Designing Privacy-Enhanced Interfaces on Digital Tabletops for Public Settings

by

Arezoo Irannejad

A thesis

presented to the University of Waterloo

in fulfillment of the

thesis requirement for the degree of

Master of Applied Science

in

Management Sciences

Waterloo, Ontario, Canada, 2013

AUTHOR'S DECLARATION

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Arezoo Irannejad

The University of Waterloo

January 2013

Abstract

Protection of personal information has become a critical issue in the digital world. Many companies and service provider websites have adopted privacy policies and practices to protect users' personal information to some extent. In addition, various governments are adopting privacy protection legislation. System developers, service providers, and interface designers play an important role in determining how to make systems fulfill legal requirements and satisfy users. The human factor requirements for effective privacy interface design can be categorized into four groups: (1) comprehension, (2) consciousness, (3) control, and (4) consent (Patrick & Kenny, 2003).

Moreover, the type of technology that people are engaged with has a crucial role in determining what type of practices should be adopted. As Weiser (1996) envisioned, we are now in an "ubiquitous computing" (Ubicomp) era in which technologies such as digital tabletops (what Weiser called LiveBoards) are emerging for use in public settings. The collaborative and open nature of this type of smart device introduces new privacy threats that have not yet been thoroughly investigated and as a result have not been addressed in companies' and governmental privacy statements and legislation.

In this thesis, I provide an analytical description of the privacy threats unique to tabletop display environments. I then present several design suggestions for a tabletop display interface that addresses and mitigates these threats, followed by a qualitative evaluation of these designs based on Patrick and Kenny's (2003) model. Results show that most

participants have often experienced being shoulder-surfed or had privacy issues when sharing information with someone in a collaborative environment. Therefore, they found most of the techniques designed in this thesis helpful in providing information privacy for them when they are engaged with online social activities on digital tabletops in public settings. Among all of the proposed tested designs, the first three have proven to be effective in providing the required privacy. However, designs 4 and 5 had some shortfalls that made them less helpful for participants. The main problem with these two designs was that participants had difficulty understanding what they had to do in order to complete the given tasks.

Acknowledgments

I would like to thank my supervisors Mark Hancock and Efrim Boritz for their guidance. I also thank my readers Darren Charters and Vanessa Bohns for their feedback on my work and for posing challenging questions that helped to strengthen my contributions.

Thanks also go to Zachary Cook for his help in designing the application for my study, Jim Romahn for carefully proofreading my thesis, and members of Touchlab and Collaborative Systems Laboratory for their feedback and helpful comments.

I would also like to thank my family for their support and encouragement that helped me to get through this path.

Arezoo Irannejad

The University of Waterloo

January 2013

Table of Contents

List of Figures

List of Tables

Chapter 1. Introduction

Back in 1996, Weiser and Brown (1996) discussed major trends in computing (Figure 1.1). They argued, “The important waves of technological change are those that fundamentally alter the place of technology in our lives. What matters is not technology itself, but its relationship to us (Page 1).” They predicted embedded microscopic computers in walls, chairs, clothing and many other places in our lives to the extent that we can call it “calm technology” (Weiser & Brown, 1996) meaning that things around us are informing without overburdening and recede into the background of our lives (Weiser & Brown, 1996)

Weiser and Brown’s era of ubiquitous computing has largely already been realized. Weiser proposed three forms of ubiquitous smart devices: tabs, pads and boards (Weiser, 2002). Tabs are wearable centimeter-sized devices and Pads are decimeter-sized devices we already see everywhere from iPads and iPhones to Personal Digital Assistants (PDAs). The third type is an emerging popular meter-sized interactive display device Weiser called *Live Board*. *Live board* or what is referred to as a digital table or tabletop display nowadays is the focus of this thesis and my investigation of privacy.

Nowadays people widely use smartphones and personal computers but they are not able to easily connect to each other or collaborate. As thoroughly discussed in Section 3.1, there are a lot of situations where it is useful to use digital tables instead of private devices such as smartphones. Digital tables are a promising new medium for the support of collaborative

work. Instead of individuals working independently on their own devices or workstations, people can collaborate across a shared display through touch and gesture-based interaction while maintaining eye contact and engaging in conversation. Additionally, tabletop displays offer many new possibilities for attracting the attention of passers-by in a public setting, such as museums or malls, due to their large size and their ability to support many people surrounding the same space.

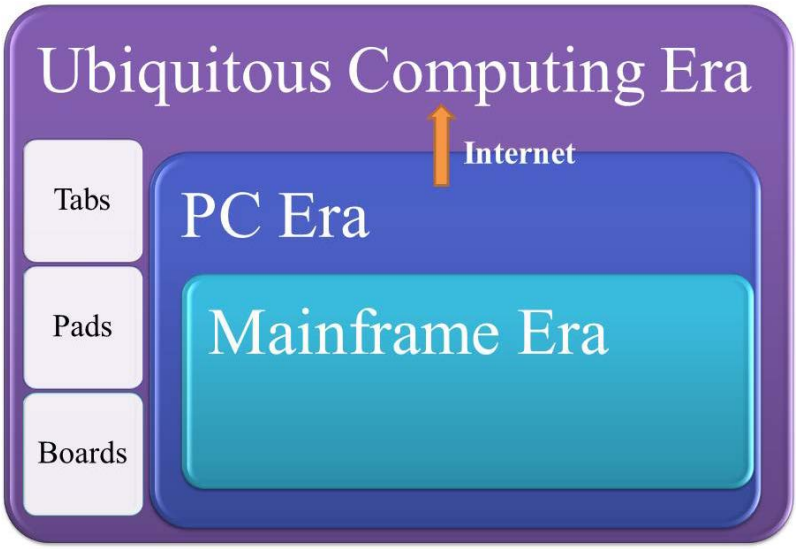


Figure 1.1 Weiser et al. (1996) Analysis of Computing Trends

However, while these devices offer the promise of new styles of interaction, they also introduce many potential threats to privacy. When collaborating around a table in a public place, a stranger walking by might be able to see what a person is typing in or entering into their device (shoulder-surfing) or one group could finish using the table and walk away, but

forget to log off or otherwise secure the machine so that another person can use or view their personal data. Additionally, within a group it may also be difficult to share information without unintentionally revealing other personal data. For instance, if one group member opens a message in Facebook, they may inadvertently show their group members other messages or personal information while navigating to that message.

To investigate privacy issues unique to the use of digital tables in a public setting, and to help privacy legislation compliance surrounding this new technology, I designed and evaluated a social networking application for use in a public space and explored associated threats of the application's interface design using an existing framework for designing software applications to support privacy. The framework comprises four core concepts: Comprehension, Consciousness, Control, and Consent.

An online social network (OSN) is chosen as an example application to test privacy concerns on a digital tabletop because online social networks' privacy practices[1] have always been controversial. Not only do they sometimes breach industry standards and government regulations but they also often violate their own privacy policies (Steel & Vascellaro, 2010). According to polls (Steel & Vascellaro, 2010); (Lippman, 2010), people are very concerned

[1] There is an important difference between privacy practices and policies; a privacy policy is a statement that companies put in their websites or application information page for users to read about how their personal information is being collected, used and disclosed. However, this does not mean the company has privacy practices in place that comply with the stated policies. One way to address this problem is trusted third-party involvement that assures the privacy practices of the company comply with their privacy policies (Boritz, No, & Sundarraj, August 25-27, 2009).

about the privacy of their information and potential cybercrimes that threaten them and their children. Over time, regulatory actions and privacy frameworks have emerged from legal cases and complaints to address people's concerns. There are regulations in different countries, such as Canada and the United States, that regulate the information rights of children under 13 (OECD, PIPEDA, FTC's FIP), as well as the flow of trans-border information. However, the existing legislation does not include new privacy concerns emerging with the use of new technologies such as digital tabletops.

The focus of this research is on anticipated privacy threats associated with using Facebook as an information-sharing website on digital tabletops in public settings. Before choosing Facebook, different information sharing websites such as Twitter, Google+, and LinkedIn were considered for this research. Facebook was chosen not only for being the most commonly used online social network, but also for being more aligned with the purpose of this research. Facebook offers a wider range of features for sharing various types of information such as photos, messages, links, and videos, compared to alternative social networks. For example, LinkedIn is limited to career-related information and Twitter is mostly used to share thoughts and quotes. Nevertheless, future research can consider and compare these and other existing websites.

I then present several design ideas based on the four elements of comprehension, consciousness, control and consent that comply with already-existing laws and regulations to better protect people's privacy. I then present the results of a qualitative study in which I validate the effectiveness of these interface designs with respect to these four elements.

It is also notable that, in this study, I neither rely on the fact that these concepts have equal importance, nor on the fact that one is more important than the other in addressing privacy issues. It may be true that one has more importance than others in improving people's information-privacy needs, but further research is needed to validate this hypothesis.

1.1 Motivation

In this thesis I examine how the interface of information-sharing websites used on digital tabletops in public settings can be designed to mitigate and address unique privacy threats. There are two primary motivations:

1. Various governments are adopting privacy protection legislation to address different aspects of personal information usage. There are different protective guidelines in well-known privacy frameworks regarding dealing with children under 13 or trans-border flows of personal data, but less attention has been paid to new emerging technologies and their potential for privacy invasion; for example, new technologies such as digital tabletop displays in public settings and social networking applications used in conjunction with such devices.
2. A significant element in the consideration of privacy threats is the mechanisms through which people can interact with their personal data. When people are provided with new technology for sharing and working with their own data in a public setting, many privacy issues can be addressed through the appropriate design of an interface. Many researchers have explored new technologies for interaction, as well as

interaction techniques that can provide faster, easier manipulation of digital artifacts; however, it is an open research question whether and how an interface can be designed to provide people with the ability to share their personal information in a safe, controlled, and comfortable way.

There has been little to no research addressing the above-mentioned issues. This thesis suggests interface designs that can be used on digital tabletops in public settings to enhance the actual and perceived privacy of personal information and to bring important considerations to policy makers' attention to enable digital tabletops to become available to and to be used safely by everyone.

1.2 Scope

The data that feeds this research consists of two main parts. One is related to the privacy domain with regard to collection, use, and disclosure of personal information, including privacy frameworks and the privacy policy of Facebook as the information-sharing website used in this research project. By comparing privacy frameworks with Facebook's privacy policy, some privacy gaps will be identified and addressed by the proposed interface design models.

The other source used in this thesis is a body of literature on collaborative and co-located tasks on interactive displays in public settings from the domain of human-computer interaction. The collaborative and open nature of digital surfaces makes them more prone to

privacy invasions. These possibilities along with characteristics of these surfaces will be examined and new privacy threats will be identified. Then privacy-enhancing design considerations will be introduced, followed by suggested design models. Figure 1.2 depicts a summary of the thesis workflow and how each section contributes to the thesis.

