such as manipulating the device or body leaning (small-scale movement) for privacy management. This illustrates that very obvious privacy behaviours, while effective, are not appropriate in many circumstances. The collaborative task had the least number of privacy protection behaviours but more looking around. While participants may have felt the information in the collaborative task was not as sensitive as in the individual task or that collaborative tasks didn't require full

engagement of both participants throughout the task, we note that collaboration means extra capacity (i.e., eyes, ears) to monitor the environment.

Frequency: The Figure 26 also shows in the game activity, participants' overall physical management behaviours were much more than the two more realistic activities. On average, participants demonstrated 16 physical privacy behaviours in game (SD=8), 3 in individual (SD=3) and 2 in collaborative tasks (SD=1.9). In 44% of the individual tasks, we observed 0-1 occurrences of explicit privacy behaviour. The collaborative tasks took 3 times as long (224s versus 74s) time to complete but had less (2 versus 3 per task) physical privacy behaviours than individual tasks. Moreover, we observed that for the same type of behaviour (e.g., turning device angle), the movement range shrunk in real-life activities. Therefore it is possible that we missed counting some of the subtler behaviours in such activities.

Scenario-specific behaviours: while we only observed 9 non-verbal behaviours in the game, we had more diversity of privacy behaviours in the realistic scenarios. For example, in the individual banking tasks, two participants stared and tried to make eye contact when they noticed the research confederate was around and one of them stopped the task for a while and pulled the tablet against her chest. Similarly, in the collaborative tasks participants from 5 different groups glared at the confederate once each and G12 stopped working once. We also observed various **collaborative privacy management strategies**. For non-verbal behaviours, two groups of participants sit very closely to each other and 3 participants helped cover the tablet with their hands, arms, bank cards. Verbal behaviours included reminding partners of the potential intruder, lowering voices, being vague when discussing security questions and spoke a different language. For example, both P4 and P9 lowered their voice and reminded their partner in first language that the confederate couldn't have understood (meaning "*he is looking at us*") when discovering the privacy threat. P4 explained the reason for using their native language was that it was easier to communicate but also because they wanted to hide information in a subtle way that didn't require them to stop and look at the confederate. P9 pointed out that she did this unconsciously and perhaps because she was afraid her partner wouldn't hear clearly

when they whispered using English (a non-native language). P15 and P16 consciously used and whispered in their native language throughout as a barrier to preserve privacy (e.g., "*even we speak loudly, people would not understand*", p16).

Categorization of Privacy Management Styles

We also analyzed different privacy management styles that participants applied. We conducted Hierarchical Clustering Analysis (Q-type) to categorize the 26 participants based on their 9 types of non-verbal privacy management behaviours. We used Between-groups Linkage method as the cluster method and Squared Euclidean distance as the distance measures. This distance measure calculates the squared Euclidean distance for each participant pair across all behaviours. Closer distance indicates stronger similarity between two participants and they will be joined first (e.g., P17 and P19 in Figure 28).

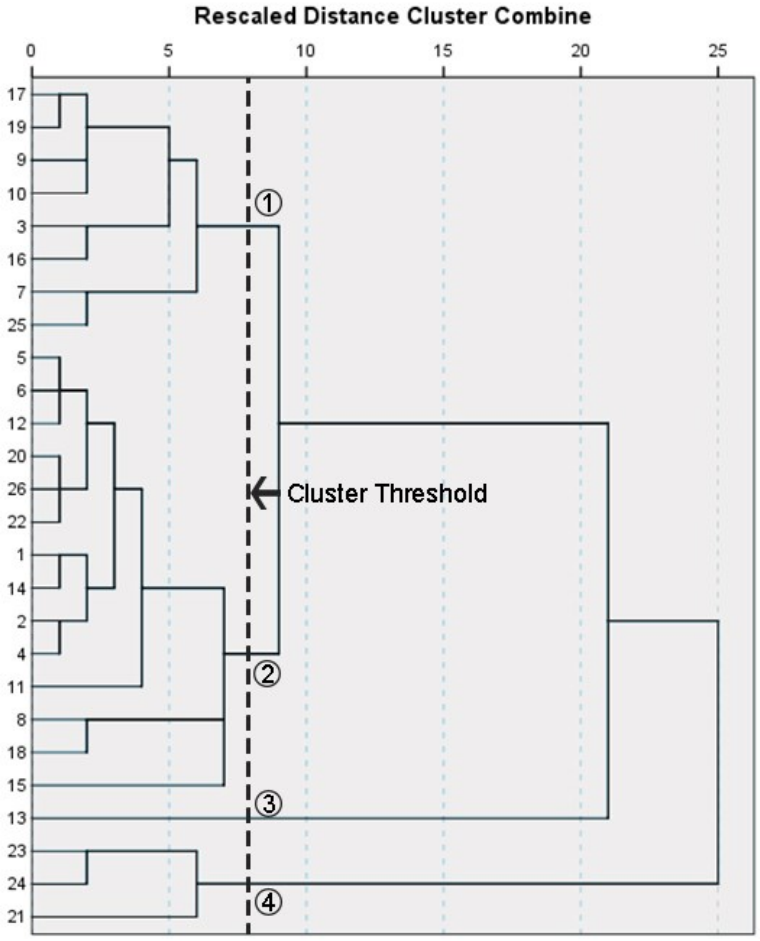


Figure 28 Dendrogram showing clusters of privacy management styles in the game tasks.

The dendrogram showed participants could be categorized into 4 clusters: cluster 1 with P17, P19, P9, P10, P3, P16, P7, P25; cluster 2 with P5, P6, P12, P20, P26, P22, P1, P14, P2, P4, P11, P8, P18, P15; cluster 3 with P13 (outlier whose behaviour is significantly different from other participants) and cluster 4 with P21, P23, P24. We visualized these four types of participants' behaviour frequency pattern with different size of bubbles: the larger the bubble, the more number of behaviours adopted by a participant (see Figure 29).

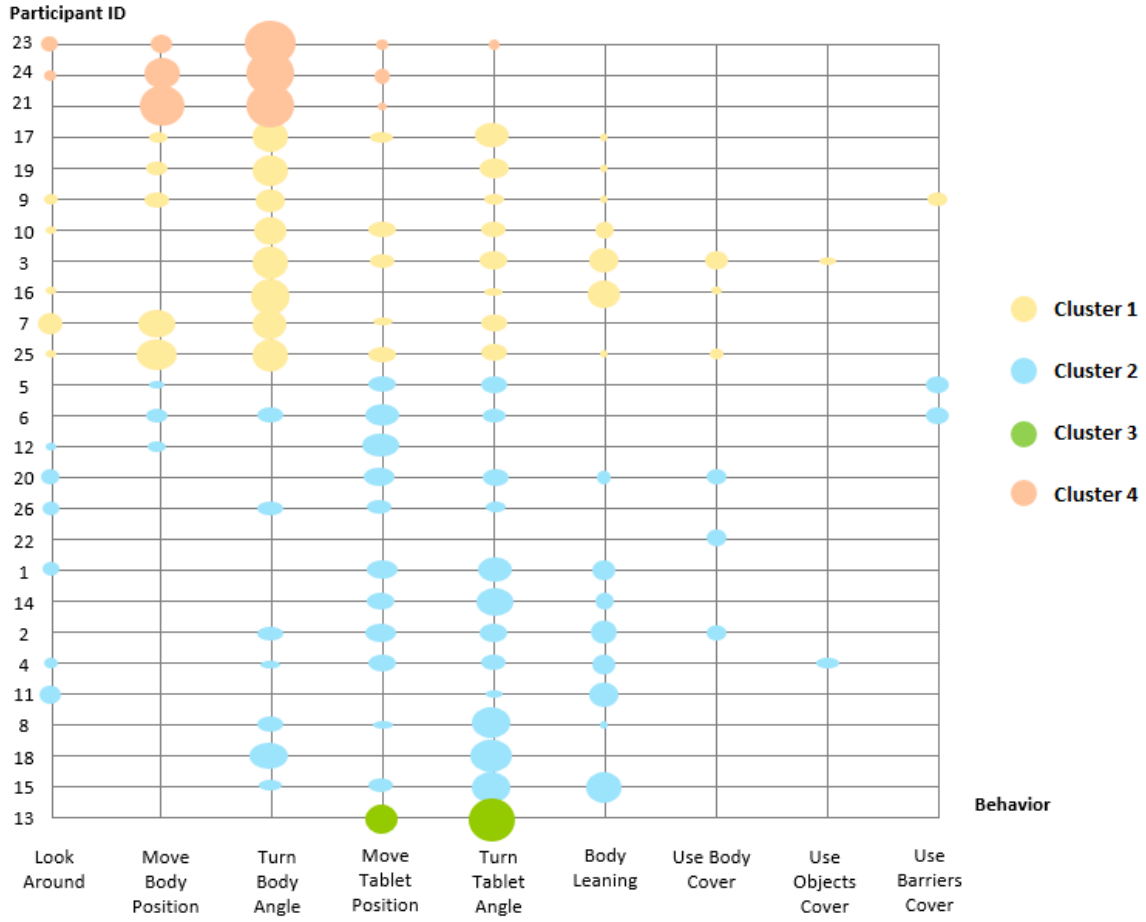


Figure 29 Four types of participants' privacy management styles. Each row represents a participant. Each column represents a type of behaviour. The area of each bubble at the intersection stands for the frequency of behaviour.

The graph showed that the first type of participants (cluster 4) frequently emphasized overt body movements. The second type of participants (cluster 1) mainly relied on a mix of moving both bodies and the device. Comparing to the previous type, they moved the

body less and the device more. The third type (the majority) of participants (cluster 2) chose to manage the device itself and the immediate space around the device (e.g., by leaning over). This required even less body movement. The last type, with only one participant P13 (cluster 3), was an extreme case that without moving his body at all throughout the game, he merely held and maneuvered the tablet and twisted it to different angles while still managed to play the game at the same time.

5.3.2 Reported Behaviours

Activity 1: Hide-and-Seek Game

Participants' self-report behaviour corroborated our observations. In the game tasks, participants reported strategies such as moving the tablet closer to the body, tilting the tablet to other directions, moving their head/whole body, using hands/arms/long hair/handle of the couch, hunching over etc. P5 who adopted a creative strategy by lying down on the couch explained: "*I just rely on the environment. Like this couch has a back, and it's very high. So I just saw that I could hide like this [lying down], I don't have to move so much… and focus on my work*." However, we also found some of the strategies were too subtle to be observed. For example, 6 participants reported paying attention to physical cues such as the "ding" or footsteps and respond accordingly. 8 participants reported slowing down or not flipping over the flags when the observer was around and working hard when the threat was gone. 3 participant reported "*do it as fast as I could*" and 1 participant carefully chose to sit in the middle of the couch to be "*far from the [proximity] circle*".

Activity 2: Individual Online Banking

Our observation showed the privacy behaviours decreased in quantity and magnitude and the confederate's observation notes corroborated this: he described participants as "*normal*", "*relaxed*" and "*no protection*" in one third of notes and used "*a minimal body movement*" for 3 participants' protection behaviours. For 7 participants with marginal privacy behaviours (1~2 times) across the tasks, most reported their strategy as "*used my body in not obvious way*", "*hold the tablet a little bit closer to me*", "*tilt a little bit*", "*not*

much" and thus very subtle behaviour. Similarly, P17 reported "*didn't move my tablet so much*" and P23 reported "*stayed still but still kept it [tablet] close*". 4 participants reported trying to do the task as quickly as possible to reduce exposure. 2 participants reported covering up the screen with the bank card. While we did notice these behaviours during video coding, we found the intentional ambiguity of these behaviours made it difficult to assess whether they were deliberate privacy management behaviours. In addition, 3 participants reported their effort to hide the physical bank card as well (e.g., cover with hand; flip around the card when done with inputting number; quickly memorize 4 digits and cover the card).

Activity 3: Collaborative Bill-splitting

Reports about collaborative tasks were also similar to our observation. 2 participants explained they didn't do much because the information was not that crucial, 1 said he was concentrating on the task. Except for the common strategies such as angling the tablet and using hands to cover, 2 participants reported watching for partners when the partner did the calculation. 3 participants reported reminding their partners. 2 participants reported looking at the face of the onlooker (glaring). 4 participants reported doing the task quickly so that others wouldn't have enough time to see. Regarding utilizing proximity, P15 mentioned: "*we got closer to have less angle available for the observer to see*." And P21 said "*talk closely*". P22 explained about being vague when discussing security questions: "*it's just names of things only she and I would know that random people wouldn't know. We didn't say the actual word, we said, like 'her dog's name' but didn't say the dog's name*."

Phenomenon: physical mechanism dominance in the game

One notable observation is that during the game tasks, participants relied more on physical mechanisms to manage privacy regardless of which interface they used. 5 participants reported that they relied more on themselves whereas no participant claimed otherwise. There are multiple reasons that might contribute to the phenomenon:

- **Focus of breach source**: Participants knew the opponents were coming over their shoulder at the moment of the audible dings by game rule and thus paid more

attention to the source of privacy breach than to digital mechanisms. For example, P24 said: "*I'm pretty competitive…I was focusing so much on her [opponent] and the flags…the dimming is a great idea, I didn't use it very much in this particular case*." P13 said: "*I was into the game…observing her [opponent] going around me…I'm very aware of my surroundings. And it occurred to me that my own vision is what helped more than that [notification]. So it's not that that was useless, but I'm just saying that I depend more on my own vision than on that icon*."

- **Focus of task**: Memory match game consumed much cognitive resources that some participants concentrated more on the primary task and didn't notice the notification or protection sometimes. For example, P1's screen dimmed 5 times during one game, but he couldn't remember because "*I wasn't really paying attention. I was paying more attention to the flags.*" Notification popped up on P10's screen for 6 times yet he claimed only saw it twice because "*I tried to have attention on the cards.*"
- **Auditory Cues**: The intermittent "ding" was designed to prevent observer from continuous and unlimited privacy breach. However, since the memory match task and the opponent occupied most of visual cognitive resources , participants unexpectedly utilize auditory cues as an indicator rather than paying attention to the competing visually presented digital system. 5 participants reported following the ding sound as a protection strategy. P14 claimed the "ding" sound was more helpful than the notification. P21 said: "*I paid more attention about the ding than the icon.*" 2 participants used footsteps to figure out their opponents' whereabouts and protect accordingly (e.g., "*I used mostly my ears, not my eyes*", P16).
- **Trust in Digital Protection**: 4 participants didn't trust that Dim could provide sufficient protection at the beginning. P2 reported: "*I don't feel it dimmed enough to help protect. I felt moving it closer to my body was more helpful than the dimming*."

This observation suggests the nature of the competitive game might have inhibited the possible impact of the digital privacy management system on participants' perception and behaviour in the game activity.

5.3.3 Opponents' Observing Experience

After the game activity, we asked participants to reflect on their experience as an observer and if there was any difference between the two rounds. We learned that users' awareness is the key to prevent shoulder surfing and that both physical behaviours and the digital protection (Dim) are effective in preserving privacy.

- **Awareness's role**: No matter where participants got the awareness — from their physical mechanisms, notifications or protections — once they were aware, the opponents found it hard to see. 2 participants described how auditory cues warned the opponent. (e.g., "*My shoes were making big noise, so it's very easy to identify I'm somewhere around him. So if he want to hide the screen from me, I cannot see it at all,*" P16). 4 participants concluded notification helped with awareness and thus privacy. P25 reported: "*when the icon popped up, she kinda of held it closer, that she was aware so it was harder to see*." 1 participant thought the protection (Dim) as a notification made it harder to see. On the contrary, if users were not aware, information was easily leaked. P5 claimed seeing 15-20 flags standing on the corner because P6 played for a long time without noticing he was there. "*I think she needed the notification to remind her,*" he concluded. Similarly, 2 other participants claimed that when their opponent forgot, it was very easy to see.
- **Physical privacy management was effective:** 7 participants found what made them hard to see was the physical movements of the opponent. For example, P1 said: "*I didn't see the tablet much. When she held it closer, it was much harder*." P17 said: "*He was very effective in keeping the screen turned away*." P13 only saw 1 card across the game activity and his opponent explained: "*Even without this function [digital system], it is also easy to hide the information…you could just slightly move, but the observer needs to move a long distance to observe.*"
- **Dim was useful**: Although some participants didn't feel confident about Dim as a user, 9 claimed it was useful when they acted as an observer. For example, P8 commented: "*[in round one] because the screen was so dim, when he tilted a little bit, I couldn't see anything. In the second round, the screen was lit brightly. And even he tilted it a bit away from me, I could see more*." P26 reported: "*When he had the screen dimmer, it was quite a bit more difficult to actually see what's on there*."

We recorded the number of corrected and wrongly identified cards from the observers for each task as an objective measurement of how much observers actually saw. We didn't observe difference for the total average observed cards (NN=3.3, YN=3.2, NY=3.1, YY=3.1), average correctly or wrongly identified cards (see Figure 30). We should note that correct observations (privacy threat) might be underestimated due to memory issues (10 observers reported forgetting a few cards they saw during the 10 second intervals) and wrong observations (safety) might be inflated because of recognition (some national flags were so similar that 11 observers couldn't recognize the flags they remembered in the answer sheet). Given the impact of physical dominance in the game and that the confounding issues were constant, we found this result explicable.

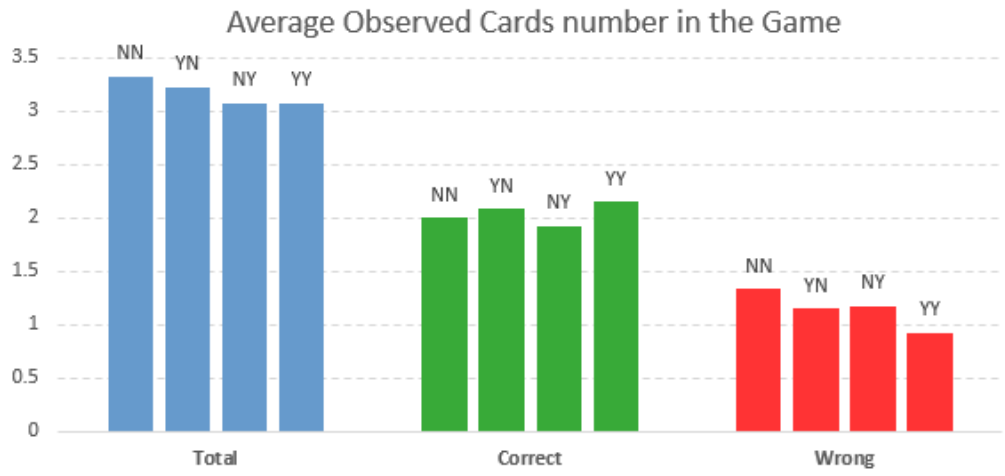


Figure 30 Average number of observed cards across all conditions. Total number equals corrected identified cards plus wrongly identified cards.

5.3.4 Real-life Implications

According to the participants, privacy threats in real life are more severe, and privacy strategies are more preventive and context-dependent. Existing physical mechanisms have several issues in managing mobile content privacy.

Privacy Threats

Mobile device users were considered to be more exposed to shoulder surfing in real life than in the study. 14 participants thought onlookers would not be as obvious to look. Onlookers were described as more "*discreet*", "*secretive*", "*subtle*", "*casual*", "*sit behind or next to the person and try to act as doing something else*", and "*without moving head very much, just move eyes*". At the same time, 12 participants thought users wouldn't be as defensive as they were in the study. 6 participants thought that most of the time users are not aware of the danger. For example, P21 said:" *If I was using my tablet somewhere like a coffee shop in public areas, obviously I wouldn't hear a ding, obviously it would be more useful then because I wouldn't be expecting someone to be observing what I was doing*." Others thought users wouldn't hold their devices as close or move their body to hide the device as much. P19 reported: "*I don't think they [users] go such extreme as moving the whole body or putting the tablets so close to themselves.*" P12 thought in reality onlookers could sit closely next to the user thus making content easier to see.

Privacy Practices

Participants reported various strategies they developed through daily life. Physical strategies such as keeping the device close to the body, leaning down, turning the screen angle were the most reported strategies. External objects such as books, paper, and folders were also used. P22 described the story of closing the cover of her tablet a bit to hide the email she was composing on an airplane. P23 also mentioned the role of other people as physical barriers to block vision: "*I will often stand with trusted colleagues…I feel like surrounding yourself in a circle with trusted people was a good idea*." One of the common strategies that couldn't have been observed in the study was **prevention** strategy: 11 participants carefully searched for a safe location (e.g., not in public place, a corner, back of the room, on the side or peripheral, against wall) to make sure no one was beside them or watching them. 3 participants mentioned stopping the current work (e.g., close the browser, turn off the screen, switch to another window) and continue later. P21 avoided having emails open for very long time in public space. For organization practice, P11 arranged the orientation of his monitor to protect prototype in development and P23 used mandatory laptop screen protectors to protect product launch plan. 8 participants appropriated built-in features (i.e., adjusting brightness) of mobile devices.

The strategies are dependent on contextual factors such as locations, types of media and number of viewers. For example, P22 said she would be less careful in a coffee shop than at an airport because onlookers would be more likely to be pick-pocket or deviant at the airport. P16 discussed the impact of screen size on ways of privacy management: for mobile phone, hands were thought to be big enough; for tablet, objects such as paper, folder could be used; for laptop, the physical ways were further limited. When not so many people are around, changing the orientation of the laptop were helpful whereas when surrounded by people, the participant had to stop working.

Issues with Physical Mechanisms

Participants identified several issues with physical privacy management. 8 participants said it is difficult to **stay aware** of the surroundings when concentrating on a task. Other issues include the need for **precautionary behaviours** like looking behind one's back (5 participants); less **convenience** to work with hands covering the tablet (3). P25 reported shielding the keyboard with his hands when typing the password "*it's hard*"); **advertising** through their actions that they are engaging in a private activity (3). P6 commented: "*If you do some weird pose to protect your screen, people will notice that…You're actually telling people around that I'm doing something secretly. So better not protect at all*"; and **social concerns** about appearing awkward or signaling that they don't trust those nearby (5). For example, P2 tried to block the vision from students when she entered iPad password. She commented: "*I'm trying to make it so that it was not obvious that I'm hiding it from the students. I don't know why I don't want people to know that I don't trust them*." Finally, certain screens are difficult to protect with physical measures because of their **sizes**. P3 mentioned laptops or desktop computer are hard to protect.

5.4 Digital Privacy Management

To address the research question that how a digital privacy management system might be designed to work with physical privacy management mechanisms, we found that adding

digital privacy notification and protection mechanisms improved our participants' self-reported awareness, confidence in privacy, ability to balance work and privacy and overall satisfaction, but this didn't significantly alter their observed physical privacy behaviours. Notification didn't hold as much weight as protection, but both awareness and response are indispensable in the processes of privacy management. Automatic and manual protection were closely favored due to their respective strengths in protecting privacy or supporting task efficiency. We further provided an information-context-intention framework for on-screen content privacy.

5.4.1 Impact on Privacy Management Perceptions

We examined the impact of the digital privacy system on participants' attitudes (measured by questionnaire) across the 3 activities. We asked participants to rate the easiness to be aware of the potential onlookers, the confidence to hide the information, easiness to balance between continuing work and preserving privacy, and the overall satisfaction towards different combinations of notification and protection (interfaces) for each task. As shown in Table 15, Kruskal-Wallis tests showed that for the **game tasks** we didn't observe significant difference between different study conditions, but for both **individual** (see Figure 31) and **collaborative** (see Figure 32) tasks we found significant differences on almost all of the measurements among interfaces.

Table 15 Differences among 4 types of interfaces (NN, NY, YN, YY) in terms of awareness, protection, balance and satisfaction across three activities.

	Game		**Individual**		**Collaborative**	
Measurements	$\chi^2(3)$	***p***	$\chi^2(3)$	***p***	$\chi^2(3)$	***p***
Awareness	2.771	.428	21.074	.000	40.360	.000
Confidence in Protection	2.263	.520	23.466	.000	31.900	.000
Balance	2.063	.559	25.911	.000	11.739	.008
Satisfaction	4.712	.194	16.663	.001	28.682	.000

Awareness

We expected with notification it would be easier for the tablet users to tell whether a potential onlooker is nearby. For game tasks, the digital privacy system didn't help improve awareness could be explained by the fact that participants were already very aware of their surroundings in a competitive game. For individual and collaborative tasks, we performed a series of Mann-Whitney tests for post-hoc pairwise comparisons using Bonferroni correction. The results showed that not only interfaces with notification (YN, YY) but also interface with only protection (NY) were thought to help awareness than without digital system support (NN) in both individual (p_{yn} = .000, p_{ny} = .024, p_{yy} = .000) and collaborative tasks (p_{yn} = .000, p_{ny} = .000, p_{yy} = .000). One explanation is the automatic nature, the way the protection techniques suddenly change the screen, serves the purpose of notification. 8 participants mentioned the role of protection techniques as notification. For example, P2 said: "*the whole screen dimmed, so I find that's enough of an indicator that someone is around.*" P10 said: "*when you put Mask there, it is kind of notification because after the protection I noticed someone is looking.*"

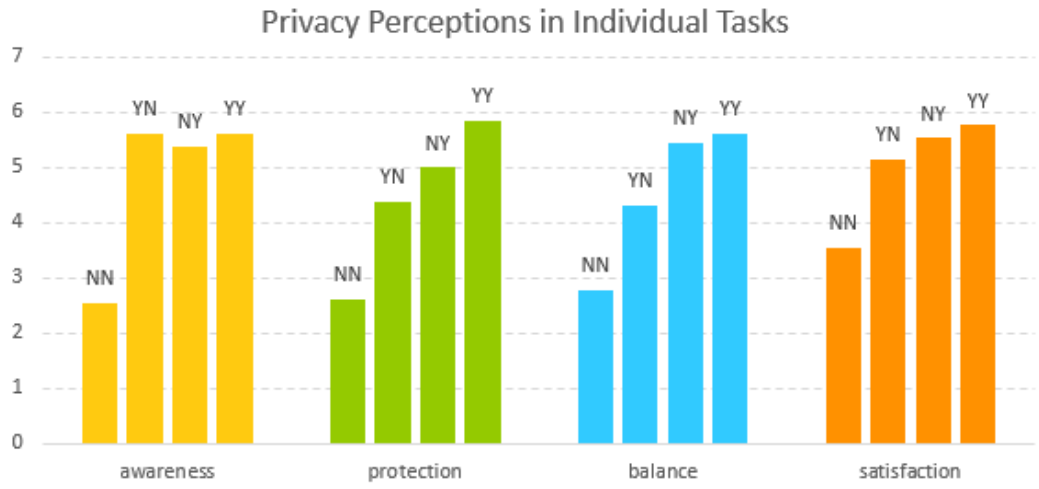


Figure 31 Participant' privacy perceptions across study conditions in individual tasks.

Confidence in Protection

We measured from the **user**'s perspective whether the digital system would make them feel that protecting privacy was easier or feel more confident about protecting privacy. Participants didn't feel it was easier to hide the screen content with digital support than NN condition in the game. This could be because the opponents were persistent in observing and participants heavily used physical mechanisms to manage privacy.

However, in both individual (p_{yn} = .03, p_{ny} = .000, p_{yy} = .000) and collaborative (p_{yn} = .000, p_{ny} = .000, p_{yy} = .000) scenarios, with the system they did feel more confident.

On the other hand, we also measured from the **onlooker**'s perspective whether it is easy to see the user's screen (rating was done by opponents in the game and the research confederate in individual and collaborative tasks on a 7 point Likert scale). We didn't find difference for either the game ($\chi^2(3)$ =4.2, p<.244), individual ($\chi^2(3)$ =2.8, p<.429) or collaborative ($\chi^2(3)$ =6.7, p<.081) tasks. However, we did find the mean easiness to see decreased as participants get more digital protection support: NN=4, YN=3.38, NY=3, YY=2.85 (smaller number means more difficult to see) in the game. According to the confederate, "*It was fairly easy to see the screen. However, screen's elements were extremely hard to be identified because of the privacy protection technique [Mask]*."

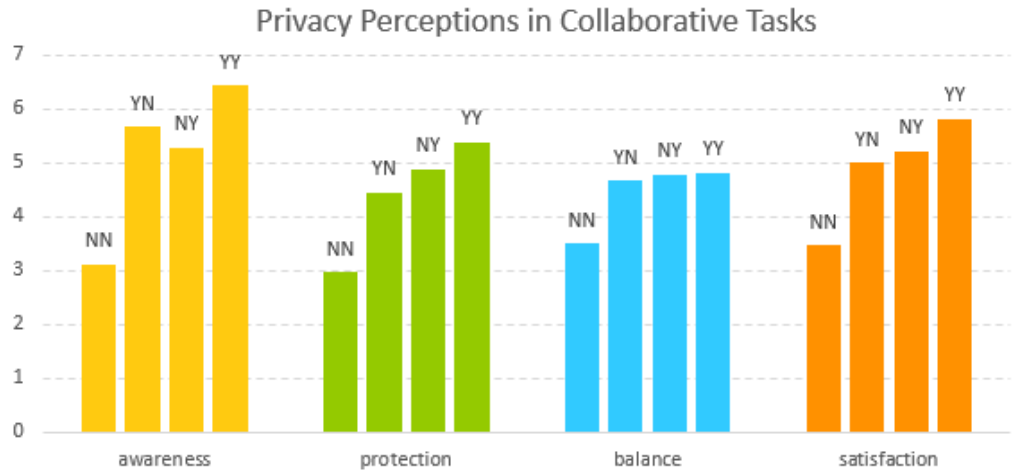


Figure 32 Participant privacy perceptions across study conditions in collaborative tasks.

Balance

When asked whether it is easy to continue work (both individual game or banking and sharing the tablet with a partner) while preserving privacy. We observed similar trends among different interfaces: no significant difference in balancing work and privacy in game tasks, but significant improvement in individual tasks (p_{yn} = .03, p_{ny} = .000, p_{yy} = .000) or marginal significant improvement in collaborative tasks (p_{yn} = .06, p_{ny} = .03, p_{yy} = .066) with the system than without the system (NN).

Overall Satisfaction

For the overall satisfaction of interfaces used in all three activities, again we found that participants didn't have a preference for any interface in the game activity. But they felt more satisfied when the digital privacy management system helped them in real-life scenarios (p_{yn} = .048, p_{ny} = .006, p_{yy} = .000 for individual and p_{yn} = .006, p_{ny} = .000, p_{yy} = .000 for collaborative tasks) than dealing with the privacy issue by themselves (NN). The YY interface got the highest satisfaction in both tasks.

5.4.2 Impact on Behaviours

Privacy Behaviours

To understand the impact of digital privacy management system on people's physical privacy management behaviour, we compared the privacy management behaviour between NN (without the system) and other conditions with Wilcoxon signed-rank test. We didn't observe an impact of interfaces on observed physical privacy behaviours in any activity (see Figure 33).

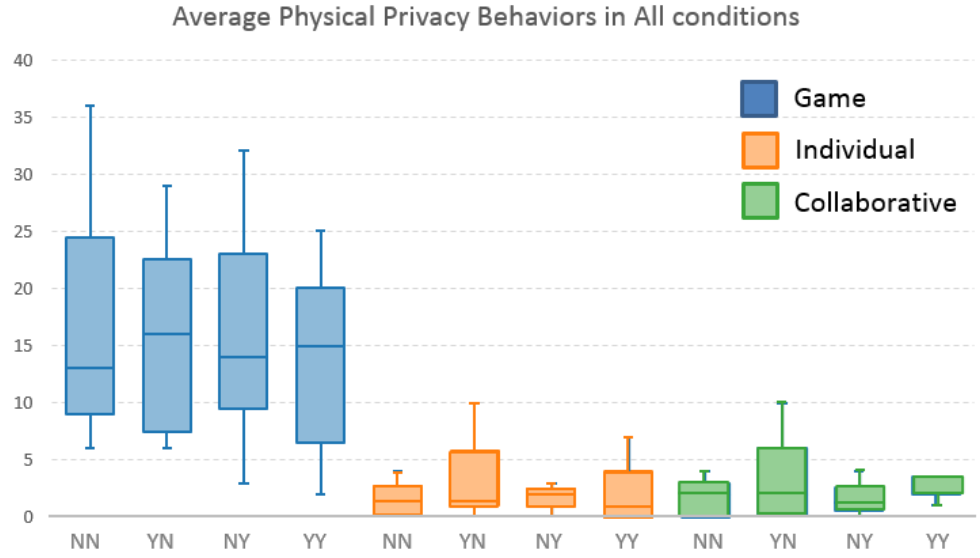


Figure 33 Privacy behaviour comparison among all conditions across all activities.

For the game activity, although there is no overall difference in behaviours, when we combine all three digital conditions and compare with the physical condition (see Figure 34), we saw a shift from macro protection to micro blocking behaviours in digital

conditions which may indicate the digital system helps reduce drastic behaviours to some extent. For the financial scenarios, we combined individual and collaborative scenarios to generate a larger number of privacy behaviour occurrences. We observed an increase in device maneuver behaviours and awareness behaviours. This suggests the digital system in general raised awareness and led participants to respond in a very subtle way in realistic situations. For example, in collaborative tasks, P20 reported: "*Hunch over, make sure no one can see it when the eye pops up*." P26 said: "*Whenever there is a notification saying someone was around, I kinda want to see what's happening*."

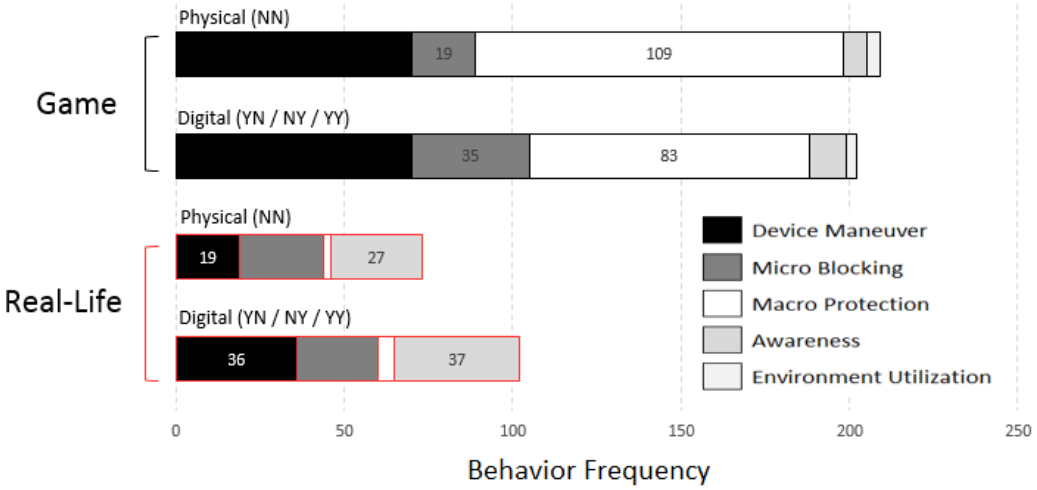


Figure 34 Privacy behaviour comparison between physical and digital conditions in game and realistic tasks.