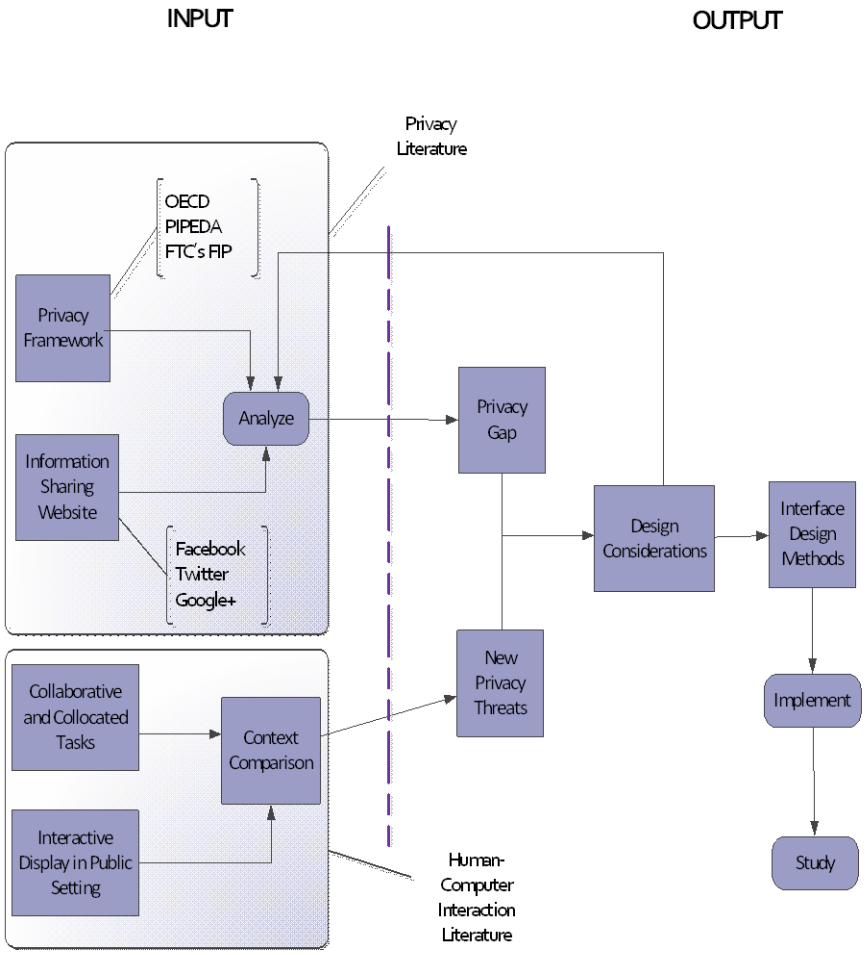


Figure 1. 2 Thesis workflow

1.3 Open Research Problems

Privacy policy and related threats have been addressed in different domains such as e-commerce and business-marketing (Boritz, No, & Sundarraj, August 25-27, 2009); (Charters, 2002) and even online social networks with respect to privacy breaches that have been controversial lately (Bardeesy, 2009); (Steel & Vascellaro, 2010). In the human-computer interaction domain, many researchers have worked on how they can technically (through hardware or software) address security issues on digital tabletops (De Luca & Frauendienst, 2008); (Hagen & Eika Sandnes, 2001). However, no research has been done from the human factors point of view, and on the elements that should be considered when designing a system to protect personal information privacy.

This research is different form other research, first because it is focused on digital tabletops and particularly information-sharing applications and bridges work between the human-computer interaction and privacy policy domains.

1.4 Contributions

The main contribution of this thesis is to support the design of online social networks for digital tables in public places that have an improved level of privacy. I make the following specific contributions:

- A better understanding of the privacy threats unique to online social networks on a digital tabletop in a public setting

- A description of how to embed privacy requirements into the design of digital tabletop systems through a set of interface designs
- The implementation of a set of privacy-improved designs for digital tabletops in public settings
- The results of a study evaluating the effectiveness of the designs in improving comprehension, consciousness, control and consent.

1.5 Thesis Outline

Chapter 1 presents the motivation and research objectives. Chapter 2 reviews previously-published literature on digital tabletops, privacy, and work that addresses privacy issues when using digital tabletops in public settings. Following that, Chapter 3 compares statements from Facebook's privacy policy with principles of privacy frameworks from the literature and identifies potential threats in both traditional desktop environments, and those unique to tabletop settings in co-located and public environments. The threats are communicated through different scenarios.

Chapter 4 describes some interface design ideas for improving user-interface compliance with privacy legislations along with pros and cons of each idea, based on the analysis of threats from Chapter 3. Then, Chapter 5 presents the results of an informal laboratory study in which the proposed interface design ideas were evaluated to better understand the strengths and weaknesses of the designs presented in Chapter 4. Finally, the research objectives that are met, concluding remarks, and recommendations for future work are discussed in Chapter 6.

Chapter 2. Related Literature

This research bridges two primary domains of active research: human-computer interaction (HCI) and privacy policy legislation. More specifically, the research focuses primarily on the subdomain of tabletop display interaction within HCI and legislation specific to information-sharing applications. Before getting into how privacy principles can be embedded in the design of information-sharing systems for digital tabletops to ensure fair information collection, use, and disclosure, we need to know what digital tabletops are, what privacy is, and how privacy differs when we are using a digital tabletop in a public setting.

Therefore, this chapter provides an overview of the literature relevant to understanding the above-mentioned domains. The background presented here is divided into three main categories. First is an overview of different kinds and characteristics of digital tabletops as an emerging technology. This is followed by a discussion of privacy definitions and different privacy frameworks. Finally, examples of privacy issues unique to digital tabletops addressed by other researchers are discussed and core elements of a privacy-enhanced design are introduced.

2.1 Digital Tabletops

Digital tabletops are interactive horizontal digital displays that enable multi-touch interaction with digital information and media for one or multiple users. Scott et al. (2003) classified four general types of digital tabletops as follows:

1) Digital Desks which are intended to integrate digital media with traditional desks.
2) Workbenches that are top-projected virtual reality environments. Some characteristics that distinguish a workbench from other virtual reality environments such as CAVEs are its flat and limited-size display.
3) Drafting tables are meant to replace an artist's or drafter's table which has an angled surface and are usually used by one person at a time.
4) Collaboration tables are horizontal computer displays with an interactive touch-sensitive area that serves as the surface of the table and are intended for use by several people at the same time. They allow people to interact with them directly by touching, gesturing, etc. or indirectly with input devices such as a mouse, keyboard, etc. and are applicable for group collaborations in educational settings, workplaces or public places by providing a shared environment[2]. They are also a blend of the traditional with the modern, allowing the power of today's computer systems to be combined with the natural environment of a physical table, along with all of the intuitive understanding of face-to-face communication and collaborative strategies that accompany such an environment (Scott, T. Carpendale, & Inkpen, 2004).

In this thesis, I direct my attention to digital tabletops as collaboration tables (category 4) (Figure 2.1). The reason for this choice is that among the categories above, collaboration

[2] Shared environment is a technical term applied to any system or device that has an environment where people can work on it together either collaboratively or separately.

tables are the most suitable for collaboration activities, especially in public settings, because of their big display size, horizontal surface, and touch screen.

Figure 2.1 Digital tabletop (Collaboration table)

In spite of the fact that digital tabletops offer several advantages for collaborative work, they have some technical barriers. For example, a picture that was right side up may be up-side down for other users standing in the other side of the table. Several researchers worked on different mechanisms to overcome these barriers. Hancock et al. (2006) identified five different rotation and translation mechanisms, investigated which ones are more suitable for digital tabletops and discussed the tradeoffs between using any of the techniques. Parker et al. (2006) investigated different interaction methods on digital tabletops including fingers,

stylus, mouse, trackballs, and tangible artifacts and introduced a novel interaction technique called TractorBeam. This technique enables users to interact with closer objects as well as selecting distant targets by seamlessly switching between these interaction methods.

Moreover, there are also several non-technical barriers as well. When working in collaborative environments, there are often times when accessing personal or private information is required; this is also true for working on a digital tabletop. For example, when in a collaborative group an email or message needs to be accessed to show to the group, the user might not be comfortable revealing other information in that email, such as the name of the sender or a portion of the message. Therefore, there are some information privacy considerations specific to digital tabletops that will be discussed in more detail in Section 2.3.

2.2 Privacy

Before discussing privacy concerns specific to digital tabletop environments, it is useful to consider privacy frameworks in general. Privacy has different meanings in different domains. One of the very first privacy definitions was provided by Judge Louis Brandeis in 1890 which stated that privacy is "the right to be let alone" (Brandeis & Warren, 1890). There are many other definitions such as:

"Privacy is the ability of an individual or group to seclude them or information about themselves and thereby reveal them selectively. Privacy is sometimes related to anonymity, the wish to remain unnoticed or unidentified in the public realm" (Wikiquote). "A capability to determine what one wants to reveal and how accessible one wants to be" (Belloti, 1997)

"The selective control of access to the self" (Altman, 1975). "The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967). However, the following is the closest definition of privacy to the context of this thesis and also to the spirit of the privacy legislation used in this research:

> **"Privacy** is the right of an individual to determine to what degree he or she is willing to disclose personal or other information about him- or herself. When such information is provided to other entities, individuals, or organizations, this right extends to the collection, distribution, and storage of that information (Boritz, No, & Sundarraj, August 25-27, 2009)."

Governments of some countries (e.g., European Union, Canada, Australia, and Switzerland) have adopted privacy protection laws that are imposed through governmental bodies with supervisory powers. However, they are more focused on sensitive sectors such as health care and financial services, unless there is an extreme breach of privacy such as RealNetworks (Macavinta, 1999), DoubleClick (Charters, 2002), ChoicePoint (Kane & Hines, 2005), and most importantly, online social networks such as Facebook, whose privacy practices have always been controversial. Not only do they often breach industry standards and government regulations, but they also often violate their own privacy policies (Bardeesy, 2009).

According to polls (Steel & Vascellaro, 2010); (Lippman, 2010), people are concerned about the privacy of their information and potential cybercrimes that threaten them and their children. Because of such concerns, some governments (including the Canadian government), monitor the privacy policies and practices of controversial non-public bodies to make sure they comply with privacy regulations (e.g., PIPEDA). However, in spite of all the governmental supervision, there has been little guidance made available to designers and programmers on how to implement such systems[3].

As will be discussed in the next section, some prior research has investigated privacy issues associated with OSNs and the methods to be used to minimize threats in such contexts (Gross & Acquisti, 2005); (Stutzman & Kramer-Duffield, 2010), but there has been virtually no research on privacy risks associated with using OSNs on digital tabletops in public settings and how to address them by embedding the privacy requirements into the design of the system. This research is an attempt to address the existing gap and focuses on the use of Facebook as an online social network on a digital tabletop in public settings and the privacy threats associated with this environment.

2.2.1 Privacy Frameworks

To be able to embed the privacy requirements into the interface design of the system, it is necessary to identify and understand the privacy principles that are essential to privacy frameworks and that will be used to evaluate compliance by a particular system. Most of the

[3] Recently Ontario's privacy commissioner initiated "Privacy by Design" as a philosophy of embedding privacy into the design of the technology (http://privacybydesign.ca/).

principles of privacy frameworks are abstracted from legal complaints and codes (Patrick & Kenny, 2003), and are designed to govern the collection, use and disclosure of personal data. Personal data (AKA Personally Identifiable Information, or PII) can be any data that either directly or indirectly through combination with other data identify an individual. Privacy frameworks distinguish the requirements and responsibilities of a "Data Controller" who is knowledgeable to decide about the contents and use of personal data and a "Data Processor" who can be an entity inside the organization responsible for all or part of processing activities or a separate legal entity processing personal data on behalf of the Data Controller.

There are different privacy frameworks, some of which are for particular countries or are focused on a special aspect of privacy principles. In this section, I describe the three privacy frameworks (OECD, PIPEDA, and FTC's FIP) that were used as a basis for analysis in this thesis (see Appendix I for a full description of each). Their principles are later mapped with the core concepts of privacy-enhanced design (Section 2.3). Also there is a full analysis of Facebook's privacy policy mapped to the privacy principles of all of these frameworks in Appendix II.