Task Completion

Table 16 Task completion time comparison across three activities.

Task Condition	Game (S)		Individual (S)		Collaborative (S)	
	M	SD	M	SD	M	SD
NN	100	34	75	33	218	51
YN	118	37	74	26	221	52
NY	104	28	77	30	219	48
YY	105	30	69	20	253	89
Average Time	111		74		227	

On average, each game task lasted for 111 seconds, individual task for 74 seconds and collaborative task for 227 seconds (see Table 16). A Kruskal-Wallis test showed that the task completion time didn't differ across study conditions. Regarding the task completion errors, all participants completed the memory match games; 6 participants retrieved the wrong information in the first online banking task, but 4 out of 6 were due to reasons irrelevant to the interface (took May 16th for June 16th); 1 group made the wrong calculation in the collaborative task because of the calculation method they used. These results suggested that the introduced digital privacy management system didn't impede the task performance (time or error). We should note, however, this impact should be further explored with tasks that requires longer time.

5.4.3 Preference among Digital Privacy Management Models

After participants experienced each type of interface (NN, YN, NY, YY) in the first two activities, we asked them to rank their preferences for the interfaces. The same question was asked after they performed the collaborative activity. The Friedman test showed a significant difference in ranking of different interfaces for both the individual scenarios (game + individual banking scenario) ($\chi^2(3) = 57.625$, $p = .000$) and the collaborative scenario ($\chi^2(3) = 50.236$, $p = .000$). The trend of mean rank for different interfaces was similar (see Figure 35) for the individual (NN=1.04, YN=2.33, NY=3.02, YY=3.62) and collaborative scenario (NN=1.15, YN=2.37, NY=2.87, YY=3.62). Post hoc analysis with Wilcoxon signed-rank tests was conducted with a Bonferroni correction applied (see Table 17).

Table 17 Post hoc analysis for preference ranking differences among 4 types of interfaces (NN, NY, YN, YY) for individual and collaborative scenarios.

	Individual		**Collaborative**	
Measurements	**Z**	***p***	**Z**	***p***
YN - NN	-4.682	.000	-3.928	.000
NY - NN	-4.569	.000	-4.405	.000
YY - NN	-4.642	.000	-4.538	.000
NY - YN	-2.857	.024	-1.992	.372

	Individual		Collaborative	
Measurements	**Z**	***p***	**Z**	***p***
YY - YN	-3.442	.006	-3.718	.000
YY - NY	-2.327	.120	-2.753	.036

For both individual and collaborative scenarios, the interfaces with digital privacy management features (YN, NY, YY) were preferred over managing privacy by participants themselves (NN). YY condition is rated the highest in both scenarios. Although notification was regarded as less effective than protection, people prefer to have both on the grounds of "*maximum protection*" and "*two is better than one*". In the individual tasks, 19 participants preferred protection to notification mainly for three reasons: protection techniques actually reduce the chance of sensitive information being seen (14 participants), protection took over the responsibility to protect and saved users' effort (e.g., sit in a corner, be careful, hide the device) (6), and the issues with notification (e.g., annoying, distrust, socially impolite) (8). 6 participants preferred notification mainly to have more control over the device and benefit from the awareness while leaving protection to themselves or manual protection. In the collaborative scenario, 4 participants changed their ratings to prefer notification because notification became more noticeable (2), and protection hindered collaboration (e.g., partner couldn't see) and became less necessary (2). For example, P13 said: "*You need two people to be able to see the screen. Also you now have two people who can protect the information.*"

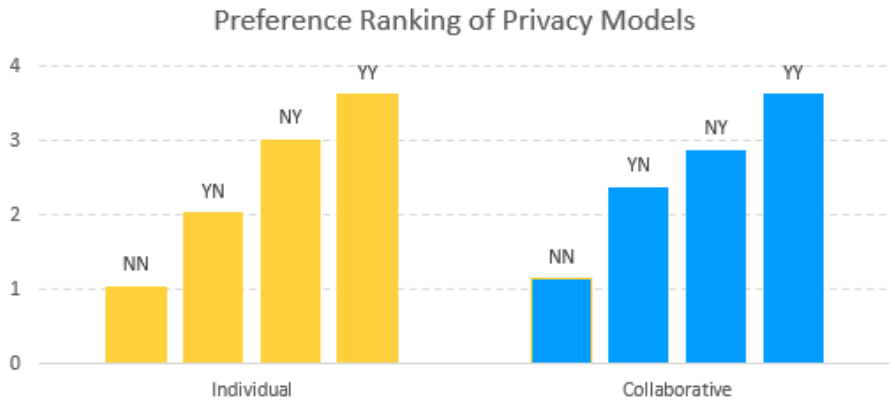


Figure 35 Mean preference ranking for 4 privacy models for individual and collaborative tasks.

In addition, the preference could be impacted by contextual factors such as information sensitivity, location, or potential viewers (4 participants). For example, with less sensitive information, or trusted colleagues / friends as potential viewers, notification would be enough – the user could take actions or onlookers could self-regulate behaviours. But conducting sensitive activity or surrounded by strangers, protection would be preferable.

5.4.4 Relationship of Notification and Protection

Notification

Privacy notifications were seen as somewhat useful by 20 participants, with 4 undecided and 2 who did not find them useful. The notification was likened to icing on the cake that is "*good to have*" and "*better than nothing*". P13's comments were typical: "*You know they have these cameras at the back of the car now where you can use it to reverse. Even if you can reverse by yourself, it's still good to have a camera, in case if you want to use it at one point.*" 12 participants felt they would help promote awareness in unfamiliar or dynamic surroundings. Other benefits were to help address human perceptual limitations (e.g., "*you don't have an eye on the back of your head*", P26), save attention for primary tasks, reduce the need for precautions, or indicate whether a protection action was successful ("*If you didn't protect yourself well, the notification will come again*". P14). On the other hand, notification is not useful if there are many false alarms or misses (10 participants). 4 participants worried that frequent notification in busy environments would be overly disruptive or cause confusion. Other reasons include distraction (5), being too obvious to the onlooker (5), occluding display content (4), or going unnoticed (2).

Protection

In general, almost all participants agreed that protections were useful. Dim was described as an "extra layer" that add subtle protection and made 15 participants feel content was safer but not completely protected. 8 participants had already adopted it as a privacy strategy in daily life (e.g., when using Facebook, Tumblr, IM). Participants expected it to be useful when working with a whole document containing medium-sensitive information, and it could protect detailed text information from a distance. Mask was

trusted by 19 users to be "*totally safe*" and "*effective*", suitable for highly-sensitive data within close proximity given familiarity with the information layout and the ability to work in a small region. Overall, protection techniques were seen as an *extension* of physical measures that added extra protection (5 participants); a *substitute* of physical mechanisms that helped concentration (4), freed our hands (2), and would make prevention (e.g., find a better spot) unnecessary (3); and an *alleviator* of socially "*funny*", "*awkward*" and "*uncomfortable*" protection behaviours (4). For example, P5 commented: "*I want to be as natural as possible because I don't want to hurt other people's feelings.*"

Usage Pattern and Privacy Processes

Participants chose three different combinations of notification and protection based on the same underlying assumptions: both awareness and protection are necessary. The first type of participants (7) preferred to only have automatic protection because it encompass both awareness and protection. As P26 noted: *"It's almost two in one. Because it is protecting and the fact that it is protecting is a notification.*" The second type of participants (4) chose both notification and protection to serve their own intended roles. For example, automatic Dim may not easily draw users' attention and manual protection lacks awareness. Thus, notification would be useful in these cases. The third type of participants (3) preferred only notification but then the responsibility to protect is shifted to user's physical mechanism. For example, P25 said:" *The physical I did when I saw the notification was good enough.*

5.4.5 Automatic versus Manual Protection

We tested two different models of protection mechanisms: the automatic (NY) one that was triggered by the system and the manual (YY) one that was decided by the user. We found 4 behavioural patterns in using the manual protection (YY), see Figure 36:

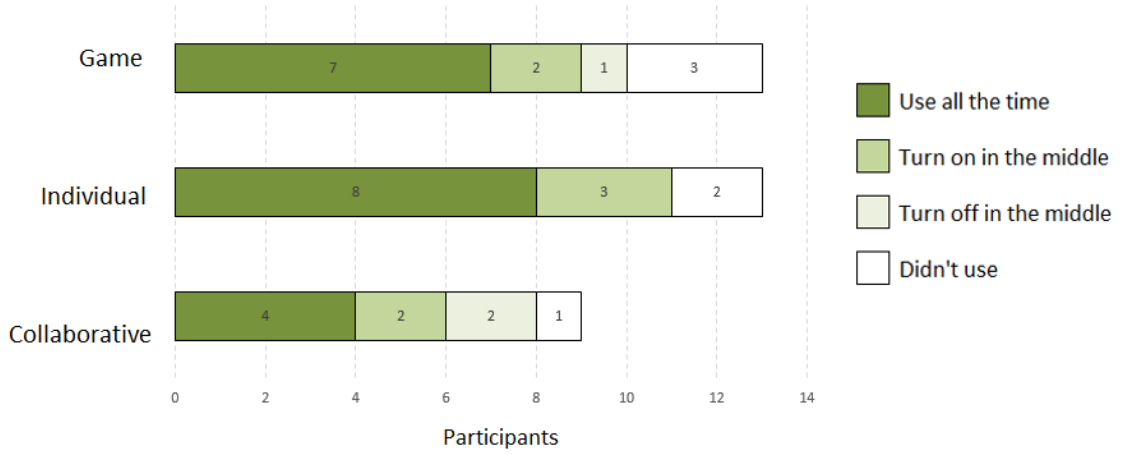


Figure 36 Participants' behaviour patterns for using manual protection across three activities. For collaborative tasks, the number of groups using manual protection is less than other conditions.

First, most participants chose to turn the protection on throughout game (Dim) and individual (Mask) tasks but less so in collaborative tasks. Second, when participants felt privacy threatened (e.g., opponent was looking over) or they tried to access highly sensitive data (e.g., the summary page of all bank accounts information), they turned on the protection in the middle of the task. Third, interference is the main reason to turn off the protection in the middle of the task. For example, P6 turned Dim off in the game and G2 turned Dim off when typing security questions. As an interesting counterexample, P13 spent around 5 minutes (average time = 74 seconds) working with the Mask to retrieve the task information but didn't turn it off. He explained: "*the loss of speed in accomplishing the task is worth it…if it's something like banking information*." Fourth, not using the protection at all is also because of task efficiency (e.g., can't see well with Dim (P3), or hard to continue work with Mask (P16)). We can see the choices were the result of weighing privacy value against the cost of task completion.

We asked participants about their preferences for automatic and manual protection. 9 preferred automatic protection, 13 preferred manual protection, and 4 thought both had their merits and demerits. The benefits of **automatic protection** are that it promotes task focus (5, e.g., "*you don't have to think about all the different things that you're doing*," P26), it prevents users from forgetting (4), it is fast (2, e.g., "*When you notice…it's*

already too late)", P5), and it helps task efficiency by not having to be always on. Stated benefits of **manual protection** are feeling more in control (5), avoiding interruption from an unpredictably changing screen (5, e.g., P8 and P10 described the experience of brightness changing the whole time "*hard to focus*" and "*stressful*"), and not being dependent on the system's reliability (4, e.g., "*it's more predictable. Otherwise you're not really quite sure if it's working*", P1). To reduce cognitive burden, manual protection was expected to be used together with notification (8) or as an always-on prevention (3).

5.4.6 Three levels of On-screen Privacy Protection

We encountered three kinds of privacy: information, context and intention privacy, and protection techniques vary in their capability of preserving them. Firstly, both Mask and Dim are good for **information privacy**. Mask covers most of the screen. It's easy for users to see through the translucent mask to get an overall understanding but difficult for an onlooker to do so given the distance from the screen. The only risk is the small circle-shaped viewport, but it could either be moved around fast to non-essential areas (P22, P4) or be easily covered with hands (P25). Dim is also good for protecting detailed on-screen data. Second, Mask also protects **context privacy,** which is essential for an onlooker to understand the activity of the user and the meaning of the information (6). For example, P8 commented: "*When you're doing banking, that one spot, that piece of information is meaningless unless you know the context it is in. That one number doesn't really tell anyone a whole lot of information unless they see the whole page.*" Dim, on the other hand, doesn't protect the context as much. As P11 noted: "*To make it dim, it gives the other person an idea of what's going on, what I'm doing now.*" Third, **intention privacy,** the look of users trying to hide something, is also worth protection because abnormal behaviour or unusual interface would attract attention or stimulate unwanted curiosity. 5 participants talked about the problem of Mask as being obviously setup for privacy purpose and advertising users' private activities. As P26 commented: "*it almost catches your eye, and you might be interested in looking over*." Dim, on the other hand, is subtler and less noticeable for onlookers. Thus it could better preserve intention privacy.

5.5 SMALL GROUP PRIVACY MANAGEMENT

We wondered how a digital privacy management system might be designed differently to support multiple users. We found that privacy management at a small-group level is different as collaboration leaves information more open, increases the contradiction between task efficiency and privacy, and have to accommodate potentially disparate individual needs. Participants reversed to prefer pro-efficiency protection techniques. In general, notification was believed to be more useful whereas the usefulness of protection was questionable.

5.5.1 Nature of Collaborative Work

8 participants thought collaborative work didn't differ from individual work in terms of content privacy management. (e.g., "*If you are close enough together that you could both see the screen even it dims or masks or whatever*", P20). The rest of the participants, however, agreed that collaborative tasks have different characteristics from individual tasks. Firstly, 3 participants thought privacy in collaborative scenario were more **vulnerable** in that the tablet would be held more open between partners for both to see (P6, P11), collaborators were more verbose and distracted (P22). Secondly, 3 thought when two people are working together towards a same goal, the importance of **task efficiency** increases that slowing down would be less tolerable. For example, P16 commented: "*[with Mask] calculation, moving around the circle is very time consuming. I don't think people will really do that*." Thirdly, 4 participants mentioned that digital privacy management system now needs to accommodate multiple people's potentially **conflicting needs**. For example, P7 from G4 preferred to have protection (Dim) on but P8 felt very difficult to see the screen content, so they ended up not using protection. In addition, 2 participant mentioned the screen protector didn't work in collaborative situations. "*If you have to be straight on your laptop, and then you just have to go back and forth, that's not the most collaborative way*", P23 said. Fourthly, 2 participants thought the level of **awareness** would be enhanced in a collaborative task by an extra person. As P16 noted: "*His [collaborator's] eyes and ears, his physical ways will be much efficient than the notification on the tablet*."

5.5.2 Preference for Protection Techniques

We asked participants to rank their preferences for Dim and Mask after the game and the individual activity. 18 participants preferred Mask to Dim whereas 7 participants preferred Dim over Mask and 1 participant didn't have a preference. 5 out of 8 participants who already applied strategy similar to Dim (e.g., change brightness of the screen) in their daily life turned to Mask. We further analyzed their reasoning behind this preference: people who are in favor of Mask unanimously listed effective protection and confidence in using Mask as the major reason (privacy oriented). On the other hand, people who were in favor of Dim mostly (5/7) because Dim didn't interfere with work as much and it's easier for users to see (efficiency oriented). Again, we observed a trade-off between privacy and task efficiency.

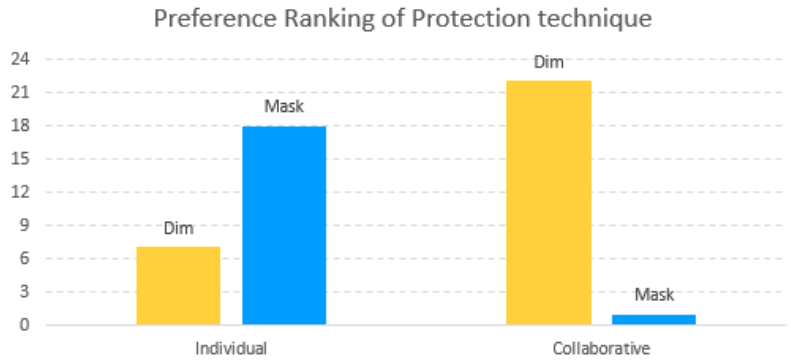


Figure 37 Participants' preference for Dim and Mask in individual and collaborative tasks.

We also asked participants after the collaborative activity what it would be like to use Mask in a collaborative task and whether their preference would change. The preference is reversed in this situation (see Figure 37): participants almost unanimously (22/23) felt Dim was more appropriate than Mask for collaborative tasks: "*I can see how it would be challenging with Mask in this one [Task]. For collaboration, dimming is the way to go just because we both need to be able to look at the screen*" – P23. Almost all the reasons against Mask in this scenario pertained to the inconvenience to perform the task and time cost for moving around the viewport. 2 participants also pointed out that Mask made the collaborator much harder to interpret the task at hand.