OECD Privacy Framework

The OECD privacy principles (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) were developed in the 1970s by the Organization for Economic Co-operation and development (OECD) (Development, Organization for Economic Co-operation and Development, 2012). OECD is an organization officially launched in September 1961, and is committed to democracy and market economy. "The

Organization provides a setting where governments compare policy experiences, seek answers to common problems, identify good practices and coordinate domestic and international policies (Development, OECD Privacy Principles, 2010).” OECD Privacy Principles form an internationally and commonly-used privacy framework. The OECD guidelines are a global benchmark for privacy protection and serve as the basis of many other privacy practice programs and frameworks, as well as being a recommended model for privacy legislation in many countries (Boritz, No, & Sundarraj, August 25-27, 2009).

A list of eight OECD Privacy Principles and guidelines that should be regarded as minimum standards and are complementary to other measures to protect personal information privacy and individual liberties (OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data) can be found in Appendix I.

PIPEDA Privacy Framework

The *Personal Information Protection and Electronic Document Act* (PIPEDA) incorporates the key elements of the privacy code of the Canadian Standards Association (CSA). PIPEDA governs private-sector organizations such as charities, corporations, and partnerships, including online businesses. It also includes provisions for electronic document use. PIPEDA is a law that gives individuals control over how their personal information is handled in the private sector. Personal information is information that can be related to an identifiable individual, or can be used to directly or indirectly identify an individual (Boritz & No, 2011).

The law consists of 10 principles of fair information practices that are the essentials for the collection, use and disclosure of personal information (Incorporation, 2001). PIPEDA’s

10 privacy principles are defined in the section "Model Code for the Protection of Personal Information" of the PIPEDA Act (Department of Justice, 2012) and can be found in Appendix I.

FTC Privacy Framework

The United States Federal Trade Commission (FTC) was created in 1914 to protect customers against fraud, deception and unfair business practices, to maintain fair competition in the marketplace, and to ultimately advance its performance in organizations. The FTC prepared and collected a set of documents, reports, and guidelines regarding the best practices to collect, use, and disclose personal information. The core principles to all these documents are five main privacy protection principles (Fair Information Practices or FIP) (See Appendix I).

The FTC recently expanded its final privacy report and added some amendments including "Privacy by Design" (Cavoukian, 2012) . It explains that companies should think about and include customers' privacy in every stage of building a system or product (Federal Trade Commission, 2012).

While there has been significant work in the domain of privacy policy legislation, there has also been some work in the domain of HCI that addresses or discusses privacy issues. In the next section, previous research that explores the issue—i.e. privacy specifically on digital tabletops—is discussed and then an analysis of the above privacy frameworks is integrated with these HCI considerations.

2.3 Digital Tabletops and Privacy

One appeal of digital tabletops is the social dimension; they enable interaction among and between people by having an open and collaborative interactive surface. However, interaction between people that is mediated by technology is prone to both intentional and unintentional invasions of privacy. With the emerging popularity of the digital tabletop and public display devices (Patrick and Kenny, 2003), it is becoming more critical to provide a method to protect private information from being seen by the other people at the table. There are many different types of information that may appear on a tabletop, ranging from personal sites on the Internet, to passwords and pin codes involving different levels of concern about privacy. Each of these levels may require different types of privacy protection. In this section I provide the context from the related work on different techniques and technologies that address privacy issues on digital tabletops to identify necessary vocabulary and to also position my research in the context of the significant amount of related work:

Hardware-based Technologies

Some researchers have already developed hardware-based technologies to hide or show information to individuals for supporting people's privacy in a co-located collaborative setting. For example, Chan et al. (2008) developed a privacy-enhanced digital tabletop composed of two types of displays, the table surface and a virtual panel. The virtual panel is created by a special optical mechanism that offers privacy, in that it can only be viewed by

those within a limited range of the viewing angle. In this scenario, when the virtual panel is placed correctly, other viewers behind or next to the desired viewer, will only view a partial, distorted or blind view of the content being displayed. In their study, they gave the example of a poker application, which requires that each player can see only their own cards.

Scott et al. (2003) suggested some guidelines that technology should support for tabletops. One of the guidelines is to support transitions between personal and group work. In this case, they have suggested that separate personal displays may be used, but also caution that separate devices often hinder interpersonal interaction.

Skinput (Harrison, Tan, & Morris, 2010) was developed as a method to use the human body as an input device. The device is a wearable bio-acoustic sensing array that was built into an armband. One appeal of this technology is that the body has roughly two square meters of external surface area, and the other is that most of it is easily accessible by our hands. In their experiment, they attached the Skinput device to the arms of the participants and displayed the images on their forearms and palms. The users then used their other hands to push the buttons on their skin, resulting in data input. This technology would be very helpful when working at a digital tabletop unit and entering a password is required. If the hand or leg is used as the input device, it can be well protected and shielded from the eyes of other participants at the table.

Software-based Technologies

Another category is software-based techniques that allow people to protect their information. Apted and Kay (2006) describe their experience with Cruiser, a multi-user, gestural collaborative digital media to share media such as photos on a tabletop. They had a specific mode that allowed *personal space*, where objects are colored triangular elements that are drawn on the display to illustrate an area exclusive to each user. While in this mode, other users are not able to access or make changes to anything in the designated area, nor are they allowed to add or remove objects from someone else's personal space.

Territoriality was examined in Scott et al. (2004), where they found that collaborators tend to use three types of tabletop territories to divide the tabletop. This includes group space at the center of the table, personal space generally right in front of each individual and storage space, which can usually be found off to the side. When considering options to protect private information on a tabletop, it is important to keep people's natural desire for partitioning the space in mind. Another factor to consider is the shape of the table. A study was performed in a school library that showed students would avoid round tables because it is more difficult to partition them into individual workspaces, so they often chose the rectangular tables (Thompson, 1973).

Hagen & Sandnes (2001) discussed anaglyph image information hiding to be used for information hiding on digital tabletops. In this method a pair of glasses that has a unique color will be given to participants. If an observer is wearing red glasses, information in red will be filtered for them. Therefore, a participant with different color glasses can type things

without others noticing. Still the method is limited and does not guarantee privacy because at any moment if a participant takes off their glasses, they can see all the information (Figure 2.2).

Figure 2.2 Filtering the information with anaglyth images [4]

Hand Gesture Techniques

The use of hand gestures has also been considered as a technique to protect personal information. Wu & Balakrishnan (2003) examined several different multi-finger and whole hand gestures that can be used for multi-user tabletop displays. One of the whole hand gestures was the horizontal hand, where the user would place their hand horizontally along the tabletop. Although the gesture was developed originally to display the properties of the selected objects for this application, it was noted that users could use this technique to protect information from others. The hand acts as a barrier, and in order to see what the user is hiding, one would have to stand up and intentionally look over their hand, thereby breaking social protocol.

[4] © Simen Hagen, Frode Eika sandnes and Springer, used with permission

Another interesting idea from this work was the tilted horizontal hand, where the user would place their hand horizontally on the table, but tilt it away from other users. Since the setup used top-down projection, they were able to display information onto the palm of the hand. In this case, it is possible to tilt the hand towards oneself to enter private information, and then turn the hand towards the other members in order to share the information, if needed.

Figure 2.3 Two people using multi-finger and whole hand gestures[5]

2.4 A Framework for Designing Systems to Support Privacy

In addition to the development of techniques and technologies to address privacy concerns, other researchers have also explored how to apply privacy legislation to design concepts. The idea is that the user interface of a computing system can play an advantageous role in avoiding unintentional intrusions on privacy (Denning & Branstad, 1996).

[5] © Mike Wu and Ravin Balakrishnan, used with permission

Kobsa (2001); (2002) analysed how personalization services such as websites might worry some users since they sometimes collect personal information implicitly—for instance by tracking usage patterns. He then examined implications of privacy laws and developed some design guidelines to help personalization websites build privacy-sensitive systems. "These guidelines include suggestions such as to: (1) inform users that personalization is taking place, and describe the data that is being stored and the purpose of the storage, (2) get users' consent to the personalization, and (3) protect users' data with strong security measures (Kobsa, 2002)."

Patrick & Kenny (2003) also discussed specific interface techniques that comply with the spirit of the European Privacy Directive. They introduced several human factor requirements that need to be met for an effective privacy interface design. These requirements are fundamental to this thesis and form the basis of the designs categorized into four groups: comprehension, consciousness, control, and consent (Patrick & Kenny, 2003). Below each of these categories is discussed:

Comprehension: In the category of comprehension, design requirements suggest that the user should understand the context of the domain and comprehend when a process such as data collection or consent is happening. One method to support comprehension is to mandate both traditional and digital training. Traditional methods include classroom training, manuals, and demonstrations which are time-consuming and in most cases expensive. Today, with the emergence of information systems and online applications, much effort is devoted to supporting easier forms of training (digital training) such as user documentation or tutorials.

Another form of informal training is built-in help systems that provide short, targeted information based on the context. Patrick & Kenny (2003) discuss other forms of comprehension methods that are used in HCI research, namely mental models and metaphors. In this research comprehension means the user should understand or has the data collection, use and disclosure practices that happen when using a social network's information-sharing website (Facebook, in this research) on a digital tabletop. For example, people should understand when they are giving consent, when their information is being collected, and how their information is being handled.

Consciousness: In the category of consciousness, interface design requirements suggest that the interface should make people aware or get their attention, especially at specific times. Consciousness and comprehension are interrelated and sometimes interchangeable in the sense that the user has to have some knowledge and understanding about the context before conscious attention is useful. In this thesis, consciousness refers to bringing knowledge and understanding to the attention of the user about collection, use, and disclosure of personal data and related privacy risks.

"The human-factors discipline has a long history of designing systems in a way that makes users aware of certain things at the right time (Wickens & Hollands, 2000)". There are various interface techniques that address consciousness such as pop-up windows, "help assistants", and many others. For some techniques, the user has to acknowledge receiving and understanding the message in order to proceed, while others just give suggestions or inform users of something without interrupting them. There are also other subtle methods

that use display characteristics such as color, sound, and placement of features and arrangement of interface components to have the maximum effectiveness. For example, displaying text in red can draw attention or playing a sound when filling out a form that collects data to make people aware of what is happening.

Control: In the category of control, design requirements suggest that the interface should provide users with the ability to control processing of their personal information. As with consciousness, control is also interrelated with both comprehension and consciousness. In other words, the user has to be aware that they are supposed to do something (consciousness) and know what to do (comprehension) in order to perform the action (control). For example, if a website's privacy practices do not comply with their privacy statement, first the user should know what data collection purposes are not legal and not mentioned in the website's privacy policy. Then they should notice and become aware that, for instance, the website is collecting their information for purposes other than those mentioned. Assuming all the conditions are valid, the user has to have the ability to control the way their PII is handled or should be able to object to the data collection practice.

There are some important concepts that contribute to the effectiveness of the control factor. One such concept is *affordance* (Norman, 1990)—to design an interface component to have attributes that allow people to know how it is used. If it is complicated, then it will not be effective and users may have problems using it. For example, in order to log out of a system, it should be obvious how, rather than providing this feature through a hidden button or an unrelated icon.