5.5.3 Feedback on Privacy Management Systems

8 participants thought **notification** would be more useful in a collaborative task because with enhanced physical mechanisms from an extra person, notification became more noticeable when the other collaborator was too focused on the task. P17 commented: "*It would be valuable when it comes to notification because it will get attention if somebody notice it*." On the contrary, **protection** techniques were described as "*quite problematic*", "*not ideal*" or "*really challenging*" in collaborative scenarios. 8 participants thought they didn't suit teamwork. P8 emphasized the conflict between privacy and collaboration and argued that neither physical nor digital mechanisms would be useful in this situation: "*When you turn it away…you make it harder for the other person to see…with Mask, it would be inefficient because you can't look at two things at the same time. Dimness, it was hard to tell how well the other person can see*." 4 participants thought the protection techniques should at least be as less interfering to both parties as possible. 2 claimed prevention strategies would be better (e.g., choose a closed room) for collaboration.

3 participants proposed that privacy management could also be done in a more *collaborative* way (e.g., one person controls privacy feature and the other collaborator performs the task, P15). P17 suggested multiple visible areas for more people. In addition, 2 participants raised the question of the system's ability to differentiate individual and collaborative scenarios due to the conflicting nature (privacy versus sharing) of the tasks. P23 commented: "*If I was doing something on my tablet and then I call the colleague over and said 'take a look at this'…would it realize that I'm sharing my screen with someone?*" P13 suggested arranging privacy setting by profile: in a collaborative (e.g., meeting) context, apply the setting that turns on the notification but turns off the protection whereas in an individual context turn on all the protections the user specifies.

CHAPTER 6 DISCUSSION

In this chapter, we first discuss factors to be considered in designing usable mobile content privacy management systems. We then present design feedback such as the context of usage for notifications, protections and the whole system; suggestions for the system; and design guidelines derived from the results. We also reflect on the suitability of the lab approach taken in this research. Finally, we identify limitations of this work and possible research directions in the future

6.1 HOLISTIC PRIVACY MANAGEMENT

Dourish et al. proposed the term "*holistic security management*" to illustrate how online data security is protected not only online but also in the physical world by space arrangement and demarcation [32]. Similarly, we found participants didn't perceive privacy management of digital information solely through a digital system. The existing physical mechanisms and the physical world were considered to be integral parts of "*holistic privacy management*".

First of all, users' physical movements and changing screen appearances are parts of privacy management that can be used together to reduce the possibility of privacy breach. Hawkey and Inkpen found users wanted to conceal the web browser interface with colored privacy feedback that is directly visible to collaborators [51]. Our results showed users also tend to manage physical behaviours (e.g., avoid obvious behaviours) and are concerned about the appearance of notification and protection mechanisms (e.g., red notifications, high-contrast Mask) when faced with casual shoulder surfing threats as these visual elements worked against user's intention to conceal information. A holistic design should consider ways of reducing the user's physical obviousness as well as the digital system's ability to attract attention or to advertise the intent for privacy. For example, a privacy notification could resemble a regular system notification or notify through vibration.

Secondly, a mobile content privacy management system is meant to be used in social situations. Such a system should be socially acceptable for the user, collaborators, and bystanders. Most participants thought obvious physical protection used in the game would be "*difficult*", "*strange*", or "*awkward*" in real life, making them look "*creepy*" or like "*a freak*". For example, P3 commented: "*even you know like somebody is looking at your tablet, you cannot do a full protection like this. It's kind of creepy*." Similarly, 10 participants were concerned about the straightforward meaning being easily digestible by the potential viewers. Some participants suggested more subtle notification glyphs (e.g., an animal, star) and less prominent protection. 5 participants wanted to switch the eye design to a customizable icon that is "*only known to the user*" (P15). Traditional notification design values universality and visibility, but obfuscation may be more appropriate for privacy. The need for privacy is a delicate matter when among friends or colleagues. For example, P2 commented: "*I think I'd be embarrassed that I want privacy… Feeling like I have something to hide, or that I don't trust people around me*." Appearing not to trust people nearby was also a concern regarding strangers as most participants believe the majority of onlookers would have benign intentions. Systems could reflect these concerns by offering flexibility in establishing the parameters for detection, and the nature of notification and protection.

Thirdly, our prototype was expected to consider the user's and the onlooker's physical circumstances. If users are fully aware (e.g., see, hear) and can easily manage privacy with physical mechanisms, the digital system is unnecessary. Participants in both studies expressed a similar expectation that notification should work only when someone is behind and not blocked by the user's back. Moreover, users expected the privacy management system to "*see*" what they see and "*know*" what they know. For example, it is possible for technology not constrained by visual occlusion (e.g., the Polhemus system used in this work) to detect people behind objects or barriers. However, 1 participant considered the system "*not working correctly*" if the notification showed up when he sat with his back against barrier. . These suggest a holistic system might kick in when there

is loud noise or when an onlooker is detected beyond the user's visual field, but not when an onlooker is at an obtuse angle or their vision is occluded.

Finally, no matter how users choose combinations of physical and digital measures, the underlying awareness, detection and response privacy processes are both integral parts of a whole. Different choices reflect personal preference over trust in technology versus self-control, or responsibility distribution between physical and digital privacy mechanisms. For example, users could detect a privacy breach by themselves while delegating the response to the digital system or be reminded by the digital system and respond physically on one's own. System designs should allow for such choices.

6.2 The Issue of Trust

The trustworthiness of a mobile content privacy management system became a recurrent theme in participant feedback. 12 participants expressed concerns about reliability and accuracy of the system, 6 due to false alarms and 6 to missed detection. This could be due to the limited tracking range of our sensor (1.5m around the source) or magnetic field distortion from metal in the environment. **False alarms** caused participants to be confused, hyper-vigilant, or to ignore the system. P24 said: "*The problem is when it comes to privacy that trust factor is so big. That it's like I need to know it works right if I'm going to believe it at all.*" P22 wondered that whether the system would alert when a dog walks by or somebody is looking at places other than your screen. **Missed detections** had a similar impact, but were more acceptable. For example, P11 said: "*It was ok sometimes it works sometimes it doesn't. But the time it worked, it was helpful*." As Dourish et al. noted, delegation of security and privacy to technology is "*an investment of trust*" [32]. Trust also affected participants' preferences to take over control or rely on the physical mechanisms. P14 said: "*I didn't rely on it because it's not that precise*", and P11 noted: "*I felt I couldn't trust the system that I have to be careful of myself than just relying on the system*." While Fried argued "*there can be no trust where there is no possibility of error*" [40], the issue of errors affected people's trust in adopting a privacy system in a fundamental way, such that users have little patience in building trust with the

system. Iachello and Hong claimed privacy concerns could be alleviated if the users trusted the system [54]. It would be important to implement privacy management systems with a high degree of technical trustworthiness upfront to increase acceptance.

On the other hand, trust in the protection techniques (Dim in particular) seemed to grow with experience. 8 participants who agreed protection was useful extrapolated from their real-life experience or experience formed during the study. For example, P26 trusted Dim from her real-life experience when she looked over and couldn't see the screen contents of her classmates with the dimness on. 5 participants reported not having confidence in the Dim technique at first but changing their opinion after playing the onlooker in the game. P22 changed her ideas towards Dim after collaborative tasks:: "*I learned through the study how well the dimming does help when it's dealing with numbers. Because I couldn't see P21's numbers when it's right there. And she wasn't trying to hide it from me.*" Distrust could be built in the same way. For example, P24 stated: "*When the screen get dimmer, I didn't have much challenge reading it…So I assume somebody over my shoulder would have no real trouble reading it either.*" Similarly, Iachello et al. found that positive direct experiences are the most important influencers of a user's trust in a system [54]. Nonetheless, we must note that such confidence or distrust might not necessarily align with the truth as the ability to see depends on the onlooker's vision, the environment, and other factors, not on the users' egocentric inferences.

Trust could also be reinforced by a clear understanding of the technology's capabilities and limitations both during design and in use. 3 participants expressed that they thought the notification only considered distance and not the field of view of the onlooker. This may have created the impression of false detections. As P22 stated: "*I don't know how else it would notify you. I wouldn't have known that technology existed*." Providing more information on how the system works and helping users build a mental modal about the technology would be useful. P24 suggested how demoing the system in a safe environment, "*...gives me an idea of not only what it's supposed to do, but what it's not supposed to do so that I could feel more informed about what the thing is doing,…more comfortable with the program*." P22 also said: "*I would want more information on how it*

senses somebody behind me like how accurate it was. So that's why I didn't trust it enough because it just wasn't making sense a lot if I don't know how it's working."

6.3 Cultural Implications

Altman et al. claimed that privacy management involved cultural-specific regulatory mechanisms [5]. Half (13) of our participants were from North America and the other half were from Asia and the Middle East. In this section we discuss possible differences due to cultural background. Brudy et al. argued designs that enhance mutual awareness between the user and the onlooker could exploit social protocol to regulate both parties' behaviour [18]. This strategy was only mentioned by 3 participants from North America. P21 said: "*If the observer sees that [notification], and they might back off, which I guess it's a good thing*." P25 said: "*If the observer saw the icon, then it could potentially scare them off…even make them move to different locations. But I think I would want to scare people. I felt like that would be better [laugh]*. " Similarly, P23 commented: "*maybe it's like guilting them into not looking…They should feel bad if they're trying to see my information, I wouldn't feel embarrassed at all…. Maybe it would teach people to not look at other people's screens*." Only 1 North American participant expressed concern for the impropriety of the eyeball design. On the contrary, no participants from Asia or the Middle East perceived mutual awareness as a strategy but 9 of them repeatedly used "*impolite*", "*unfriendly*" or "*not respectful*" to judge the social appropriateness of a design and suggested resorting to more secretive designs. For example, P12 described how the system could help her protect Facebook or Instagram passwords from close friends: "*You're politely protecting your password…When you do it in normal situation, you understand it, and you can still have your privacy, even with your close friends.*"

1 Middle Eastern and 1 Asian participant also seemed to be hesitant to take actions upon a privacy breach because "*It's sometimes not respectful to turn it like this…It's kind of rude…in my culture. But in Western culture, it's quite normal. People are much easier to do their personal stuff or hiding these things*." (P11). "*My concern is… even though I noticed someone is staring at the tablet, how could I react? Just say 'what are you*

looking at'?... It's not something polite to do" (P4). On the contrary, P1, a participant from North America, said: "*I think if you are in public and someone was doing that, you just stop… It would just be, you call security*."

When talking about the difference from real life as an onlooker, most participants agreed they had the chance seeing others' screens, they would be less obvious (e.g., "*Just sit behind the person or next to the person and try to act as I am doing something else*", P18; "*I want to be subtle*", P19), and they didn't want others to know that they were looking. 3 participants from Asia and the Middle East indicated that looking at others' stuff was bounded by social protocols. For example, P7 said: "*I would try not let other person know that I'm seeing his tablet. [if they know] That would be very unpolite. Should respect privacy"*. P9 claimed watching even family members' digital devices "*This is difficult. It's very rude*." P11 explained: "*As a person, if I'm curious of seeing what is happening on someone's screen… I feel guilty to do so*." 2 Participants from North America thought they wouldn't mind seeing others using digital privacy systems as an onlooker. P2 commented: "*That's funny. I don't think I would care as an observer… I guess I would just feel like they want privacy.*" "*It is private stuff*," said P17.

A potential explanation is through Hofstede's individualism-collectivism dimension of culture which highlights the difference of relationship between individuals and ingroup members [52]. According to Triandis et al., the core of collectivism includes "*concern for the integrity of the ingroup*" and "*subordination of personal goal to ingroup goals*" whereas individualism suggests pursuit of personal goals and less concern about the ingroup [95]. A number of Asian and Middle Eastern cultures are traditionally collectivism-oriented, whereas North American culture is often characterised as more individualistic. Anthropologic research [100] observed significant cultural differences in maintaining personal privacy: compared to American college students, Arab students faced each other more directly, moved closer, touched each other more often, looked each other more squarely in the eye and talked in louder voices. Our results suggest that culture might also play a role in perceptions and usage of such mobile content privacy management systems. While we have interesting observations that suggest potential

cultural implications for further research, we don't claim to have validated any cross-cultural differences.

6.4 Designing Content Privacy Systems

We summarize the contexts in which notification is useful and not useful (see Table 18), strengths and weaknesses of Dim (see Table 19), Mask (see Table 20), the possible usage scenarios of the proposed content privacy system (see Table 21), and suggestion for improvement (see Table 22, and 23). We also provide design guidelines in the end (see Table 24).

6.4.1 Notification

Table 18 Useful and non-useful scenarios for notification.

Notification	Useful	Not Useful
When	Users don't expect someone looking or are not aware (12) - Focus on primary tasks, forget about surrounding (P9, P16) - The onlooker is quiet and doesn't make noise (P22, P16) It complement human physical mechanisms It works reliably It is noticeable but not overwhelming	Users are aware of the danger Users could be aware using human physical mechanisms It doesn't work accurately (10) - False alarm: alert unnecessarily (P24) - Miss: doesn't alert when there is potential threat (P26) Users fail to notice it (2) Alert too frequently so that it is ignored The meaning of the design reveals user's intention for privacy (P11)
What	Very sensitive visual information Browsing, login to account, enter password, etc. (P12, P15, P20)	Sensitive verbal information (P11) Non-sensitive information
Where	In public (subway, bus, library), semi-public (work space) place (4)	In private place
Who	mainly strangers, acquaintance (P16)	Family members, colleagues (sometimes)

Notification	Useful	Not Useful
Why	Limitation of human cognition (P26) Save attentional resources Decrease precaution (P25) Indicator of whether following protecting action is successful (P14, P23) Guide privacy response or recover (e.g., move locations, change passwords P10)	Fail to serve its purpose Get in the way (e.g., size, location) (4) Be distracting/annoying (5) Attract undesired attention (P25) Lead to social embarrassment (P2)

In addition, regarding participants' expectation of how notification should work, the system's **detection algorithm** is important: the system should only alert the user when someone not in the position of trust is behind, looking towards the device without occlusion (e.g., a wall), and looking for a relatively long period instead of glancing (P18). Controlling the alert **frequency** in busy environments to avoid cognitive burden, habituation, and confusion is also a major concern. Disabling it after raising awareness (P18, P26) or varying frequency based on information sensitivity (P10) could be useful.

6.4.2 Protection

Dim

Table 19 Strengths and weaknesses of Dim.

Dim	Strengths	Weaknesses
What	Harder for observer to see (15) Low interference with user's work (6) Don't require user's reaction Work also as a kind of notification (5) Subtleness protects privacy intention (P5) Save battery life (P22)	Harder for the user to see (7) Not strong protection (8) Frequent changing screen (automatically) is distracting (P18) Conflict with built-in brightness setting (P3)

Dim	Strengths	Weaknesses
When	From far away For text information For details protection The environmental brightness contrast is low Medium-sensitive information Working with the whole document Observer looking from an angle User with good vision	From close proximity For color, shapes, images For overall understanding protection The environmental brightness contrast is high (too bright) Highly sensitive information Working with details Observer looking straight User with weak vision

Mask

Table 20 Strengths and weaknesses of Mask.

Mask	Strengths	Weaknesses
What	Strong protection (22) Allow for fine-grained user control (P17, P2) Protect information privacy Protect context privacy Work as a kind of notification (2)	Difficult to navigate through Require user effort (8) Slow users down Limit user's visible area (8) Attract unwanted attention
When	From close proximity For overall understanding protection For familiar layout/structure For sparse text information Working with a small area For information retrieval tasks For highly-sensitive information (e.g., bank, login, email, employment detail, weight monitor)	From very close proximity For information within the viewport For unfamiliar layout/structure (P8) For condensed text information Working with full screen (P11, P22) For inputting (e.g., typing) task Time-sensitive tasks

Selective Hiding

Participants were given a medical record prototype and asked to reflect on the strengths and weaknesses of Selective Hiding at the end. The "*absolute level of protection*" (P13) came with a cost of "*compromising the user's experience for retrieving the data, which is why you're using it in the first place*". Comparing to the demoed all-or-none protection,

users expressed desire for more fine-grained control (e.g., content type/part, timing, transition between hide/display). The usefulness was also thought to depend on if the hidden data is relevant to the current task (3) and how well the system could discern between sensitive and non-sensitive data (3). Examples of usage scenarios included selectively sharing personal profiles (e.g., student, tax record) to colleagues, patients checking in at the waiting room of doctor's office or nurse reading complaints in public.

6.4.3 Digital Privacy System as a Whole

Expected Usage Scenarios

Table 21 Usage scenario for digital content privacy management system.

	Digital Privacy System Usage Scenario
Where	Public transportation (e.g., bus, subway), traveling (e.g., airport) (10) Workplaces (e.g., office, lab) and study places (e.g., library, classroom) (12) Coffee shop, restaurant, benches, parks (7)
When	Not very often, only really in emergency and have to do something Sit side by side with other people or people passing by No private spot is available Feeling unsafe or uncomfortable with others around
What	Banking (e.g., check, transfer) (16) Logging into accounts/typing passwords (9) Writing private emails (5) Viewing personal or potentially embarrassing photos (5) Chatting with friends with sensitive text messages (4) Other personal use such as social media, browsing/searching on the internet, viewing video galleries, viewing medical data (6) Organizational trade secrets (product launch plan, customers profiles), (3)
How	Mostly use protection techniques, may turn it throughout the task to focus Notification mostly used in work place or with familiar people Turn it on if need it (7)

	Digital Privacy System Usage Scenario
Who	Ordinary user for personal use Business people with confidential data (e.g., stock, trade secret) (2) Government or institutes employee with access to confidential data (1)
Viewer	Mostly strangers Colleagues, or acquaintance with no personal relationship (2) Friends --only with high sensitive info like bank, accounts/password (2) Family --only with embarrassing chats and photos (e.g., drunken stupors) (1)
Platform	Desktop computer, laptop, mobile phone, tablet, ATM (6)

In summary, people would use the system in absolutely necessary occasions. Due to the high subjectivity of privacy, participants expected the digital privacy system to be enabled or disabled based on users' own discretion (based on location, activity, perception of safety of the environment, and time). As P24 noted: "*the most important is setting it up in a way that people can personalize that the way they like it*".