Consent: In the category of consent, design requirements suggest that if a user is giving consent to the processing of their personal information it should be informed, unambiguous and specific. The most common method of getting consent is through a "User Agreement" or "Terms of Service", which the user has to agree to in order to proceed. There are some guidelines for creating click-through agreements and obtaining consent that were developed by the Cyberspace Law Committee for the American Bar Association, such as the opportunity to review terms, the ability to reject terms, the ability to print terms, and the opportunity to correct errors.

In order to make sure all the circumstances are covered, many click-through agreements tend to be complex, lengthy and written in "legalese" resulting in users having difficulty understanding the document and its legal terms (comprehension problem) and then agreeing to the term without considering the terms and consequences (consciousness problem). People have constrained ability to process large data at once and this ability is affected by a number of factors. Interface techniques that are sensitive to human cognitive ability are useful and can provide better decision-making and control.

The above-mentioned elements are the core concepts of a privacy-enhanced design (Patrick & Kenny, 2003). In Table 2.1, elements of each privacy framework discussed in this thesis are mapped together with the core concepts discussed above.

Table 2. 1 Comparison of privacy principles and core concepts of privacy-enhanced design

PIPEDA	OECD	FTC's FIP	Core Concepts
Accountability	Accountability	NA	NA
Identifying Purpose	Purpose Specification	Notice/Awareness	Comprehension, Consciousness
Consent	Connection Limitation	Choice/Consent	Comprehension, Consent
Limiting Collection	Connection Limitation	NA	Comprehension, Consent
Limiting Use, Disclosure and Retention	Use Limitation	NA	Comprehension, Consent
Accuracy	Data Quality	Integrity/Security	NA
Safeguards	Security Safeguard	Integrity/Security	NA
Openness	Openness	Notice/Awareness	Comprehension, Consciousness, Control
Individual Access	Individual participation	Access/Participation	Comprehension, Consciousness, Control
Challenging Compliance	NA	NA	NA

Chapter 3. Identifying Privacy Threats of Digital Tabletops in Public Settings

3.1 Introduction

As discussed in Chapter 2, there has been a significant amount of research on technologies and techniques that addresses privacy issues relevant to digital tabletops. However, depending on what application is being used and in what situation, the privacy threats can change. Therefore, in order to distinguish the type of threats that can occur in this specific research setting (the use of OSNs on digital tabletops in public settings) three factors of privacy (location, screen size, data accessibility) are mapped in a 3D space. The points in this space represent different scenarios involving technology, each with unique threats to privacy.

The focus of this thesis is on applications with public data accessibility (e.g., Facebook) on large display devices (such as digital tabletops) when being used in public locations (such as shopping malls). The privacy threats specific to this setting will be identified by presenting scenarios addressing both desktop computers and digital tabletops to better distinguish the respective threats. Finally, based on the identified unique threats to this research setting, two common threat categories will be described that will lead the discussion in Chapter 4.

3.2 Factors Affecting Privacy

There are a number of factors, which may influence people's information privacy. (See Boritz & No (2011) for a comprehensive discussion of such factors.) Three of these factors are discussed in this thesis (Figure 3.1): location, screen size and data security.

Location: Exposure to privacy threats differs depending on where a person is physically located. This can vary from being in a very private place such as a corner in one's bedroom to a very crowded public place such as a busy shopping mall with a lot of unfamiliar people walking around.

Screen size: The smaller the device's screen, the harder it is to view the information, especially from farther away. Smaller screens in electronic devices reduce the visibility especially from farther distances and can make shoulder-surfing more difficult. Also, it makes it easier for the user to hide or face down small devices such as cell phones or laptop computers. Therefore, the size of the device's screen can play an important role in the information privacy of users.

Data accessibility: Information privacy concerns vary significantly when typing a piece of text on a personal computer versus commenting on a public page in an online social network. Generally activities on public websites are not as safe as working on one's own document offline. There are bugs and privacy breaches associated with public websites that makes them prone to privacy invasions.

Figure 3.1 depicts the three-dimensional space generated by these three factors. Each condition has some degree of privacy threat associated with it, but the nature of the threats

varies drastically between examples such as working in an online social network on a digital tabletop in a public setting versus listening to music on a cellphone while in bed.

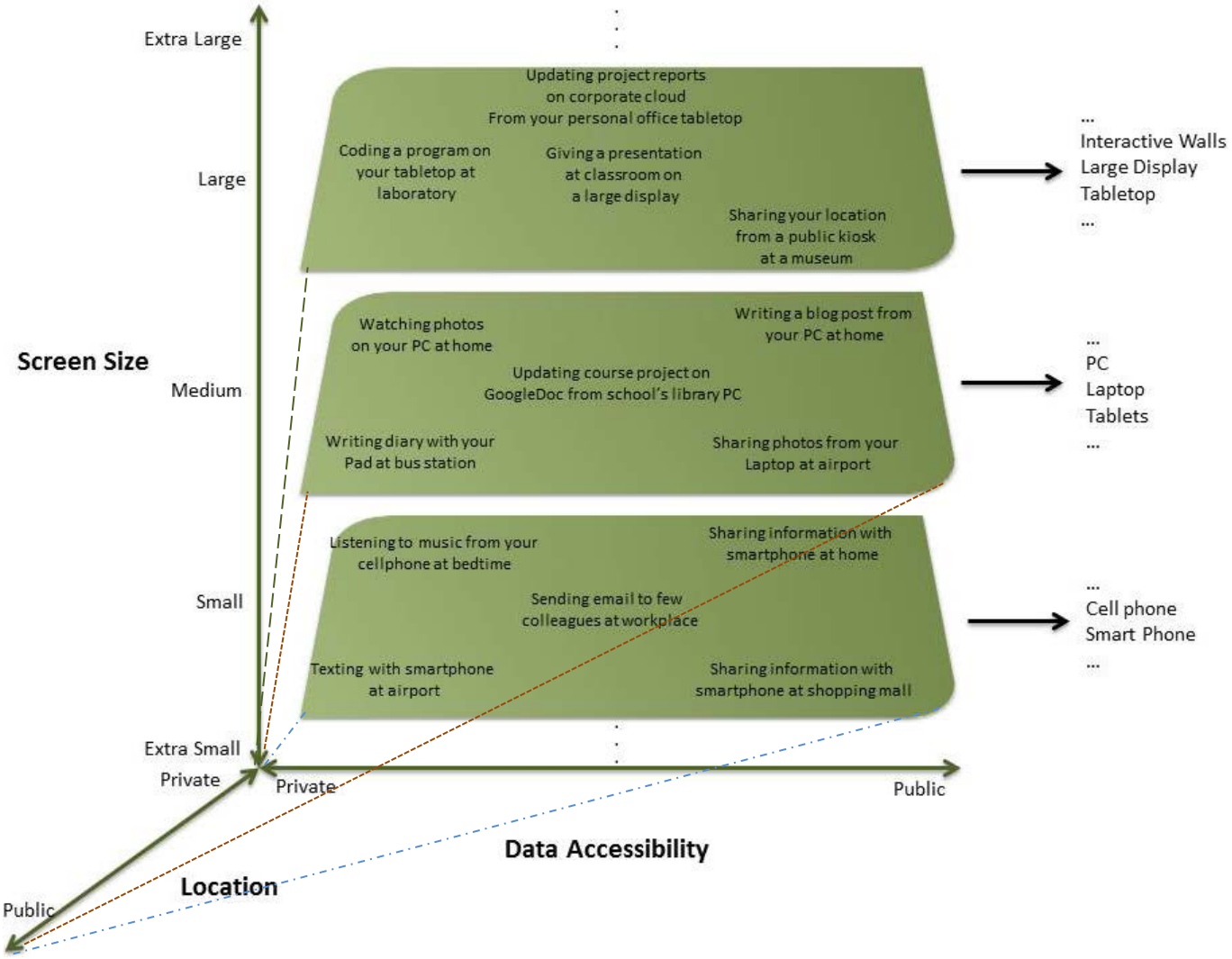


Figure 3.1 The three factors of privacy (location, screen size, data accessibility) mapped in a 3D space.

The points in this space represent different scenarios involving technology, each with unique threats to privacy.

3.3 Privacy Threats on Digital Tabletops

In the previous section, a 3D space of possible threats was defined. D_f(location, medium, data accessibility) and T_f(location, large, data accessibility) are identified to better distinguish between threats on desktop computers and digital tabletops. Since the focus of this research is on digital tabletops, in this section I only discuss two main categories of privacy threats on digital tabletops that cover all the threats recognized in the previous section: 1.*shoulder-surfing and 2.information sharing*.

Shoulder Surfing

A simple and very common threat when using digital tabletops in a public setting is called shoulder surfing. This situation involves someone looking over another person's shoulder, and in the process obtaining access to personal information, such as passwords or private emails. It can be done either intentionally or unintentionally by actively trying to spy on the information from a nearby spot or just noticing information by passing by someone who is working on a digital tabletop.

The size of digital tabletops makes shoulder surfing particularly easy to do. If the digital tabletop is located in a public and crowded place, this problem is exacerbated, since it is hard to notice whether someone is actually looking or not.

Information Sharing

Digital tabletops can be a useful collaborative tool, for instance for a group of people to plan a trip or organize a shopping adventure. This collaborative process can often involve the sharing of information among group members on the projected surface or even through their

own set of tools such as paper, laptops, smartphones, etc.

One consequence of sharing is that everything on the display becomes visible to everyone in the group. There may be a situation in which some contents should not be shared with all the participants but only one or a few of them. Examples of this type of information can be email and system notifications. In other situations, information may not be private but it is also not directly relevant to the discussion or may even be distracting. For instance when a person wants to show a specific line of text from a large document, they may prefer to show the final result to the audience instead of scrolling many pages in front of them.

3.4 Facebook Analysis

To demonstrate and evaluate interface designs to address privacy threats unique to digital tables in a public setting, I use the example of the social networking application *Facebook*. To set the stage for the remainder of the thesis, in this section I first provide the motivation for using a social networking application as the focus of my analysis, then use the framework (Patrick & Kenny, 2003) described in Chapter 2 to highlight threats to privacy that exist in the desktop version of Facebook. I then highlight new threats that would occur were the *same policy* to be used for the *same (unmodified) application* on a digital table in a public setting. In the following chapter, I will describe how to design interfaces for digital tabletop applications to address some of these threats.

Motivation for the use of Facebook

I chose Facebook as my illustrative social network because it is the most widely used social networking application and is often criticized for its privacy policies. However, at first consideration, one might question why a person might want to use a social networking site on a large table in a public setting, but there are several scenarios where I hypothesize such a device might be considered useful. For example, at a furniture store, a person may wish to show the retailer some pictures of their home from Facebook to see which sofa matches their wallpaper. If the person does not have any smart device with him at the store, he may be willing to use the digital tabletop placed in the store to access his Facebook account. Another example might be in a hotel, when a family decides to plan a day and the daughter of the family remembers a picture of her friend on Facebook travelling to a beautiful park. If they don't have their personal electronic devices with them, she may use the digital tabletop located in the hotel lobby. Yet a third example could involve an ad-hoc encounter between friends at a mall, where one wishes to show the other something from her Facebook page and a convenient way may be to use a digital tabletop in the mall that is located near the a customer service booth.

These scenarios illustrate situations in which accessing a social networking application on a large screen may be useful; however, the collaborative and open nature of digital tabletops increases threats to privacy already present in the current Facebook system, and may make people wary of using a digital table in this manner. For example, people might not be comfortable displaying the entire conversation with a loved one when looking for a phone

number or to enter their password in front of a friend while they need to log into their Facebook account.