Trade-offs in System Design

We observed a real or perceived trade-off between work efficiency and **physical** privacy management. 6 participants claimed it hard to do two things (play the game and hide the tablet) together. For example, P25 reported: "*The game was more difficult when trying to, you know, be aware of the fact that people are watching you. It made the game more difficult to enjoy and to do well*." We also observed trade-offs in the digital system design. The dilemma between being noticeable and not distracting of **notification** design was echoed by 4 participants (e.g., "*Sometimes…I don't see the notification at all and whenever it gets my attention I just forget what I was doing so it is distracting*", P18). Moreover, notification should attract users' attention without attracting onlookers' attention. The trade-off between protection and utility existed in all **protection** designs: for Dim, "*I see the point of being dim so no one else can see. If you lighten it more then I guess more people can see too*" (P8); for Mask, "*Mask is more protective, but Mask is also interfering*" (P11); for Selective Hiding, "*It will be a trade-off between having the information to do the task and maintain the privacy*" (P17). Similar as the previous study, for protection mechanisms, it is a fine line between people's willingness to put up with

interference versus their desired level of privacy in a specific context (e.g., *"With the mask, it was uncomfortable enough that I believe in it…But that wasn't super annoying", P24*). The perceived usefulness is also subjective and situational dependent.

Concerns about the System

Unlike the previous study, the top concern became the **reliability and accuracy** of the system. Nearly half of the participants mentioned this to be the major or the only concern. For example, P15 thought "*The precision is very important in this case*" that it would lead to confusion and distrust about the system. P16 stated: "*If it's not correct enough, I think it'll be better that I use nothing*". P25 said: "*Just trying to improve the accuracy. **That's always something, I guess, everything***." 4 participants were concerned about whether the privacy system itself put users' general privacy at risk: 2 participants would worry about whether this privacy management system comes from a credible developer. 2 participants worried about sensitive personal information accessed or stored by a third-party software (e.g., in the case of how Selective Hiding search and selectively anonymize crucial information) or the application tracks and saves what the user is doing. 3 participants had **social concern** that the system might make other people uncomfortable or offended. 1 participant asked about the feasibility of deploying the system in the real world. 1 participant further worried about risks beyond a physical person (e.g., sitting with a mirror behind, cameras in the room). Others talked about aforementioned challenges for notification or protection design such as being annoying or not noticeable, or slowing user down. One participant worried that the protection system might take up system memories that make other apps slow down or crash.

6.4.4 Suggestions for the System

Notification

The main suggestions for notification focus on enabling customizability, and solving the problems of noticeability, getting in the way and distraction (see Table 22).

Table 22 Suggestions for notification.

Dimension	Suggestion
Customization	Location, size, color (3) Icon (e.g., a star, animal, or keyword) (5)
Noticeability	Add color contrast between the notification and background (P16, P13) Turn 4 edges of the screen red and blinking in extreme conditions Change the color and location regularly to combat habituation (P10) Make the location in the center (2) Make it cover the whole screen (P17)
Getting in the way	Movable notification or shrink to a smaller size after some time (P25) Use LED lights as notification (P5) Make it transparent like watermarks (P16) Change it to smaller size Alternatively show and hide
Distraction	Less obvious or "flashy" (P6) Stay on for some time once pop up (P8, P17) [add tolerance to detection] Notify when someone is staring instead of glancing (P8) Easily disable it in crowded places (P25)
Consistency	Change it to built-in notifications (e.g., message box) (2)
Multi-model	Use vibration (P11, P18) Use optional sound alerts (4), but it could be annoying or not heard in busy environments (P21), and it should avoid obvious meaning (P25) Combine different modalities of notifications
Source of Threat	Point out the whereabouts of the potential shoulder surfer Identify the shoulder surfer from multiple people in the surrounding (P17)
Other	Notification could be applied to conversation or activity privacy (P16)

Protection techniques

The suggestions for protection techniques concentrate on increasing utility (e.g., easy access, less effort), customizability (to address diverse individual needs) and level of protection (e.g., intention, speed) (see Table 23).

Table 23 Suggestions for protection.

Dimension	Suggestion
Dim	Dim differently based on angle (mimic screen protector) (P2) Lower contrast between Dim and the information to protect (P24) Gradually dim the screen to differ from automatic brightness adjust (P15) Customize the default value of brightness (P16)
Mask	Blur the masked area to protect intention privacy (P9, P3) Make the viewport size adjustable (e.g., by gesture) (3) Multiple viewports to increase visible area (P11) Move the viewport automatically by gaze detection (P15, P16) Customize the color of Mask for users with different eye conditions
Selective Hiding	Easy switch between hide and display (e.g., touch, long press, double click) Use viewport over the hidden information to deanonymize it Decrease the fidelity of the information but still allow the user to read Preserve the appearance of anonymized data (e.g., pictures still look colorful)
Other	Automatic protection should stay on for certain amount of time (P8) Manual protection should support prompt trigger (P19) Combine Dim and Mask (P11) Change the size of the content as a protection measure

In addition, participants suggested increase the reliability and accuracy for the whole system (3). It is also important that the system provide context-awareness: 3 participants wanted to customize the locations (bus, office) to enable notification / protection; 4 wanted the system be turned on automatically in intended usage situations or remind users to turn it on; 1 suggested infer the risk of privacy breach by detecting how busy the environment is (e.g., how often people walk by) and how often the same person appears for fine-grained protection (e.g., dynamically adjust level of dimness).

6.4.5 Design Guidelines

Bellotti identified 11 criteria for designing for privacy access control in ubiquitous computing environments: *trustworthiness, appropriate timing, perceptibility, unobtrusiveness, minimal intrusiveness, fail safety, flexibility, low effort, meaningfulness, learnability* and *low cost* [13]. For designing privacy control of on-screen content on mobile devices, some of the same criteria can be applied (see Table 24, highlighted in blue). On the other hand, there are principles specific to mobile content control that emerged from the study (see Table 24, highlighted in yellow)

Table 24 Design guidelines and implications.

Guidelines	Explanations and Design Implications
Trustworthiness	System accuracy, design within a technology's limitations, management of expectations, and general privacy settings would help build user's trust towards the system and promote adoption. [*5.4.4, 6.2, 6.4.3*]
	The system accuracy has to achieve an acceptable level. Cultivate direct positive experience of using the system. Allow for configuration of whether the system tracks the user's activity or store their data.
Appropriate timing	Users required awareness at the point shoulder surfing occurs and prompt protection. [*6.2*]
	Notification should be accurate in timing. Manual protection should support easy trigger and immediate response.
Perceptibility	Notification needs to be perceptible as awareness is the foundation for subsequent privacy management behaviours. [*3.4.3, 5.3.3*]
	Use polymorphic [7] notifications (e.g., change shape, color) to mitigate habituation, use moticons [12], combine multiple privacy modalities
Unobtrusiveness	System should impose low cognitive burden on the users: notification should avoid excessive occurrences especially in busy environments; protection should reduce interference particularly in work-related tasks. [*3.5, 5.4.4, 6.4.1*]
	Using different cognitive processing channel (e.g., sound, vibration), meta information [91] (e.g., information about severity of privacy breach, source of breach etc.) to reduce information overload. Avoid complicated design such as fine-grained notification and literal design. Limit the frequency of notification in busy environments.

Guidelines	Explanations and Design Implications
Flexibility	Support flexible configuration of design aspects to accommodate subjectivity of privacy issues (e.g., user preferences, task sensitivity) [*3.4.3, 5.4.3, 5.4.4, 6.1*]
	Support customization of preferred awareness (e.g., size, location, color, granularity) and protection techniques, level of delegation to the technology, privacy modalities and working mechanisms. Allow users control (override the system behaviour, fine-grained).
Low effort	Protection techniques which require user's physical or mental effort to control (e.g., Mask) should involve as little user interaction as possible. [*5.4.3*, *5.5.1*]
	Integrate gaze-based control (e.g., viewport of the Mask).
Subtlety	Support non-obvious physical movements and apply non-prominent digital system appearances to avoid unwanted attention or curiosity [*5.3.1, 5.3.2, 5.3.4, 6.1*]
	The meaning of notification should be clear to the users but obscure to onlookers (e.g., customizable glyph icon / sound / vibration). Protections should also avoid drastic changes to or striking contrast with the primary interface. Avoid conspicuous gestures to trigger system response.
Complementarity	Base (digital) system decisions on an understanding of the environment and both the user and the onlooker's (physical) capabilities and limitations [*3.4.1, 5.4.4, 6.1*]
	Avoid unnecessary alerts / responses by precise inference and detection of real threat (e.g., stranger looks in the direction of the device without occlusion for some time)
Context-awareness	The usage scenarios of digital privacy system is highly dependent on contextual elements such as screen size, information sensitivity, potential viewer, location, time, movable and fixed built of the environment. [*5.3.4, 5.4.3*]
	Integrate context information (time, location, identity recognition, environment sensing)
Transparency	Misunderstandings about how the system works will affect the perceived usefulness of the system and adoption. [*6.2*]
	Provide information that facilitates building a correct mental model of the sensing technology, detection algorithm etc.
Fluid transition	Support quickly changing context of use [*5.5.3*]

Guidelines	Explanations and Design Implications
	Allow users to easily turn the system on or off, switch between usage scenarios (e.g., personal mode, collaborative mode), and transition between hiding and displaying data in cases where partial data is hidden for privacy
Socio-cultural awareness	The visual presentation of the system should be sensitive to social norms (for both users and onlookers). [*3.4.4, 6.1, 6.3*]
	Whether obvious designs should be used for social regulation depends on social and cultural acceptability.
Work precedency	Efficiency takes precedency over privacy in work-related scenarios [*3.5, 5.5.2*]
	Avoid compromise work-related information. Avoid protection techniques that interrupt workflow.
User compatibility	Collaborative content privacy management should support potential conflicting needs of collaborators. [*5.5.1*]
	Protection techniques should enable multi-view visibility, match different privacy preferences, and be as less interfering as possible.

Similar as Kindberg et al.'s classification of users in terms of security concerns in mobile interaction [58], the 14 design guidelines of mobile content privacy could be grouped into 3 categories: **trust-oriented** principles include *trustworthiness*, *appropriate timing*, *complementarity*, *transparency*; **convenience-oriented** principles include *perceptibility*, *unobtrusiveness*, *flexibility*, *low effort*, *context-awareness*, *fluid transition*, *work precedency* and *user compatibility*; **socially-oriented** principles include *subtlety* and *socio-cultural awareness*. These guidelines could overlap (e.g., *transparency* is one way to achieve *trustworthiness*) or contradict each other (e.g., *perceptibility* competes with *unobtrusiveness*). In general, the guidelines could help make decisions during design process or be used as evaluation criteria to assess mobile content management systems.

6.5 Observing Privacy Behaviours in the Lab

Many social and psychological studies conducted on personal space intrusion and people's privacy reactions in 1970s followed a field study approach. Researchers

manipulated confederates' physical distances, body positions, or excessive intimate behaviours (e.g., gaze, touch) to study patients in hospital public areas and day-ward rooms, university students in libraries, and people at street corners waiting for buses etc. [4]. The results showed people invaded either fled quickly or displayed systematic non-verbal behaviours such as moving/facing away, fidgeting, using arms, hands or barriers such as books to block the invader [28, 73, 30]. More recent studies examining physical privacy management behaviour in everyday life [21], organizations [32] or hospitals [68] through archival analysis, case study and ethnographic approaches. There is relatively less direct research of physical privacy management in lab settings. When evaluating pure physical privacy mechanisms, more naturalistic approaches would be helpful to introduce invasion and observe responses directly. However, when evaluating the impact of novel digital mechanisms and technologies on mobile content privacy, field studies face a number of challenges: 1) people's privacy concerns inhibit them from accessing very sensitive information in public spaces due to insufficient existing ways to help maintain privacy. It is less likely to observe such behaviours in the field than in lab settings. 2) Due to the mobility of mobile devices, the usage of privacy-sensitive information is highly context-dependent and ephemeral. It would be difficult to capture such moments to introduce intrusion or record the responses. 3) The immaturity of current technologies used to support the interface make it infeasible to deploy the system of interest in the field.

One of the central criticisms lab studies receive is the lack of realism or ecological validity. According to Brunswik who coined the term "ecological validity" in 1940, the essence of an ecologically-valid approach lies in retaining the integrity of environmental causal factors [30]. Falk and Heckman argued that realism or generalizability problems is not a feature that distinguishes lab study from field study, and that the true issue is to isolate causal effect [38]. Moreover, ecological validity is argued to be achieved through employing representative settings, stimulus and task design to help generalize research findings from a particular study [87, 60]. We argue that our lab approach was not only necessary but also appropriate for the following reasons: 1) The diverse privacy behaviours we observed in the study had their counterparts in reality. For example,

participants who carefully chose to sit in the middle of the couch were similar to people who deliberately pick a corner of a room; Participants who moved from one side to the other side of the couch simulated people who move away or leave an area. 2) With only 3 participants claiming to be willing to participate if the study used their real bank accounts, it verifies that the recruitment didn't preclude participants with high financial privacy concerns. 3) Participants reported a high degree of realism in the individual and collaborative task design and their role-playing. They also agreed the tasks contained highly sensitive materials (e.g., bank information) and reported a high motivation to preserve privacy of the fake study data and respond accordingly. Although undesirable effects of fake data still existed (e.g., 2 participants reported not behaving as carefully as they would in real life), it was largely mitigated.

6.6 LIMITATIONS

While we claim the methodology was appropriate for the research questions and the study results were validated from multiple perspectives, there are several limitations of the current study.

Drawbacks of lab evaluation: Firstly, we must note while our observations of privacy behaviours in the lab are good in terms of diversity and analogy to the real world, they are by no means precise reflections of real-life behaviours. There are differences in terms of quantity, magnitude, and types of behaviours. For example, the study setting restricted participants to stay and complete tasks regardless of their actual concerns thus prohibited them from demonstrating prevention measures or effectively utilizing the environment features. Secondly, participants were very aware of the need to manage privacy and perhaps overreacted in comparison to real life behaviours. They might also behave a certain way in order to be a good participant because they know "*the point was to provide protection*" (P21). They might be primed from the post-session interview questions such as "*did you try to protect Casey's bank information*", or from the fact the research confederate conspicuously wore a headband. Thirdly, we did not put participants in a

setting that matches intended usage (e.g. workplace, coffee shop). This might exclude certain contextual factors such as trust in other people or perceived safety of the locations that might have resulted in different behaviours. Finally, we have a limited sample size and representativeness, making it problematic to generalize our results to the general population. Due to time limits and concerns for a fatigue effect, we didn't have participants experience all interface conditions in every activity.

Ambiguity of privacy behaviour: Altman et al. identified the issue of whether the observed behaviours truly hold a privacy-related meaning [6]. Non-verbal behaviours are often ambiguous due to multiple meanings, and the meanings vary with individuals, contexts, and culture. We encountered similar issues in coding participants' privacy management behaviours. For example, two researchers had different interpretations of the behaviour "*smiling*": one thought it was a nice way to say "*move away please*", the other thought it could be interpreted as a knowing smile to family or friends which didn't necessarily contain privacy meaning. We resolved this issue by using approaches in related literature and especially our participants' self-reported behaviours to corroborate all the coded behaviours. The drawback of this decision is that people often aren't aware of their own behaviours and can be bad at articulating our strategies post hoc. We argue that participants were very aware of the purpose of the study, explicitly instructed to protect their information and reflect on their strategies. Thus privacy behaviours are rather conscious in this context. We also found it is hard to infer the meaning of participants' subtle movements (e.g., look around, body leaning, pull the tablet towards the body) as having a privacy-related intention. We addressed these issues by keeping the coding standard consistent across the tasks so that the impact of error was equally distributed across all conditions.

Tracking technology: The limited tracking range, metal in the ceiling, floor, and objects not able to be moved (e.g., tabletop, host computer) might have biased the tracking data to cause inaccurate alerts or responses of the digital system (i.e., false alarms, misses). The inaccuracy led some of the participants to be confused or even paranoid, and to develop mistrust towards the system so as to ignore the notifications (less protective) or

rely more on their own behaviours (more protective). As the sole purpose of notifications is to provide accurate awareness, the usefulness of notifications might have been undermined. As for protection techniques, the inaccuracy might have biased some participants to prefer manual control instead of automatic control. We argue that participants' attitudes (as measured through questionnaires) were not fundamentally influenced by limitations of the tracking technology because firstly despite the error, all digital system supported conditions were rated as providing more awareness, protection, balance and satisfaction than pure physical methods. Secondly, each participant completed 9 tasks both as a user and an observer. Most participants experienced the system working both properly and not so well thus could evaluate it in an all-round manner. Thirdly, only a small portion of participant preferences were attributed to the factor of reliability.