Threats to Privacy in Facebook on a Desktop vs. a Public Tabletop Setting

In Figure 3.1, every point represents a situation in the 3D space (location, screen size, data accessibility). This section focuses on two points that are most closely related to this research. The first is when an application with public data accessibility (Facebook) is used on a medium screen size device such as desktop computer in a semi-public place such as at home (D_f: semi-public, medium, public). The second point which is more important for this work is when an application with public data accessibility (Facebook) is used on a large screen size device such as a digital tabletop in a public place such as a shopping mall (T_f: public, large, public).

In order to determine what the privacy requirements are that should be met in either of the situations, a few statements representing privacy risks are taken as examples from Facebook's privacy policy. Then, some of the potential privacy threats existing in Facebook's privacy policy statements are recognized in both regular and tabletop settings and are demonstrated using scenarios.

Moreover, in the left column of each table the related privacy principles from each of the privacy frameworks (OECD, PIPEDA, and FTC's FIP) are identified because, as it is explained in Patrick and Kenny's (2003) work and mentioned in Chapter 2, the four core concepts of privacy design framework originated from privacy legislation.

Statement 1

"Facebook pages are public pages. Because pages are public, information you share with a page is public information. This means, for example, that if you post a comment on a page, that comment can be used by the page owner off of Facebook, and anyone can see it (Facebook, 2012)."

Principle	Privacy Threats	Description	Tabletop-Specific Privacy Threats	Description
Collection Limitation Principle/ Notice and Awareness /Limiting Collection	• User may not realize pages are public. • User may not know how public pages work such as information posted in a page might be used off of Facebook. • User may not be aware what information will be collected from him/her. • User does not know for what purposes his/her information	**Scenario:** This scenario addresses the privacy risks of public pages with current Facebook version. **Action:** John Doe is at home and opens his laptop computer to surf on his Facebook. While on his home page, he notices one of his friends commented on a debatable political post on a famous magazine page. He replies to the post and goes off of Facebook. Next day, he checks the magazine website and notices his comment with his name and a link to his profile is	• User may not pay attention to being in a public page, or commenting on a pubic page because his/her activities are visible to the public and they want to finish ASAP. • User may skip the user agreement because of public exposure of his/her information.	**Scenario:** This scenario addresses the privacy risk of using public pages on a digital tabletop with current Facebook version. **Action:** John Doe is a great fan of a clothing company. While he is at its store in a shopping mall notices there is a digital tabletop in one corner of the store with the store's fan page open on top. He goes closer and reads some

	will be used off of Facebook. • User does not know for how long his/her information will be retained. • User does not know who is accountable for the data collection. • There is no option available to inspect and challenge his/her PII discrepancy. • User does not know whether his/her PII will be deleted after opting out (unsubscribing, unliking) from the page.	posted on the website's discussion board section without his consent. John Doe who did not want his colleagues to know his political point of view is very upset about this situation and goes to the page and deletes his comment. But his comment still is on the website. He goes back to the page looking for an email or contact information but cannot find any. He sends a message to the page owner. Two weeks passes and he still did not get a response. All in all John Doe had an unpleasant experience and feels he has no control over his information privacy and his PI is being used despite the Facebook privacy policy being linked on that page which normally means they obey this privacy policy.	• User may forget to log off and other people take advantage of the logged profile.	comments on the page and suddenly notices someone posted some false information about the brand. He who is very loyal to the brand, immediately logs in with his account and agrees with some terms being shown to him and replies to that comment. Then leaves the table and goes out of store without logging off. After 10 minutes a kid comes to the table and starts leaving unpleasant messages for his friends and deleting some stuff. Next day, when John Doe found out what happened in his profile, he became very upset and promised himself to never again logs into public displays.

Statement 2

"Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social. One of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of that application, your friend would want to give the application her friend list that includes your User ID so the application knows which of her friends is also using it (Facebook, 2012)."

Principle	Privacy Threats	Description	Tabletop-Specific Privacy Threats	Description
Purpose Specification / Notice and Awareness/ Identifying Purpose	• User may not want others to know he/she is using that application. • User may not want to know what type of music he/she listens to or pictures he look at. • User may not want his/her ID to be	**Scenario:** This scenario addresses the privacy risks of above situation. **Action:** John Doe uses a music application in Facebook and listens to his favorite music through that application. One day he receives a phone call from one of his friends asking how he is doing and added that he noticed some depressing music John has been listening to recently. John assured him there is nothing important and hung up the phone.	• User may not want others track their activities. • User may not be aware that someone is shoulder surfing.	**Scenario:** This scenario addresses the privacy risk of above situation on a digital tabletop with current Facebook version. **Action:** John Doe plays violin in a classic orchestra. He does not want his friends in the group to know that he also likes hard rock songs and listens to them often. One day when he was working on the digital tabletop and also listening to rock music in the background in the music institution, one of the students who in fact is not a very good friend of John, passes behind him and

	shared with third party applications.	All in all John Doe was very upset with the situation and the fact that he does not have privacy even in listening to music and decided to unsubscribe from the application.		notices he is using that app. The day after the student registers for the app. Once he does that he can see all the music that John listens to and finds out John is a big fan of rock music. Then he spreads rumors around the institution that John is not really devoted to classical music and he probably should have been a rock musician. All in all, John was upset about people being judgmental around him and then about the fact that using the digital tabletop in the public place enabled the invasion of his privacy.

Statement 3

"If you share your contact information (such as your email address or mobile number) with your friends, they may be able to use third party applications to sync that information with other address books, including ones on their mobile phones (Facebook, 2012)."

Principle	Privacy Threats	Description	Tabletop-Specific Privacy Threats	Description
Use Limitation/ Choice and Consent/ Limiting Use, Disclosure and Retention	• User may not know his/her information can be synced or exported with other applications. • User may not want a third-party to get access to his friends' email addresses and possibly sell them to other companies for advertising purposes.	**Scenario:** This scenario addresses the privacy risks of above situation. **Action:** John Doe has a Facebook account with default privacy settings in place. He started receiving advertising emails from unknown companies recently. He also noticed all the companies he is receiving email from are those that one of his friends interacts with on Facebook. After discussing this with his friend, they figured out each time John's friend subscribed to a company's page on Facebook, he was actually giving consent that the emails of all his friends that are public can be collected and used by that company.	• User may not notice that their information such as email address or mobile number is public by default. • User may not want their information to be used by third parties for any other purpose than they gave permission for. • User may not be aware that they are giving consent to third party applications to gather their friends' information.	**Scenario:** This scenario addresses the privacy risk of above situation on a digital tabletop with current Facebook version. **Action:** John Doe works in a retail store. One day while he was using the digital tabletops in their store and he was in the middle of using an application on his Facebook, a customer came in and he had to finish using the tabletop. He agreed to the message that just popped-up on the screen and closed his Facebook account. The day after while he was using the application again he noticed that the application is sending suggestion to all his friends in Facebook without him really knowing.

Statement 4

"We like to tell you about some of the features your friends use on Facebook to help you have a better experience. For example, if your friend uses our friend finder tool to find more friends on Facebook, we may tell you about it to encourage you to use it as well. This of course means your friend may similarly see suggestions based on the things you do. But we will try to only show it to friends that could benefit from your experience (Facebook, 2012) ."

Principle	Privacy Threats	Description	Tabletop-Specific Privacy Threats	Description
Use Limitation/ Choice and Consent/ Limiting Use, Disclosure and Retention	• User may not know that features he is using are being revealed and suggested to his friends. • User may not want his other friends to know that he is using a particular feature.	**Scenario:** This scenario addresses the privacy risks of above situation. **Action:** John Doe has been single recently and started thinking about online dating applications. He connected to one through his Facebook account. The day after, John's friend called him and warned him about the freauds in online dating application. John was really surprised that his friend knew about this and decided to never again use tools and applications in Facebook.	• User may not want the Facebook's suggestions to be shown in public places. • User may not want Facebook to suggest their activities to friends in public places.	**Scenario:** This scenario addresses the privacy risk of above situation on a digital tabletop with current Facebook version. **Action:** John Doe is busy surfing in his Facebook account at an airport until his flight time arrives. Another person is using the table with him as well. The second person notices some Facebook's suggestion in John's page regarding one of John's friend's recent activities. The stranger is attracted to John's friend and remembers her name to add her to his friend list on Facebook later and pretend that he is John's friend so that they can communicate and hopefully date.

3.5 Summary

In this section I identified three factors of privacy (location, screen size, data accessibility) and identified two key threats associated with digital tabletops in public settings: shoulder surfing and information sharing. I then extended my threat assessment to the use of applications with public data accessibility (e.g., Facebook) through the use of scenarios addressing both desktop computers and digital tabletops to better distinguish the respective threats. In the next chapter I will discuss user-interface designs for addressing these threats.

Chapter 4. Designing Interfaces to Support Privacy in Public Settings

4.1 Introduction

In Chapter 3, I identified unique privacy threats present when using online social networks on digital tabletops in public settings. Location, data accessibility, and screen size were identified as three factors that affect people's information privacy. Shoulder-surfing and information sharing were also discussed as two common privacy threats when using digital tabletops in public settings.

In this chapter, I introduce five user-interface design ideas to address these privacy threats. Specifically, I present alternative designs that could be used in an information-sharing application such as Facebook on a digital table. The ideas presented contribute to an understanding of the context of privacy while using online social networks as an information-sharing application on digital tabletops in public settings such as shopping malls. Each design idea is presented and then discussed based on the four categories of requirements for the effective design of privacy in an interface that were introduced in Section 2.4: comprehension, consciousness, control, and consent (Patrick & Kenny, 2003). Each design is structured so that the least amount of information is shown where possible; however, some expansion features are available to the user to access more information upon request. Also each design can be useful in addressing both categories of privacy threats on digital tabletops (shoulder-surfing and information sharing) (Section 3.4). I first briefly reiterate the four categories of requirements for design, and then describe each of the five designs:

Comprehension:

The principle of comprehension suggests that participants should know that by using a digital tabletop in a public setting their information is open to new type of collection, use and disclosure and there might be threats and possibly malicious use, specifically, threats that are caused by the open and collaborative nature of digital tabletops.

Consciousness

The principle of consciousness suggests that participants should be aware and conscious of threats to information privacy. In the specific situation of tabletop use in a public setting, this consciousness extends to an awareness of unique threats to personal information, such as the possibility of unfamiliar people being able to observe private information, like appointments and personal pictures, as well as passwords and credit card numbers.

Control

The principle of control suggests that participants should have control over how their personal information is being handled and be able to control it as needed. Specifically, when the user is working on a digital tabletop in a public setting and a stranger joins them at the same table and wishes to change the level of information visibility, both parties should be able to easily control what information gets shared from their own part of the screen.

Consent (discussed only in interface-design ideas 2 and 3)

The principle of consent suggests that the process of giving consent should be informed, unambiguous, and explicit. In the specific setting of a digital table in a public setting, the design should be particularly concerned with providing consent about what information is displayed on the screen, in addition to typical concerns about what information is stored and where.

4.2 User-Interface Design Ideas for Effective Privacy Interfaces

Design Idea 1: Blurring and Revealing Information

In some situations, it may be desirable to display information contained in a message without revealing the entirety of the message.

Scenario: Alice is in a public library and wants to check a book's name in her Facebook messages on a digital tabletop, but does not want all the information to become visible so that Bob (a passer-by) would be able to read or shoulder surf.

In this interface-design idea, I demonstrate the use of a blurring technique that blurs the entire message to prevent information from being unintentionally revealed. The user can unblur the text (i.e., make it visible) by dragging on the screen from left-to-right and can blur it again by dragging from right-to-left (**Control**). Therefore, if a user wants to show some information to another person, he/she has control over not revealing personal information, yet still has the opportunity to share. One possible drawback of this technique is that, if the message is lengthy, it might take too long to find information

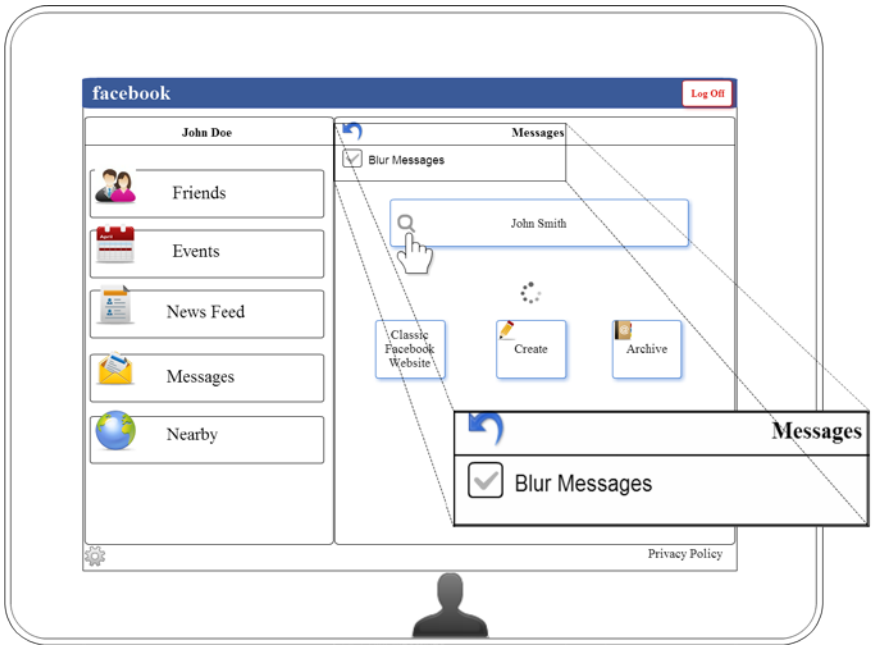


Figure 4.1 "Blur messages" checkbox

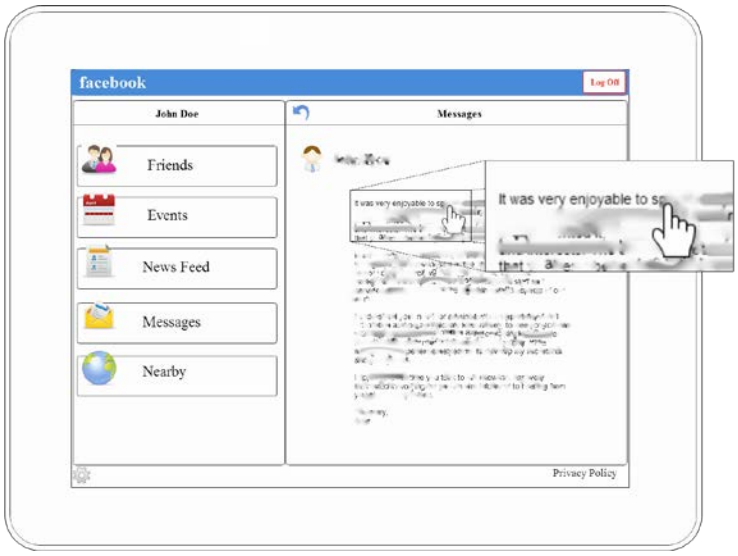


Figure 4.2 Visibility touch

Design Idea 2: Pattern Consent

As discussed above, although each design was created using the principle of minimalism, the user still has the ability to view any level of detail of the information (**Control**). Moreover, many current designs use the concept of a message box to obtain consent. In this interface-design idea, I investigate the use of a dragging technique to address privacy threats when navigating through such a message box.

Figure 4.3 shows the interface when the user is looking at their message inbox. The user might, for instance, decide to see all the messages at once, similar to how they would be currently presented in Facebook on a desktop. Selecting the "Classic Facebook Website" button changes the interface so that all messages are visible. The revealing of all messages is an event that, without proper design, could easily introduce privacy threats.

One way to ensure that users pay attention to the message is to engage them in an activity. One example, as illustrated in Figure 4.3, is to require that the user make a hand gesture on the surface in order to proceed, an idea inspired by the "Pattern Lock" locking mechanism on Android devices. The idea is to ensure the user understands and is aware of his/her action and anticipated consequences (**Comprehension and Consciousness**). This message is implied with the red glowing border, warning message, and the action of making a gesture on the table to

unlock the code. By giving the user a pattern to unlock the code, the user likely becomes more aware of his or her decision. Also, as is shown in Figure 4.4, the “Okay” button is not activated until the user makes the whole gesture on the screen and verifies that he or she has read the message. Using this technique, a user cannot easily skip the message without paying attention and reading the message.

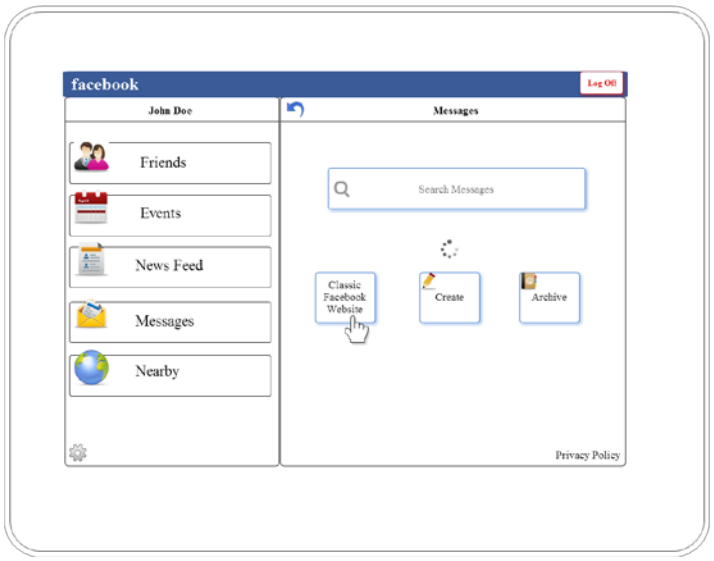


Figure 4.3 Switching to classic Facebook website in message inbox

Figure 4.4 Unlocking the page to reveal all information

Figure 4.5 Unlocked page and activated Okay button

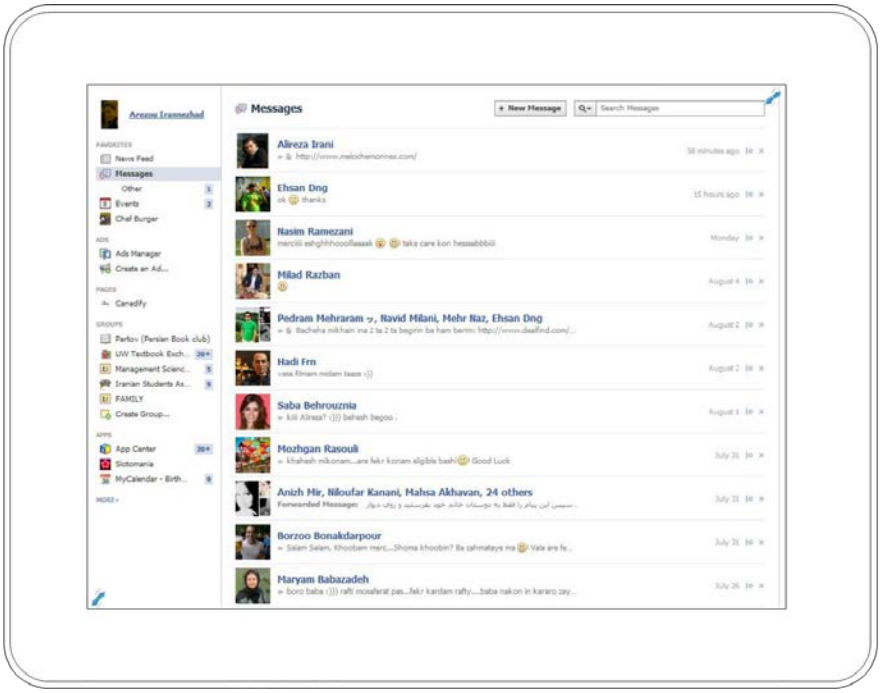


Figure 4.6 User pressed the okay button and switched to the classic Facebook page

Design Idea 3: Swipe Consent

Interface-design idea 3 is an alternative technique for avoiding threats to privacy when navigating through a message box (**Control**). This technique follows the idea of Just-In-Time-Click-Through agreement (Patrick & Kenny, 2003) and tries to inform the user of his/her decision (**Comprehension**) and makes him/her aware of the possible consequences (**Consciousness**). Upon completing the necessary dragging actions, the user can be expected to have provided consent to present the information on the following screen (**Consent**).

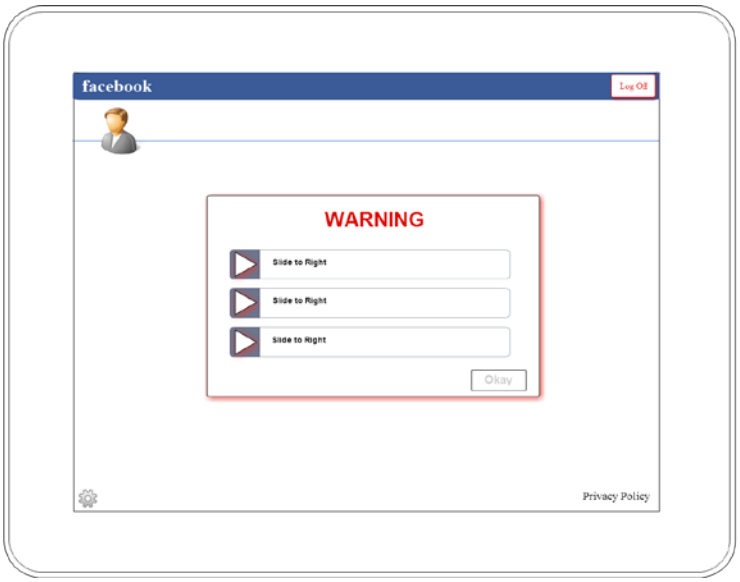


Figure 4.7 Revealing the warning message by sliding the cursor

The idea of requiring the user to slide the bar in order to read the text, inspired by the lock screen on Apple's iPhone, is to obligate the user to read the warning message before being able to proceed to the next page (**Consent**). Therefore, the Okay button will not be activated even half way through (Figure 4.8) but only once the user slides the cursors and reveals the whole message (Figure 4.9).