Task design: While the hide-and-seek game design allowed us to observe a variety of explicit privacy management behaviours, we didn't expect that the rules of the game which were meant to add realism (e.g., the spatial constraint by the proxemics circle and temporal constraint by the "ding") led the participants to not only consciously use but also heavily rely on their physical mechanisms in the game. Thus participants didn't use the digital system as much and it's hard to observe a difference between the physical condition and digital conditions. It also indicates that in extreme conditions when users are super-aware of immediate privacy threat, they naturally and involuntarily resort to physical methods. For objective measurement of visibility from the observer, the actual observed information was mixed with memorability and recognizability of the material. Thus more stable and direct measurements could be used in the future. Secondly, we chose financial information which had universally high privacy concern to probe privacy behaviour and judgment. Because the security and privacy concerns are so high that too often in real life people take prevention measures (e.g., only perform such tasks at home) instead of physically managing the risk in public. While we are trying to support scenarios where prevention strategies are not available (e.g., can't find a private spot, must perform a transaction at the moment), we don't claim the digital system is suitable for everyday usage. We wanted to evaluate when people do have privacy concerns in

certain absolute necessary situations whether the interface could help address their concerns. Also, such public privacy management might become more acceptable if they feel their data is safe when doing so. Finally, one flaw of the collaborative task design is that the bill-splitting scenario, while familiar, didn't often occur in public places for our participants. The task also didn't fully engage both participants throughout. Scenarios like hospital collaboration or those involving secretive activities might be used to better elicit collaborative privacy responses. In addition, other types of tasks such as reading email, texting message, viewing profiles could also be used for further exploration.

6.7 FUTURE WORK

This work explored the effect of privacy notifications and protection techniques on people's content privacy management on mobile devices. There are a number of possible improvements for the future design of such proxemics based systems.

- **Awareness indicator**: For on-screen privacy notifications, the effectiveness of text, icon, and animation has yet to be determined. Parameters such as size, location, alerting frequency, lasting time, sensitivity, granularity (coarse-grained or fine-grained), and polymorphism can also have an impact. Other modalities of notification such as LED lights on mobile devices, sound, vibration, or combinations of two or more modalities could also be further explored. The role of automatic protection as an implicit notification could be compared with explicit notifications. Additional information such as the number of viewers, distances and bearings of the threat, the shoulder surfer's gaze point and visible area could be integrated to assess risk and enhance awareness.
- **Detection technology**: Vigliensoni and Wanderley found that Vicon had the overall best performance comparing to Polhemus, Kinect and Gametrak [97]. The main drawbacks of the Vicon system is its high cost and the setting up procedure [17]. It also requires people to wear markers and thus is not feasible for a field deployment. Markerless motion capture (MMC) technology like Kinect sensors are less-expensive, markerless and portable alternatives for potential more practical deployment. The

distance accuracy (e.g., a minimum of 8.4 cm error for static postures, [104]) could be acceptable for detecting interpersonal spatial relationships but questionable for detecting more subtle movements. The angle estimation depends on joints (e.g., shoulder was good, wrist and ankle were poor) [14]. On-board cameras could be another alternative but have the limitations of narrow field of view or detecting shoulder surfing with the corner of eyes. This suggests that eye tracking technology might also be integrated to the system. Google's Project Tango prototype (a tablet-like device with a 7-inch screen, a motion tracking camera and a 4MP 2um Pixel camera, and infrared depth sensors) could track the 3D movements of the device and constructed a 3D model of the environment at a recommended distance from 0.5-4 meters [81, 82]. The spatial perception ability is possible to take physical built of the environment into consideration to better facilitate holistic mobile content privacy management.

- **Protection techniques**: Other protection techniques could consider different types of information (e.g., text, image), semantic analysis of the information (phone numbers, names, photo), tasks (e.g., searching, typing, reading). One alternative protection technique could introduce noise into current information (e.g, change pictures or text segments). The level of protection could be studied from an observer's perspective in a more objective manner, as user trust isn't always consistent with an observer's ability to see. For example, grayscale might be more useful than the participants thought for certain data under the right conditions.
- **Other privacy processes**: The roles of awareness, detection and response were implemented and discussed in the study. Other processes such as prevention and recovery should be incorporated into a holistic system. For example, the system could recommend pro-privacy management locations, help users to quickly switch to a different window or turn off the screen when a threat is present. If the system detects that the information being exposed to onlookers for a long time, it could remind and help user modify/delete sensitive information as a recovery method.
- **Proxemic behaviours**: We used the distance between the tablet and onlooker as well as the looking direction of the onlooker relative to the tablet to trigger privacy awareness and system response. With an increased tracking and sensing ability of

mobile devices, other types of proxemic behaviours observed in the study (e.g., moving the tablet, turning the tablet angle) could also be used to mediate privacy management. The built-in proximity sensors on mobile devices might also sense a barrier or blocking from users' body parts to trigger or delay privacy processes. One challenge with explicit protection is to distinguish users' privacy management behaviours from users' spontaneous and subtle movements. In other words, an ideal system would correctly infer user intention. Moreover, correctly inferring the intention of the onlookers (e.g., accidental or purposeful, benign or malignant) would clearly be beneficial. Such inference may not always be possible, especially using proxemics information alone.

- **Platforms**: We used 10.6-inch tablet interface for the evaluation. Mobile phones carry more sensitive data, and are more pervasive thus more exposed to visual privacy threat. On the other hand, phones have smaller screen sizes, and people's physical privacy mechanisms could be more effective (e.g., use hand to cover, easier to move, turn, block) but the interference from the digital system (e.g., notification that takes up screen space; protection that lowers visibility) could be more problematic. How to design systems to accommodate these characteristics is worth future research.
- **Field evaluation**: With a more practical implementation, field studies would be beneficial because some contextual factors might impact the effectiveness of system design, especially for a system which alternates visual attributes of the information to manage privacy. For example, in our design exploration, 1 participant performed the tasks in the evening. The environmental brightness was low making Dim less useful. Field experiments and experiential sampling methods [1, 55] could help to understand user decisions *in situ*.
- **Multiple onlookers**: The privacy system is meant to be used in public spaces with potentially multiple people around. Designing for a crowded environment is more challenging. With a single onlooker and less than 30-minutes task time in the study, some participants already reported the notification being annoying. It would be necessary to examine how to design awareness features that are informative without overly disrupting users in the long run.

- **Workplaces**: Privacy management in workplaces where working efficiency is often the first priority is different from personal information management when users are more tolerant toward inconveniences the system brings in exchange for privacy. Users are less likely to put up with even minor interference. Design for minimal interference that best supports efficiency while respecting privacy is another topic.
- **Perspective of the onlooker**: Due to the social implications of digital privacy management, it is interesting to investigate onlooker's behaviours and perceptions. For example, the *type* of onlooker in terms of social relationship with the user (e.g., stranger, acquaintance, friend, family) would likely to have an impact on the social dynamics between the user and the onlooker.
- **Cross-cultural comparison**: Different cultures bring different norms and customs surrounding privacy management. One possible research strategy here is to use case studies to investigate cultures with high social contact (e.g., Mehinacu Indian) versus cultures with lower social contact (e.g., Pantellerian) [6]. This strategy could be used to compare the usage patterns and attitudes towards the digital system by people from cultures with distinct privacy regulations.

CHAPTER 7 CONCLUSION

With the widespread diffusion of mobile devices, the ever-expanding smartphone screen size, and the diversity and fragmentation of mobile usage in a variety of dynamic social situations, the possibility of breaching mobile content privacy is expected to increase in the future. Physical movements could be used to maintain privacy but users face the challenge of being cognitively aware of constantly changing contexts, the inconvenience of covering the screen while focusing on the primary task, advertising desire for privacy through obvious management and the social awkwardness of implying distrust towards other people. This thesis work builds on privacy management theories and proxemics interactions, and serves as an early exploration of how software-based solutions such as privacy notifications and protection techniques could preserve privacy by alleviating cognitive, physical and social burdens.

We first designed privacy notifications in the form of on-screen glyphs and protection techniques that alternate visual attributes (e.g., color, brightness, visible area) of on-screen content to address awareness and response which are the two essential processes in privacy management. We evaluated these designs with typical privacy-related scenarios in a university library with Wizard of OZ methodology and 12 participants. The findings are as below:

- **Notification**: Participants preferred notifications that could be immediately understood, and that would capture attention (*perceptibility*) when necessary and not distract from the primary task (*unobtrusiveness*) with subtle changes or movement. Metaphorical notification is preferred over literal ones for being less distracting.
- **Protection:** Protection methods have their own strengths and weaknesses. The choice of a specific technique is dependent on the task at hand, information type and sensitivity, individual users, identity of potential viewers, time and location. This suggests flexible user configuration (*flexibility*) so that users' privacy preferences match the level of privacy desired.

- **Overall usefulness**: Participants considered both notification and protection mechanisms to be useful by complementing existing physical ways to manage privacy (*complementarity*): notification could reduce looking around and cognitive load by "adding an eye in your back"; protection could allow work to continue in a normal pose and alleviate social awkwardness of physical protection.
- **Workplace privacy**: evaluation with two healthcare professionals showed that privacy in the workplace is usually compromised for efficiency of work (*work precedency*). Any added system should be sensitive to extra cognitive burden enforced on the user under existing mental stress.

We then implemented a working prototype which leveraged proxemics information sensed by the tracking technology to provide just-in-time detection in addition to privacy notifications and protection. We evaluated the prototype in the lab setting with 26 participants to systematically observe physical privacy management behaviour, further our understanding of the relationship between awareness and response process which seemed to be divergent in the design evaluation, and explore the digital system at a small-group level. The major findings are as follows:

- **Physical privacy behaviour**: We found that physical nonverbal privacy behaviours observed in the study cluster into 5 types: awareness, macro protection, micro blocking, device maneuver, and environment utilization. Participants gave up effective but obvious macro protection and resorted to smaller-scale body movements in more realistic scenarios.
- **Digital privacy management**: Digital privacy system was perceived to help raise awareness, facilitate hiding information, balance work and privacy and bring more satisfaction. While we didn't observe a clear change of behaviours, participants reported that digital support could promote awareness (notification), enhance protection, help concentration, and reduce prevention (protection).
- **Mechanism design:** Both notification and protection were preferred for maximum protection, but different combinations of notification and protection were preferred depending on the contextual factors such as individual users, information sensitivity, location and relationship with viewers (*context-awareness*). Automatic protection

help user concentrate, avoid forgetting and provide prompt protection; manual ones allows for more user control, less interference, and less dependence on the reliability of the system. Visual protection techniques vary in their abilities to protect information, context and intention privacy.

- **Small-group privacy management**: slowing down became less tolerable that participants' preferences for protection were reversed in favor of task efficiency. Collaborative mobile content privacy management face the challenges of more difficult physical management and multiple people's potential conflicting needs for digital management. Notification is more noticeable due to the extra attention of members in the group. Protection designs should impose as less interference in workflow as possible.
- **Holistic privacy process**: Content privacy system should consider both the user's and the onlooker's physical circumstances. Users' explicit physical movements and changing screen appearances are also part of the privacy management process in revealing user's intention for privacy or attracting unwanted attention. Moreover, the privacy management processes as a whole could be seen as a distribution of responsibility between physical management and digital management depending on the user preference.
- **Trust**: trust is a key factor for perceived usefulness and adoption of mobile content privacy management system (*trustworthiness*). False alarms, miss detections or inappropriate timing of the system response lead to distrust. More *transparency* on the working principles of technology and direct positive experience could help cultivate trust.
- **Socio-cultural implication**: Obfuscation of the meaning of notifications is considered more useful for privacy purpose (*subtlety*). The visual presentation of the system should be sensitive to social and cultural norms for both users and onlookers (*socio-cultural awareness*).

In conclusion, we believe this thesis work has paved the way for a new area of research on mobile content privacy management. It will benefit the research community in understanding privacy perceptions, behaviours and privacy management models. It will

also benefit the design and engineering community in designing mobile content privacy management systems that meet users' privacy expectations while supporting fluid workflow. We have further shown that the Wizard of Oz method could be used in situ whereas privacy behaviours could be evaluated in the lab with careful control. Designing a holistic mobile content privacy management system that is trustworthy, socio-culturally aware and deeply integrated with physical behaviours is challenging, but it will become increasingly important in the future.

BIBLIOGRAPHY

[1] Abdesslem, F. B., Parris, I., & Henderson, T. N. H. (2010). Mobile experience sampling: Reaching the parts of Facebook other methods cannot reach.

[2] Ackerman, M., & Mainwaring, S. (2005). Privacy issues and human-computer interaction. *Computer*, *27*(5), 19-26.

[3] Almaula, V.K. (2008). *Protecting the login session from camera based shoulder surfing attacks*. Master's thesis, University of California, San Diego, USA

[4] Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding*. Monterey, Calif.: Brooks/Cole.

[5] Altman, I. (1977). Privacy regulation: culturally universal or culturally specific?.*Journal of Social Issues*, *33*(3), 66-84.

[6] Altman, I., & Chemers, M. M. (1984). *Culture and environment* (No. 2). CUP Archive.

[7] Anderson, B.B., Kirwan, C.B., Jenkins, L.J., Eargle, D., Howard, S., & Vance, A. (2015, April) How polymorphic warnings reduce habituation in the brain – insights from an fMRI study. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 1649-1658). ACM.

[8] Ashcraft, N., & Scheflen, A. E. (1976). *People space: The making and breaking of human boundaries*. Anchor Books.

[9] Balebako, R., Jung, J., Lu, W., Cranor, L. F., & Nguyen, C. (2013, July). Little brothers watching you: Raising awareness of data leaks on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (p. 12). ACM.

[10] Ballendat, T., Marquardt, N., & Greenberg, S. (2010, November). Proxemic interaction: designing for a proximity and orientation-aware environment. In ACM *International Conference on Interactive Tabletops and Surfaces* (pp. 121-130). ACM.

[11] Barlas, D., Sama, A. E., Ward, M. F., & Lesser, M. L. (2001). Comparison of the auditory and visual privacy of emergency department treatment areas with curtains versus those with solid walls. *Annals of emergency medicine*, 38(2), 135-139.

[12] Bartram, L., Ware, C., & Calvert, T. (2003). Moticons:: detection, distraction and task. *International Journal of Human-Computer Studies*, *58*(5), 515-545.

[13] Bellotti, V., & Sellen, A. (1993, January). Design for privacy in ubiquitous computing environments. In *Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW'93* (pp. 77-92). Springer Netherlands.

[14] Bonnechere, B., Jansen, B., Salvia, P., Bouzahouene, H., Omelina, L., Cornelis, J., ... & Van Sint Jan, S. (2012, September). What are the current limits of the Kinect sensor. In *Proc 9th Intl Conf. Disability, Virutal Reality & Associated Technologies, Laval, France* (pp. 287-294).

[15] Boyle, M., Neustaedter, C., & Greenberg, S. (2009). Privacy factors in video-based media spaces. In Media Space 20+ Years of Mediated Life (pp. 97-122). Springer London.

[16] Braun, C. C., Mine, P. B., & Silver, N. C. (1995). The influence of color on warning label perceptions. *International Journal of Industrial Ergonomics*, *15*(3), 179-187.

[17] Brudy, F. (2013). *Is anyone looking? Mitigating shoulder surfing on public display through awareness and protection*. Master's dissertation, University of Calgary, Calgary, Canada

[18] Brudy, F., Ledo, D., & Greenberg, S. (2014, April). Is anyone looking?: mediating shoulder surfing on public displays (the video). In *CHI'14 Extended Abstracts on Human Factors in Computing Systems* (pp. 159-160).

[19] Brunk, B. (2002). Understanding the privacy space. *First Monday*, 7(10).

[20] Brunk, B. (2005). A user-centric privacy space framework. *Security and Usability, LF Cranor and S. Garfinkel, Eds*. O'Reilly, 401-420.

[21] Caine, K. E. (2009). *Exploring everyday privacy behaviors and misclosures*. Doctoral dissertation, Georgia Institute of Technology, Georgia, United States

[22] Chen, Y., & Xu, H. (2013, February). Privacy management in dynamic groups: understanding information privacy in medical practices. In *Proceedings of the 2013 conference on Computer supported cooperative work* (pp. 541-552). ACM.

[23] Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012, July). Measuring user confidence in smartphone security and privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (p. 1). ACM.

[24] Cluster Analysis. (2015, September). Retrieved from: https://www.qualtrics.com/wp-content/uploads/2013/05/Cluster-Analysis.pdf

[25] Comscore. (2014). The U.S. mobile app report. Retrieved from: http://www.comscore.com/Insights/Presentations-and-Whitepapers/2014/The-US-Mobile-App-Report

[26] Conduct and Interpret a cluster analysis. (2015, September). Retrieved from: http://www.statisticssolutions.com/cluster-analysis-2/

[27] Cranor, L. F., Guduru, P., & Arjula, M. (2006). User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction* (TOCHI), 13(2), 135-178.

[28] Dabbs, J. M. (1972). Sex, setting, and reactions to crowding on sidewalks. In *Proceedings of the Annual Convention of the American Psychological Association*. American Psychological Association.

[29] Dalhousie Univeristy (2013). Student life news, digital image. Retrieved on May 17, 2015 from http://www.dal.ca/campus_life/student-life-news/archive/oct9.html

[30] Dhami, M. K., Hertwig, R., & Hoffrage, U. (2004). The role of representative design in an ecological approach to cognition. *Psychological bulletin*, 130(6), 959.