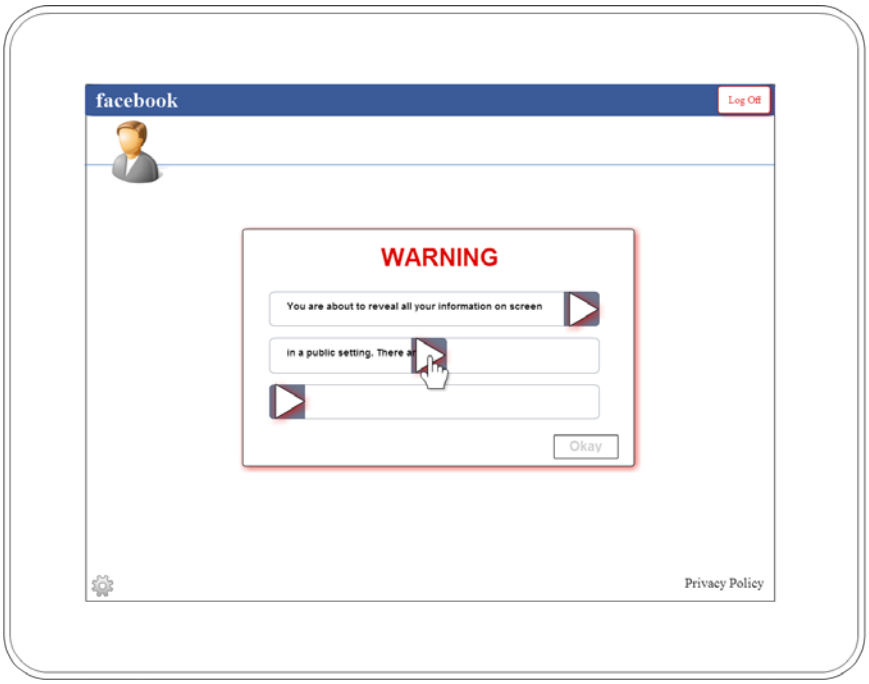


Figure 4.8 The okay button is not activated until the whole message is activated

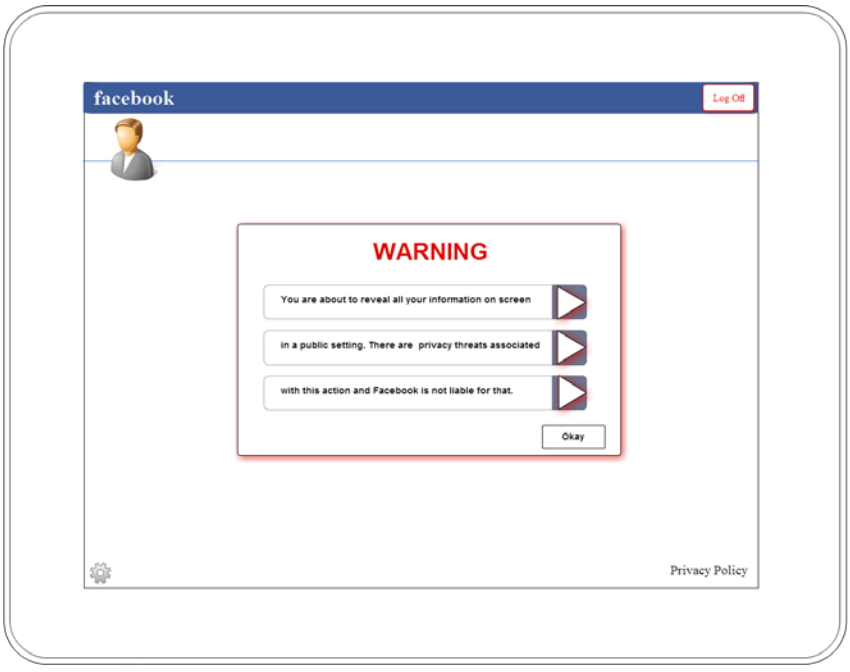


Figure 4.9 The whole message is revealed and the okay button is activated

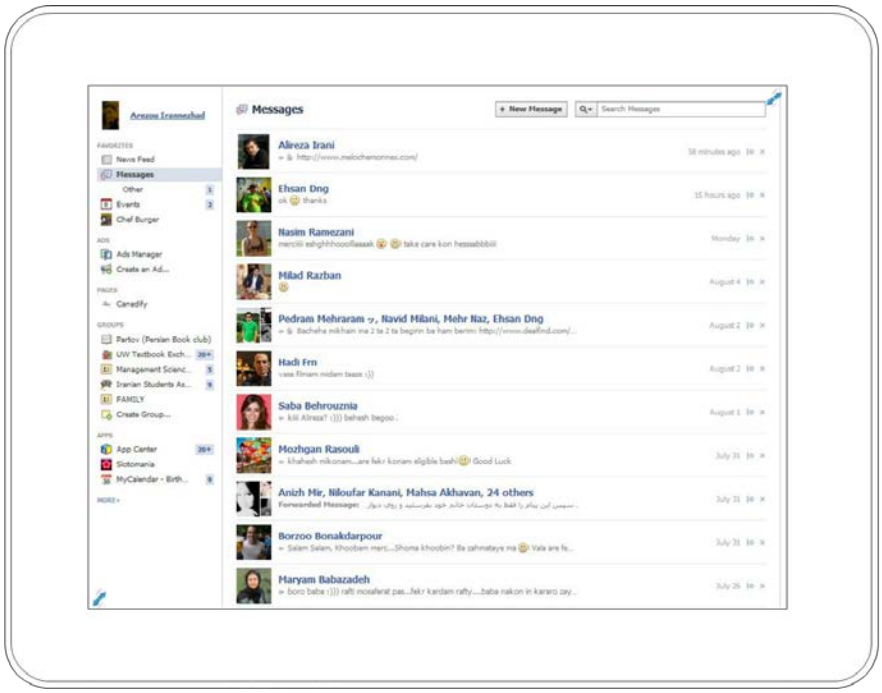


Figure 4.10 User pressed the okay button and switched to the classic Facebook page

Design Idea 4: Semantic Zooming

Semantic zoom is an information visualization technique for zooming into information in which not only the size of the data is affected but also the presentation level is different (Bederson & Hollan, 1994);(Perlin & Fox, 1993). The idea is that when a user is using a digital tabletop in a public place where people around who can shoulder surf, they can control the level of information as the people come and go. In this design, they can receive more or less information by pinching on the screen and resizing the page. When performing this action, the amount of presented information will be reduced or increased as the user zooms in or out (**Control**). There are arrows at the corner of the tabletop surface to signal to the user that semantic zooming is available (**Comprehension and Consciousness**).

As can be seen in Figure 4.11, the smallest level of message archive is being shown. If the user pinches on the screen, the page becomes bigger and more information is revealed (Figure 4.12). Figure 4.13 shows the largest zoom level available, which has as much information as in a classic Facebook website.

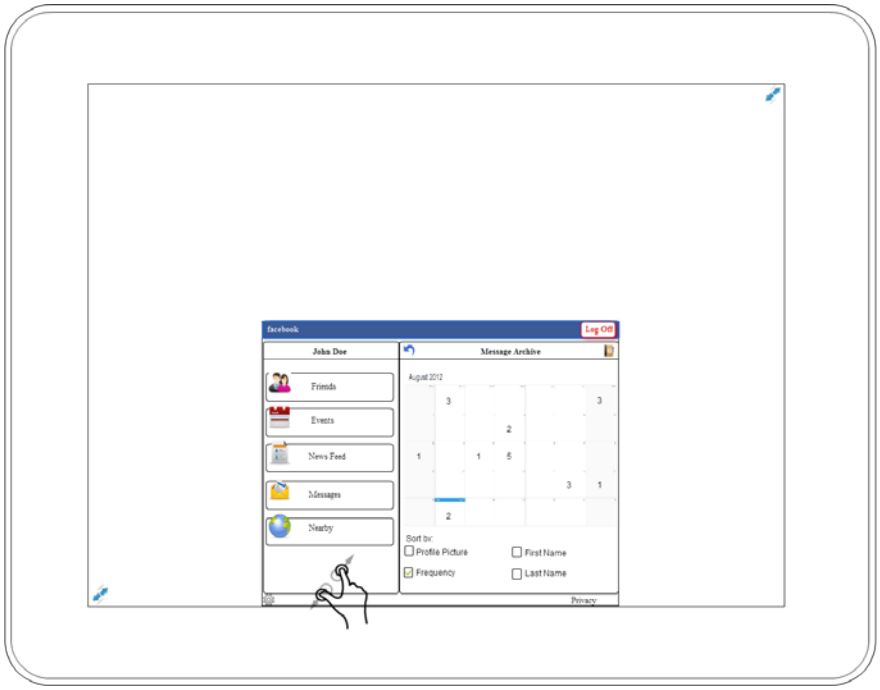


Figure 4.11 User is logged in message archive

Figure 4.12 When the page is zoomed in by pinching more level of information will be shown

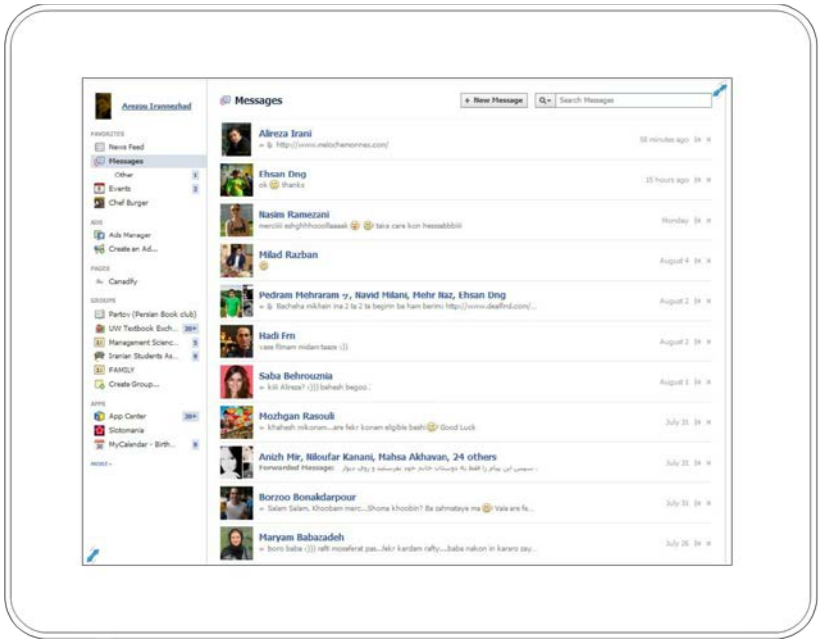


Figure 4.13 The most zoomed in level in classic Facebook version

Design Idea 5: Managing Multiple People Using Facebook

Designing systems that make users aware of certain information at specific times has a long history (Wickens & Hollands, 2000). There are some interface techniques that use display characteristics to draw attention (Patrick & Kenny, 2003). In this interface-design idea, display characteristics are used to make users conscious about special features in the application that otherwise might be ignored.

Scenario: Bob is in a shopping mall and suddenly sees his friend Alice. He remembers that he was supposed to share some information with her that is in a message in his Facebook account.

The redesigned Facebook interface in Figure 4.14 demonstrates an interface that not only provides the ability to share information with others but also provides control over personal information. As can be seen, the glowing border around the Facebook page plays a consistent role in reminding the user of being in a public setting and consequent potential privacy threats. Use of a glowing border for digital tabletop applications is discussed by Seto (2012) as a method to provoke interaction. This same idea is used here, but instead for

providing awareness about the environment and associated privacy threats (**Consciousness**).

Additionally, as soon as the system knows about another person's activity on the same tabletop, a red triangle appears in the same direction so that user constantly has in mind possible information theft from the other user. Alternatively, in systems that can sense the presence of another person around the digital table without them doing any activity, this red triangle could appear on approach rather than upon interaction. In addition, if the user taps on the red triangle a pop-up menu appears giving the user the option to either "Duplicate" the page for the user standing on that side so they can have a same view of the same page or "Pass to Left" which rotates the same page towards the other user (**Control**).