[31] Dostal, J., Kristensson, P. O., & Quigley, A. (2013, June). Multi-view proxemics: distance and position sensitive interaction. In *Proceedings of the 2nd ACM International Symposium on Pervasive Displays* (pp. 1-6). ACM.

[32] Dourish, P., Grinter, R. E., De La Flor, J. D., & Joseph, M. (2004). Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing*, 8(6), 391-401.

[33] Downs, J. S., Holbrook, M., & Cranor, L. F. (2007, October). Behavioral response to phishing risk. In Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit (pp. 37-44). ACM.

[34] Duffy, M. (2012). Tablet technology for nurses. AJN The American Journal of Nursing, 112(9), 59-64.

[35] Edworthy, J. (Ed.). (1996). *Warning design: A research prospective*. CRC Press.

[36] Egelman, S., Oates, A., & Krishnamurthi, S. (2011, May). Oops, I did it again: mitigating repeated access control errors on facebook. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (pp. 2295-2304). ACM.

[37] Epocrates, Inc. (2013). Epocrates 2013 mobile trends report. Retrieved on Feburary 17, 2014 from http://www.epocrates.com/sites/default/files/2013_Epocrates_Mobile_Trends_Report_FINAL.pdf

[38] Falk, A., & Heckman, J. J. (2009). Lab experiments are a major source of knowledge in the social sciences. *science*, *326*(5952), 535-538.

[39] Forget, A., Chiasson, S., & Biddle, R. (2010, April). Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1107-1110). ACM.

[40] Fried, C. Privacy: A rational context. In Computers, Ethics, and Society; Ermann, M.D., Williams, M.B., Guiterrez, C., Eds.; Oxford University Press: New York, NY, USA, 1990

[41] Green, T. M., Ribarsky, W., & Fisher, B. (2008, October). Visual analytics for complex concepts using a human cognition model. In *Visual Analytics Science and Technology, 2008. VAST'08. IEEE Symposium on* (pp. 91-98). IEEE.

[42] Greenberg, S., Marquardt, N., Ballendat, T., Diaz-Marino, R., & Wang, M. (2011). Proxemic interactions: the new ubicomp?. *interactions*, 18(1), 42-50.

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

[44] Hall, Edward T. (October 1963). A System for the Notation of Proxemic Behavior. *American Anthropologist* 65 (5): 1003–1026.

[45] Hall, E. T. (1966). *The hidden dimension*. Garden City, NY: Anchor.

[46] Hansson, R., Ljungstrand, P., & Redström, J. (2001, January). Subtle and public notification cues for mobile devices. In *Ubicomp 2001: Ubiquitous Computing* (pp. 240-246). Springer Berlin Heidelberg.

[47] Harrison, C., & Dey, A. K. (2008, April). Lean and zoom: proximity-aware user interface and content magnification. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 507-510). ACM.

[48] Harrison, C., & Hudson, S. E. (2011, October). A new angle on cheap LCDs: making positive use of optical distortion. In *Proceedings of the 24th annual ACM symposium on User interface software and technology* (pp. 537-540). ACM.

[49] Hasegawa, S., Fujikake, K., Omori, M., & Miyao, M. (2008). Readability of characters on mobile phone liquid crystal displays. *International Journal of Occupational Safety and Ergonomics*, *14*(3), 293-304.

[50] Hasegawa, S., Omori, M., Matsunuma, S., & Miyao, M. (2006). Aging effects on the visibility of graphic text on mobile phones. *Gerontechnology*, *4*(4), 200-208.

[51] Hawkey, K., & Inkpen, K. M. (2007, May). PrivateBits: managing visual privacy in web browsers. In *Proceedings of Graphics Interface 2007* (pp. 215-223). ACM.

[52] Hofstede, G. (1980). Culture's consequences. Beverly Hills.

[53] Hudson, S. E., & Smith, I. (1996, November). Techniques for addressing fundamental privacy and disruption tradeoffs in awareness support systems. In *Proceedings of the 1996 ACM conference on Computer supported cooperative work* (pp. 248-257). ACM.

[54] Iachello, G., & Hong, J. (2007). End-user privacy in human-computer interaction. *Foundations and Trends in Human-Computer Interaction*, 1(1), 1-137.

[55] Iachello, G., Truong, K. N., Abowd, G. D., Hayes, G. R., & Stevens, M. (2006, April). Prototyping and sampling experience to evaluate ubiquitous computing privacy in the real world. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 1009-1018). ACM.

[56] Ishiguro, Y., & Rekimoto, J. (2011, March). Peripheral vision annotation: noninterference information presentation method for mobile augmented reality. In *Proceedings of the 2nd Augmented Human International Conference* (p. 8). ACM.

[57] José Ramón Padilla-López, Alexandros Andre Chaaraoui, Francisco Flórez-Revuelt. (2015).Visual privacy protection methods: A survey. In *Expert Systems with Applications*, 42(9), 4177-4195

[58] Kindberg, T., Sellen, A., & Geelhoed, E. (2004). Security and trust in mobile interactions: A study of users' perceptions and reasoning. In *UbiComp 2004: Ubiquitous Computing* (pp. 196-213). Springer Berlin Heidelberg.

[59] Kumar, M., Garfinkel, T., Boneh, D., & Winograd, T. (2007, July). Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 13-19). ACM.

[60] Kvavilashvili, L., & Ellis, J. (2004). Ecological validity and the real-life/laboratory controversy in memory research: A critical and historical review. *History & Philosophy of Psychology*, 6, 59-80.

[61] Langheinrich, M. (2001, January). Privacy by design—principles of privacy-aware ubiquitous systems. In *Ubicomp 2001: Ubiquitous Computing* (pp. 273-291). Springer Berlin Heidelberg.

[62] Lian, S., Hu, W., Song, X., & Liu, Z. (2013). Smart privacy-preserving screen based on multiple sensor fusion. *Consumer Electronics, IEEE Transactions on*, 59(1), 136-143.

[63] Lin, C. A., & Atkin, D. J. (Eds.). (2014). *Communication technology and social change: Theory and implications*. Routledge.

[64] Luff, P., & Heath, C. (1998, November). Mobility in collaboration. In *Proceedings of the 1998 ACM conference on Computer supported cooperative work* (pp. 305-314). ACM.

[65] McCrickard, D. S., Catrambone, R., Chewar, C. M., & Stasko, J. T. (2003). Establishing tradeoffs that leverage attention for utility: empirically evaluating information display in notification systems. *International Journal of Human-Computer Studies*, *58*(5), 547-582.

[66] Mitseva, A., Imine, M., & Prasad, N. R. (2006, September). Context-aware privacy protection with profile management. In Proceedings of the 4th international workshop on Wireless mobile applications and services on WLAN hotspots (pp. 53-62). ACM.

[67] Mohammed, N., Fung, B., Hung, P. C., & Lee, C. K. (2009, June). Anonymizing healthcare data: a case study on the blood transfusion service. In *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining* (pp. 1285-1294). ACM.

[68] Murphy, A., Reddy, M, & Xu, H. (2014). Privacy practices in collaborative environments: a study of emergency department staff. In *Proceedings of the 17th ACM conference on Computer supported cooperative work & social computing*.(pp.269-282).

[69] Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J., & Beznosov, K. (2013, August). 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* (pp. 271-280). ACM.

[70] Palen, L., & Dourish, P. (2003, April). Unpacking privacy for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 129-136). ACM.

[71] Patil, S., & Kobsa, A. (2009). Privacy considerations in awareness systems: designing with privacy in mind. In *Awareness Systems* (pp. 187-206). Springer London.

[72] Patrick A. (2007). Commentary on Research on New Security Indicators -essay. http://www.andrewpatrick.ca/essays/commentary-on-research-on-new-security-indicators.

[73] Patterson, M. L., Mullens, S., & Romano, J. (1971). Compensatory reactions to spatial intrusion. *Sociometry*, 114-121.

[74] Personal space. (n.d.). In *Wikipedia*. Retrieved on July 5, 2015 from https://en.wikipedia.org/wiki/Personal_space

[75] Pfitzmann, A., & Hansen, M. (2010). A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. Retrieved on November 12, 2013 from http://staging.kantarainitiative.org/confluence/download/attachments/45059055/terminology+for+talking+about+privacy.pdf

[76] Polhemus, Inc.(2013). G4 user manual. Retrieved on March 15, 2013 from http://polhemus.com/_assets/img/G4_User_Manual_URM10PH238-D.pdf.

[77] Polhemus, Inc. (2015). G4 system for web optimized, digital image. Retrieved on May 12, 2015 from http://polhemus.com/_assets/img/G4-System-For-Web-Optimized.jpg

[78] Portnoff, S.R., Lee, N.L., Egelman, S., Mishra, P., Leung, D., & Wagner, D. (2015, April) Somebody's watching me?: Assessing the effectiveness of Webcam indicator lights. In *Proceedings of the SIGCHI conference on Human factors in computing systems* (pp. 1649-1658). ACM.

[79] Preibusch, S. (2013). Guide to measuring privacy concern: Review of survey and observational instruments. *International Journal of Human-Computer Studies*, 71(12), 1133-1143.

[80] Probst, G. (2000). Analysis of the Effects of Privacy Filter Use on Horizontal Deviations in Posture of VDT Operators (Doctoral dissertation, Virginia Polytechnic Institute and State University).

[81] Project Tango. (n.d.). In *Wikipedia*. Retrieved on July 23, 2015 from http://en.wikipedia.org/wiki/Project_Tango

[82] Project Tango Depth Perception. (n.d.) In Google Developers. Retrieved on July 23, 2015 from https://developers.google.com/project-tango/overview/depth-perception

[83] Radke, K., Boyd, C., Nieto, J. G., & Buys, L. (2013, November). Who decides?: security and privacy in the wild. In *Proceedings of the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration* (pp. 27-36). ACM.

[84] Regus. (2014). Business people globally describe their ideal work environment. Retrieved from: press.regus.com/united-kingdom/download/60669/gbs11theidealworkplaceenvironmentreport_final.pdf.

[85] Romesburg, C. (2004). *Cluster analysis for researchers*. Lulu. com.

[86] Schechter, S. E., Dhamija, R., Ozment, A., & Fischer, I. (2007, May). The emperor's new security indicators. In *Security and Privacy*, 2007. SP'07. IEEE Symposium on (pp. 51-65). IEEE.

[87] Schmuckler, M. A. (2001). What is ecological validity? A dimensional analysis. *Infancy*, 2(4), 419-436.

[88] Schneier, B. (2011). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.

[89] Sotirakopoulos, A., Hawkey, K., & Beznosov, K. (2011, July). On the challenges in usable security lab studies: lessons learned from replicating a study on SSL warnings. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (p. 3). ACM.

[90] Tan, D. S., Keyani, P., & Czerwinski, M. (2005, November). Spy-resistant keyboard: more secure password entry on public touch screen displays. In *Proceedings of the 17th Australia conference on Computer-Human Interaction: Citizens Online: Considerations for Today and the Future* (pp. 1-10). (CHISIG) of Australia.

[91] Tarasewich, P., Campbell, C. S., Xia, T., & Dideles, M. (2003, January). Evaluation of visual notification cues for ubiquitous computing. In *UbiComp 2003: Ubiquitous Computing* (pp. 349-366). Springer Berlin Heidelberg.

[92] Tarasewich, P., Gong, J., & Conlan, R. (2006, April). Protecting private data in public. In *CHI'06 Extended Abstracts on Human Factors in Computing Systems* (pp. 1409-1414). ACM.

[93] Thirumalai, M. S. (1987). Silent talk: Nonverbal Communication. Volume 40 of CIIL (Central Institute of Indian Languages) occasional monographs series. Retrieved on July 5th, 2015 from: http://www.ciil-ebooks.net/html/silent/index.htm

[94] Thompson, H.H. (2010). Visual data breach risk assessment study. Retrieved from: http://solutions.3m.com/3MContentRetrievalAPI/BlobServlet?locale=en_US&lmd=1291398659000&assetId=1273672752407&assetType=MMM_Image&blobAttribute=ImageFile

[95] Triandis, H. C., Bontempo, R., Villareal, M. J., Asai, M., & Lucca, N. (1988). Individualism and collectivism: Cross-cultural perspectives on self-ingroup relationships. *Journal of personality and Social Psychology*, *54*(2), 323.

[96] Vaniea, K., Bauer, L., Cranor, L. F., & Reiter, M. K. (2012, July). Studying access-control usability in the lab: lessons learned from four studies. In *Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results* (pp. 31-40). ACM.

[97] Vigliensoni, G., & Wanderley, M. M. (2012, May). A quantitative comparison of position trackers for the development of a touch-less musical interface. In *Proceedings of the 12th International Conference on New Interfaces for Musical Expression (NIME 2012), Vancouver, Canada*.

[98] Visual Data Security White Paper. (2012). European visual data security. Retrieved on October 15, 2015 from http://www.visualdatasecurity.eu/wp-content/uploads/2012/07/Visual-Data-Security-White-Paper.pdf

[99] Ware, C. (2012). *Information visualization: perception for design*. Elsevier.

[100] Watson, O. M., & Graves, T. D. (1966). Quantitative Research in Proxemic Behavior. *American Anthropologist*, 68(4), 971-985.

[101] Westin, A.F. (1970) Privacy and freedom. New York: Atheneum.

[102] Wiedenbeck, S., Waters, J., Sobrado, L., & Birget, J. C. (2006, May). Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the working conference on Advanced visual interfaces* (pp. 177-184). ACM.

[103] Wogalter, M. S., Conzola, V. C., & Smith-Jackson, T. L. (2002). Research-based guidelines for warning design and evaluation. *Applied ergonomics*, *33*(3), 219-230.

[104] Xu, X., & McGorry, R. W. (2015). The validity of the first and second generation Microsoft Kinect™ for identifying joint center locations during static postures. *Applied ergonomics*, *49*, 47-54.

[105] Zhou, H., Ferreira, V., Alves, T.S., Hawkey, K., & Reilly, D. (2015, April). Somebody Is Peeking!: A Proximity and Privacy Aware Tablet Interface. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 1971-1976). ACM.

[106] Zhou, H., Ferreira, V., Alves, T. S., MacKay, B., Hawkey, K., & Reilly, D. (2015). Exploring Privacy Notification and Control Mechanisms for Proximity-Aware Tablets. *International Journal of Mobile Human Computer Interaction (IJMHCI)*, *7*(3), 1-19.

Appendix A – Informed Consent

DALHOUSIE UNIVERSITY
Inspiring Minds

Exploring proximity and privacy natural user interface

Principal Investigators: Huiyuan Zhou, Faculty of Computer Science
Thamara Alves , Faculty of Computer Science
Vinicius Ferreira, Faculty of Computer Science
Mohamad Salimian, Faculty of Computer Science
Khalid Tearo, Faculty of Computer Science
Dr. Derek Reilly, Faculty of Computer Science
Dr. Kirstie Hawkey, Faculty of Computer Science
Dr. Bonnie MacKay, Faculty of Computer Science

Contact Person: Huiyuan Zhou, Faculty of Computer Science, hzhou@cs.dal.ca

We invite you to take part in a research study being conducted by Huiyuan Zhou at Dalhousie University. Your participation in this study is voluntary and you may withdraw from the study at any time. Your academic (or employment) performance evaluation will not be affected by whether or not you participate. The study is described below. This description tells you about the risks, inconvenience, or discomfort which you might experience. Participating in the study might not benefit you, but we might learn things that will benefit others. You should discuss any questions you have about this study with Huiyuan Zhou.

The purpose of the study is to help us learn effectiveness and usability of various privacy-aware interface designs for use on tablet PC. You will be asked to participate in a 1.5 hour-long study where you will perform a set of tasks with different prototype designs displayed on the tablet and provide feedback regarding the usefulness of the design. In the first session, you will play a simple game on the tablet. In the second session, you will be given a financial scenario and perform information retrieval tasks. In the third session, you will collaborate with a partner and complete a financial task. After each task, you will be asked to evaluate the effectiveness of different prototype designs. You will be videotaped for the entire study.

You will be compensated $20 for participating in the study; you can withdraw from the study at any time without consequence. A researcher is always available over the study period by email or to meet in person to answer any questions you may have or address any problems that you may experience with the tasks.

Prior to meeting us for the study, you will be asked to fill in a background questionnaire online detailing your experience with using tablets which should take about 5 minutes. For the study, you will meet with investigators in the Student Union Building where you will first be given a general description of the type of tasks we want you to do during the study. After doing a set of tasks, you will fill in questionnaires asking you about your opinions of the task. At the end of the study, you will participate in short interview.

All personal and identifying data will be kept confidential. Anonymity of textual data will be preserved by using pseudonyms. All data collected in the video, questionnaires and interviews will use pseudonyms (e.g., an ID number) to ensure your confidentiality. The informed consent form and all research data will be kept in a secure location under confidentiality in accordance to University policy for 5 years post publication.

In the event that you have any difficulties with, or wish to voice concern about, any aspect of your participation in this study, you may contact Catherine Connors, Director, Office of Research Ethics Administration at Dalhousie University's Office of Human Research Ethics for assistance: phone: (902) 494-1462, email: Catherine.connors@dal.ca.

☐ "*I have read the explanation about this study. I have been given the opportunity to discuss it and my questions have been answered to my satisfaction. I understand that being video taped is necessary to participate in the study. I hereby consent to take part in the study. However, I understand that my participation is voluntary and that I am free to withdraw from the study at any time.*"

Participant	***Researcher***
Name: _____	Name: _____
Signature: _____	Signature: _____
Date: _____	***Date:*** _____

Please select one of the options below:

☐ "*I agree to let you directly quote any comments or statements made in any written reports without viewing the quotes prior to their use and I understand that the anonymity of textual data will be preserved by using pseudonyms.*"

Participant	***Researcher***
Name: _____	Name: _____
Signature: _____	Signature: _____
Date: _____	***Date:*** _____

Or

☐ *"I want to read direct quotes prior to their use in reports and I understand that the anonymity of textual data will be preserved by using pseudonyms."*
[if this option is chosen, please include a contact email address: _____]

Participant	***Researcher***
Name: _____	Name: _____
Signature: _____	Signature: _____
Date: _____	***Date:*** _____

If you are interested in seeing the results of this study, please check below and provide your email address. We will contact you with publication details that describe the results.

☐ *"I would like to be notified by email when results are available via a publication."*

[if this option is chosen, please include a contact email address: _____]

Appendix B – Demographic Questionnaire

1. Age: _____

2. Gender: ☐ Male ☐ Female

3. Faculty: _____

4. Level/Year: ☐ 1st Year Undergraduate ☐ 2nd Year Undergraduate
   ☐ 3rd Year Undergraduate ☐ 4th Year Undergraduate
   ☐ Graduate – Masters ☐ Graduate – PhD
   ☐ Other (e.g. faculty, staff, visiting student, please specify)
   _____

5. What brand and model tablet product do you use (If you have multiple tablets, list your primary tablet)?
   Brand & Model: _____ (e.g., iPad 2)

6. How long have you used a tablet?
   ☐ 0-6 months ☐ 7-12 months ☐ 12+ months

7. How often do you use tablets?

Very Infrequently (less than once per week)	**Infrequently** (1-2 times per week)	**Sometimes** (3-6 times a week)	**Frequently** (1-2 times per day)	**Very Frequently** (3 times per day or more)

8. How many hours a week together you spend using a tablet?
   Roughly _____ hours.

9. What is the time distribution of your tablet usage in the following contexts (note: the total should be 100%):
   Study _____% Work _____% Personal _____%

10. What are the top three locations in which you most often use your tablet, and what is your purpose for being at that location at that time?
    Location 1: _____ Purpose: _____
    Location 2: _____ Purpose: _____
    Location 3: _____ Purpose: _____

11. I would be concerned if somebody were to be viewing my tablet while I'm accessing the following information on the tablet:

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
Social network chat							
Email							
Calendar							
Work document							
Financial information							
Shopping information							
Photo Album							
Game Progress/Score							
Health Information							
Other: Please specify							

12. How often are you in the situation where others could potentially view the following information displayed on your tablet:

	Never	Rarely	Sometimes	Often	Always
Social network chat					
Email					
Calendar					
Work document					
Financial information					
Shopping information					
Photo Album					
Game Progress/Score					
Health Information					
Other: Please specify					

13. I would be concerned if somebody were to be viewing my tablet while I'm accessing the following information on the tablet:

	Strongly Disagree	Disagree	Somewhat Disagree	Neutral	Somewhat Agree	Agree	Strongly Agree
Family							
Close friends							
Colleagues							
Acquaintance							
Strangers							
Other: Please specify							

14. How often does each type of viewer potentially view your tablet display?

	Never	Rarely	Sometimes	Often	Always
Family					
Close friends					
Colleagues					
Acquaintance					
Strangers					
Other: Please specify					

15. How often do you work in groups (e.g., group work for school, for your job)?

N/A	**Very Infrequently** (less than twice per year)	**Infrequently** (3-5 times per year)	**Sometimes** (6-11 times a year)	**Frequently** (1-2 times per month)	**Very Frequently** (3 times per month or more)

16. On average, how often do you do the following sharing activities **face to face** with others using the following media:

	N/A	Very Infrequently (less than once per month)	Infrequently (once per month)	Sometimes (2-3 times per month)	Frequently (1-2 times per week)	Very Frequently (3 times per week or more)
Paper						
Phone						
Tablet						
Desktop Computer						
Large Screen Projection						
Whiteboard						
Other: Please specify						

17. Approximately**,** how often do you share what you consider as **private or sensitive data** in person on the following media:

	N/A	Very Infrequently (less than once per month)	Infrequently (1-3 times per month)	Sometimes (1-3 times per week)	Frequently (4-6 times per week)	Very Frequently (almost every day)
Paper						
Phone						
Tablet						
Desktop Computer						
Large Screen Projection						
Whiteboard						
Other: Please specify						

18. This study doesn't use your real financial data (e.g. what bank do you primarily bank with, bank card No. etc.). If this study were to use your real bank account to perform tasks, would you still be willing to participate? (The answer won't affect your eligibility to current study)

☐ Yes ☐ Hard to say ☐ No

Appendix C – Game Task Material (Flags, Total Number 99)

Appendix D – Post Session Questionnaire (Game)

Session: Game PID**:** ___ Start time: ___ End time:__ R1:___ R2: ____

Please circle the rating that best describes the statement:

As a player:

	Strongly Disagree			Neutral			Strongly Agree
I try to complete the game as quickly as possible.	1	2	3	4	5	6	7
I try to protect my tablet screen as much as I can.	1	2	3	4	5	6	7

Round 1: _____

	Strongly Disagree			Neutral			Strongly Agree
It was easy to tell if there is someone near me that might be able to see my screen.	1	2	3	4	5	6	7
It was easy to hide the information on the tablet from the other person.	1	2	3	4	5	6	7
It was easy to continue my work while preserving the information's privacy.	1	2	3	4	5	6	7
Overall I am satisfied with the system used in the task.	1	2	3	4	5	6	7

Round 2: _____

	Strongly Disagree			Neutral			Strongly Agree
It was easy to tell if there is someone near me that might be able to see my screen.	1	2	3	4	5	6	7
It was easy to hide the information on the tablet from the other person.	1	2	3	4	5	6	7
It was easy to continue my work while preserving the information's privacy.	1	2	3	4	5	6	7
Overall I am satisfied with the system used in the task.	1	2	3	4	5	6	7

Appendix E – Post Session Interview (Game)

Session: Game Participant ID**:** _____

As a Player:

Q: What's your strategy to manage privacy (if any)?

Q: Do you think the notification (if any) is useful? Why?

Q: Do you think the protection (if any) was useful? Why?

Q: Is there any difference between systems used in the two tasks? Which do you like better? Please explain.

Q: Any other comments?

As an observer:

	Strongly Disagree			Neutral			Strongly Agree
It was easy to see the player's screen in round 1.	1	2	3	4	5	6	7
It was easy to see the player's screen in round 2.	1	2	3	4	5	6	7

Q: How many flags did you actually see?

Q: How would you describe your observing experience? How effective is your observing strategy?

Q: How effective is your opponent's strategy to protect the information?

Q: Is there anything different between the two rounds you want to mention?

Q: How would your observing behavior have been different in real life scenario?

Appendix F – Post Session Questionnaire (Individual)

Session: indiv PID**:** ___ Start time: ___ End time:___ R1:____ R2: ____

Please circle the rating that best describes the statement:

General:	Strongly Disagree			Neutral			Strongly Agree
The tasks I performed was realistic.	1	2	3	4	5	6	7
I treated the role play similar to my own online banking behavior.	1	2	3	4	5	6	7
The tasks contains sensitive information.	1	2	3	4	5	6	7
I try to complete the task as quickly as possible.	1	2	3	4	5	6	7
I try to protect my tablet screen as much as I can.	1	2	3	4	5	6	7

Task 1: _____	Strongly Disagree			Neutral			Strongly Agree
It was easy to tell if there is someone near me that might be able to see my screen.	1	2	3	4	5	6	7
I feel confident that my information was well protected in the task.	1	2	3	4	5	6	7
It was easy to continue my work while preserving the information's privacy.	1	2	3	4	5	6	7
Overall I am satisfied with the system used in the task.	1	2	3	4	5	6	7

Task 2: _____	Strongly Disagree			Neutral			Strongly Agree
It was easy to tell if there is someone near me that might be able to see my screen.	1	2	3	4	5	6	7
I feel confident that my information was well protected in the task.	1	2	3	4	5	6	7
It was easy to continue my work while preserving the information's privacy.	1	2	3	4	5	6	7
Overall I am satisfied with the system used in the task.	1	2	3	4	5	6	7

Question: Compare two protection techniques (**dim** used in the game vs **mask** used in the bank task) in terms of your **preference**:

A. Dim B. Mask C. No preference

Question: Regardless of protection techniques, please rank the four combinations you've seen so far in terms of your **preference** to help manage privacy:

A. No notification + No protection
B. With notification + No protection
C. No notification + With protection
D. With notification + With protection

(e.g., ABCD means you like A >B > C > D) _____

Appendix G – Post Session Interview (Individual)

Session: individual PID: ___

1. In this two tasks, which system could better support your banking task? ____ or _____ ? (task conditions: NN, YN, NY, or YY, based on their answers to the questionnaire) Why?
2. Could you explain why your prefer _____ over _____? (protection techniques: dim &mask, based on their answers to the questionnaire) What are the strengths and weaknesses of each? [If the participant didn't experience mask, then show them on the tablet]?
3. Could you explain why you rank the four systems in _____ order? (privacy model: NN, YN, NY, YY) What are the strengths and weaknesses of each?
4. Think about your own online banking scenario. Which part of the task in the study was natural to you, which was different (e.g., time, location, bank account…)?
5. Did you try to protect Casey/Jessie's bank information in the tasks? (If yes) what did you do? (If no) why not? Did you treat the role play any differently from your own experience (that you would have done something differently in real life)? Please explain how.

Appendix H – Post Session Questionnaire (Collaborative)

Session: Colla PID**:** _ Start time: ___ End time:__ R1:__ R2:__ R3:___

Please circle the rating that best describes the statement:

General:	Strongly Disagree			Neutral			Strongly Agree
The task I performed was realistic.	1	2	3	4	5	6	7
I treated the role play similar to my own online banking behavior.	1	2	3	4	5	6	7
This task contains sensitive information.	1	2	3	4	5	6	7
I try to complete the task as quickly as possible.	1	2	3	4	5	6	7
I try to protect my tablet screen as much as I can.	1	2	3	4	5	6	7

Task 1_____:	Strongly Disagree			Neutral			Strongly Agree
It was easy to tell if there is someone near me that might be able to see my screen.	1	2	3	4	5	6	7
I feel confident that our information was well protected in the task.	1	2	3	4	5	6	7
It was easy to share the tablet with my partner while preserving the information's privacy.	1	2	3	4	5	6	7
Overall I am satisfied with the system used in the task.	1	2	3	4	5	6	7

Task 2: _____:	Strongly Disagree			Neutral			Strongly Agree
It was easy to tell if there is someone near me that might be able to see my screen.	1	2	3	4	5	6	7
I feel confident that our information was well protected in the task.	1	2	3	4	5	6	7
It was easy to share the tablet with my partner while preserving the information's privacy.	1	2	3	4	5	6	7
Overall I am satisfied with the system used in the task.	1	2	3	4	5	6	7

Task 3: _____:	Strongly Disagree			Neutral			Strongly Agree
It was easy to tell if there is someone near me that might be able to see my screen.	1	2	3	4	5	6	7
I feel confident that our information was well protected in the task.	1	2	3	4	5	6	7
It was easy to share the tablet with my partner while preserving the information's privacy.	1	2	3	4	5	6	7
Overall I am satisfied with the system used in the task.	1	2	3	4	5	6	7

Question: please rank the four combinations for **collaborative task** in terms of your **preference** to help manage privacy (you actually experienced **three** of them):

A. No notification + No protection
B. With notification + No protection
C. No notification + With protection
D. With notification + With protection

(e.g., ABCD means you like A >B > C > D) _____

Appendix I – Post Session Interview (Collaborative)

Session: Collaborative PID**:** ___

1. Is this splitting bill scenario realistic to you? Which part of the task in the study was natural to you, which was different (e.g., time, partner, location, procedure…)?
2. Did you try to protect Casey/Jessie's bank information while performing the tasks? (If yes) what did you do? What are your collaborative strategies to manage privacy? (If no) why not? Did you treat the role play any differently from your own experience (that you would have done something differently in real life)? Please explain how.
3. In this three tasks, which system could better support your collaborative (splitting bill) task? ___, ____, or ___Why?
4. **C**ould you explain why you rank the four systems in _____ order? (privacy model: NN, YN, NY, YY) Comparing to previous individual banking task, does your preference (notification, protection technique, privacy model etc.) change in this collaborative scenario? Why?
5. In this scenario, we used Dim protection technique. What if we use mask? Will the experience change? Which one do you prefer? Why?

Appendix J – Observer Recording Sheet (Individual session)

Session: Indiv Participant ID**:** _____ R1:_____ R2: _____

As an observer:

	Strongly Disagree			Neutral			Strongly Agree
It was easy to see the player's screen in round 1.	1	2	3	4	5	6	7
It was easy to see the player's screen in round 2.	1	2	3	4	5	6	7

Observation (player behavior, observing experience, special things worth mentioning):

Round1:_____

_____

_____

Round 2:_____

_____

_____

Session: Indiv Participant ID**:** _____ R1:_____ R2: _____

As an observer:

	Strongly Disagree			Neutral			Strongly Agree
It was easy to see the player's screen in round 1.	1	2	3	4	5	6	7
It was easy to see the player's screen in round 2.	1	2	3	4	5	6	7

Observation (identified info, observing experience, special things worth mentioning):

Round1:_____

_____

_____

Round 2:_____

_____

_____

Appendix K – Observer Recording Sheet (Collaborative session)

Session: colla Participant ID**:** _____ R1:____ R2: _____ R3: ____

As an observer:

	Strongly Disagree			Neutral			Strongly Agree
It was easy to see the player's screen in round 1.	1	2	3	4	5	6	7
It was easy to see the player's screen in round 2.	1	2	3	4	5	6	7
It was easy to see the player's screen in round 3.	1	2	3	4	5	6	7

Observation (player behavior, observing experience, special things worth mentioning):

Round1:_____

_____

Round2:_____

_____

Round3:_____

_____

Collaboration Observation:_____

_____

_____

Appendix L – Post-Study Interview

Notification and Privacy control (model)

1. What are the physical ways that you protect tablet screen privacy in public (if any)? What are the other ways you used/heard of to protect tablet privacy? (hardware, software)
2. Given the physical ways (sense) to be aware of potential privacy intrusion, will the notification still be useful? In what situation/scenario?
3. Given the physical ways to manage privacy (turn off the screen, reorient the device), will the protection techniques still be useful? In what situation/scenario?
4. Do you prefer having both notification and protection or having just one of them is enough? Why? In what situation?
5. Considering the four different models (NN, NY, YN, YY), to best support your work (keeping information private while allowing you continue work), should the system be designed differently with individual vs collaborative task? Why or why not? Or you have a different idea about how the system should work?

Reflection on what haven't been tested

1. In the study, when there is no notification, the protection was turned on automatically. What if you could turn it on manually? Is there one you like or don't like? Why?
2. In the study, when there is notification, the protection was turned on manually. What if it was turned on automatically? Is there one you like or don't like? Why?
3. Selective hiding: this technique selectively anonymize sensitive pictures, names, numbers etc. once triggered. What's its strength, weaknesses and potential usage scenario?

General improvement:

1. If you were to use this system to protect your privacy, how are you going to use it? (when, where, what)
2. If you were to use this system to protect your privacy, will you have any concerns?
3. Could you think of other scenarios (other tasks, locations, users, other aggressors) that these systems might be useful (individual vs collaborative)? How?
4. Do you have any suggestion for improving the notification/privacy protection mechanism?
5. Do you have any suggestion for how the system might support individual versus collaborative private work?
6. Is there anything you want to add to/remove from the current system?
7. Do you have any other comments?

Appendix M – Participant Payment Receipt

Participant Payment Receipt

My signature below confirms that I received a sum of $20 (CDN) cash from Huiyuan Zhou as an honorarium payment for participating in the "Exploring proximity and privacy natural user interface" research project.

I understand this honorarium is taxable income and it is my responsibility to claim it on my income tax as Dalhousie University will not be issuing a T4A for this payment.

Name (please print): _____

Signature: _____

Date: _____

Participant Payment Receipt

My signature below confirms that I received a sum of $21 (CDN) cash from Huiyuan Zhou as an honorarium payment for participating in the "Exploring proximity and privacy natural user interface" research project.

I understand this honorarium is taxable income and it is my responsibility to claim it on my income tax as Dalhousie University will not be issuing a T4A for this payment.

Name (please print): _____

Signature: _____

Date: _____

Appendix N – Social Sciences & Humanities Research Ethics Board Letter of Approval

Social Sciences & Humanities Research Ethics Board
Letter of Approval

June 19, 2014

Ms Huiyuan Zhou
Computer Science\Computer Science

Dear Huiyuan,

REB #: 2014-3249
Project Title: Exploring Proximity and Privacy Natural User Interface

Effective Date: June 19, 2014
Expiry Date: June 19, 2015

The Social Sciences & Humanities Research Ethics Board has reviewed your application for research involving humans and found the proposed research to be in accordance with the Tri-Council Policy Statement on Ethical Conduct for Research Involving Humans. This approval will be in effect for 12 months as indicated above. This approval is subject to the conditions listed below which constitute your on-going responsibilities with respect to the ethical conduct of this research.

Sincerely,

Dr. Sophie Jacques, Chair