Lastly, the "Log Off" button has a glowing red border in order to remind the user at all times not to forget about logging off from their account. The idea is to present this feature as a button whose color is exaggerated (e.g., with red or yellow) and put it in a place on the screen that has the greatest probability of being seen (**Consciousness**). The button also glows or can be shaded to maximize its effectiveness. The anticipated consequence of not doing so may be that another user adversely uses the account.

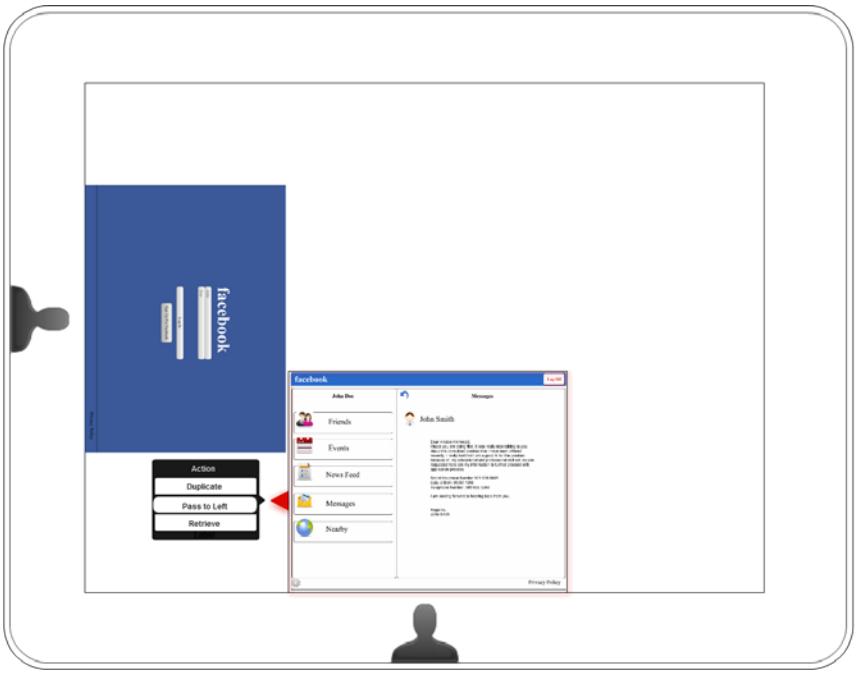


Figure 4.14 Facebook page with glowing border and red triangle

4.3 Chapter Summary

In this chapter I presented design techniques for creating user-interfaces with embedded privacy considerations suitable for the use of online social networks on digital tabletops in public settings. The focus of each set of design is on improving comprehension, consciousness, control, and consent elements. According to the privacy design framework introduced in Chapter 2, improving the above elements will lead to improvement of privacy requirements derived from privacy legislation (Patrick & Kenny, 2003). In the next chapter, I describe a study that was run to evaluate the interface-design ideas and techniques introduced in this chapter to validate these design.

Chapter 5. Evaluating New Interface Designs

The interface-design ideas presented in Chapter 4 were an attempt to build a service/system that enables users to understand how their personally identifiable information is being handled, to control their personally identifiable information, to be informed when they are giving consent, and to give clear and explicit consent to the processing of their data (Patrick & Kenny, 2003). In this chapter, I evaluate users' perceptions about the designs to validate the effectiveness of the techniques that have been proposed in the designs and assess whether they accomplish the goal of addressing the threats to privacy specific to digital tables in a public setting.

This chapter describes the results of an informal laboratory study in which the proposed interface-design ideas were evaluated to better understand the strengths and weaknesses of the designs presented in Chapter 4 and whether they meet our goals of improving personal information privacy according to framework elements introduced in Chapter 2.

5.1 Method

In this study, I evaluated the effectiveness of my designs at meeting the requirements categorized by comprehension, consciousness, control, and consent. As these properties are particularly difficult to measure quantitatively, I instead used a qualitative approach in which each participant completed some tasks with my proposed designs, and then provided feedback through questionnaires and an interview.

Participants

Ten graduate students from the University of Waterloo participated in the study. Four participants were female, six were male, and their ages ranged from 24 to 31 years (*Mdn*=27, *SD*=2.4). None of the participants had previous experience using a tabletop display, but all of

them had experience using multi-touch smartphones. All participants had Facebook accounts and 80% were used to collaboratively using Facebook with friends in public settings.

Apparatus

The study was conducted on a SMART Table, which is a rear-projected tabletop display with a 71.5 cm (diagonal) interactive touch screen (Figure 5.1). The projected display was 91.5 cm by 74 cm with a resolution of 1024 by 768 pixels, and the table itself is 65.4 cm tall. Participants sat beside the table on a chair adjusted to a fixed height so that they were within comfortable reaching distance to the entire surface of the display. The software for the study was developed in Processing (http://processing.org/), a Java-based programming language, and the Simple Multi-Touch plugin[6] [7] for Processing, which provides support for multi-touch devices and for the SMART table being used in this study. Coding was performed by an undergraduate intern at the University of Ontario, Institute of Technology.

Procedure

Each participant began the experimental session by filling out a pre-study questionnaire, which included ten background questions about their previous experiences with Facebook and their current understanding of privacy policies in general and for Facebook in particular. Then, the experimenter explained the study procedure and asked participants to imagine themselves in a public setting such as a busy and crowded shopping mall while performing the tasks in the experiment so that they had a sense of the targeted environment and the fact that unfamiliar people and strangers may pass by and they have to be careful with their information. With this scenario in mind, participants were asked to complete five tasks, each one followed by a questionnaire specific to that task. The entire session ended with a brief interview, the

[6] https://github.com/
[7] http://faculty.uoit.ca/collins/

participants were then thanked and provided with a gift certificate for $10 to a local coffee establishment.

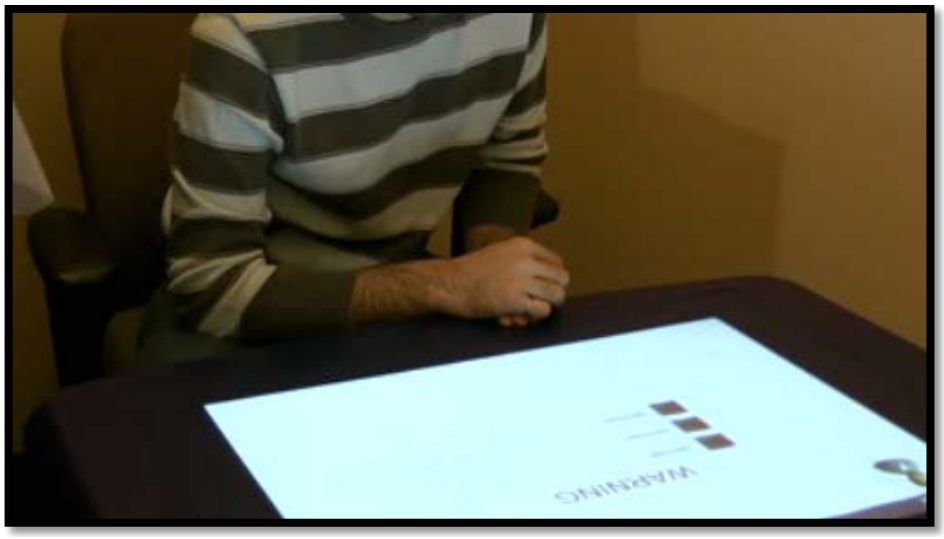


Figure 5.1 Study setup

Task 1: In task one, participants were asked to work with the tabletop and log into the application, and then to try to find John Smith's phone number in their message inbox without revealing any other information. They also were told that there was a feature available in the application that would help them to achieve this goal. The purpose of this task was to evaluate the blurring technique and to determine whether the "blurring and revealing information" technique could improve any of the comprehension, consciousness, and control elements.

Task 2 and 3: In task 2 and 3 the experimenter introduced two additional interface-design ideas for providing consent: "pattern consent" and "swipe consent". In this part of the study, participants were asked to use both techniques in order to evaluate their effectiveness at providing these improvements. In both tasks 2 (pattern consent) and 3 (swipe consent), participants were asked to find the name of the last person who sent them a message. In order to complete the task they were directed to a consent page including a warning message and an okay button. In task 2 (pattern consent), participants were shown a warning message that explained the action they were taking and described that they were to reproduce a pattern

through a gesture generated by the system in a designated area (see Chapter 4, Section 4.2). In task 3, they were asked to slide bars from left to right to reveal the whole message and be able to read it (see Chapter 4, Section 4.2). In both tasks, the okay button was disabled and they could not proceed until the dragging action was completed.

Task 4: The purpose of this task was to investigate whether or not semantic zooming is effective at providing control of one's personal information while using digital tabletops in public settings. In this task, the participant was specifically asked to find the number of notifications in the message inbox. This process required them to navigate to a page that used Semantic Zooming (See Chapter 4, Section 4.2) as a technique to access different levels of information presentation. The main purpose, however, was to evaluate whether semantic zooming is an effective technique at giving users control over their personal information.

Task 5: In the last task, the experimenter joined participants at the table and started working on a separate page on the same table as the participant was completing the task. While the participant's page had a red border at all times, a red triangle appeared when the experimenter joined the table which acted as a drop-down menu with collaboration options (See Chapter 4, Section 4.2). The idea was to evaluate the effectiveness of these options in addressing users' privacy requirements by improving comprehension, consciousness, and control.

Data Collection

Three types of data collection were used in this study: questionnaire, interview, and video recording. After each task, participants completed a questionnaire specific to that task (see Appendix III for a complete list of questions) including questions related to comprehension, consciousness, control, and consent (if applicable) to evaluate how effective each design was in improving these elements. For each task they also answered one question verbally in an interview form. Moreover, each session was video recorded so that the experimenter could go back and listen to interviews and review how they made gestures and what difficulties they had using the techniques.

5.2 Hypotheses

The following hypotheses were tested in this study and each is related to one task:

H_1: The blurring technique improves a person's ability to comprehend and be conscious of threats to privacy, and to control how much of their information is shared with others in a public setting.

H_2: The pattern consent technique improves a person's ability to comprehend and be conscious of threats to privacy, to control how much of their information is shared with others, and to give informed and unambiguous consent to the processing of sensitive data in a public setting.

H_3: The swipe consent technique improves a person's ability to comprehend and be conscious of threats to privacy, to control how much of their information is shared with others, and to give informed and unambiguous consent to the processing of sensitive data in a public setting.

H_4: The Semantic zooming technique improves a person's ability to comprehend and be conscious of threats to privacy, and to control how much of their information is shared with others in a public setting.

H_5: The use of collaboration features to manage multiple people improves a person's ability to comprehend and be conscious of threats to privacy, and to control how much of their information is shared with others in a public setting.

5.3 Results

The data sets were analyzed using SPSS software. Answers were analyzed using a combination of Chi-Square and One-Sample Wilcoxon Singed-Rank analyses for "Yes" and "No" and scale-based questions, respectively (α = .05). The null hypothesis for all Wilcoxon tests is that the median of each question is equal to the score of the "Neutral" responses. Therefore, in 5-point scale questions the null hypothesis is that the median is equal to 3 and in 7-point scale questions is equal to 4. In Chi-Square tests, the null hypotheses are that all answer's categories ("yes", "no", or "not sure") occur with equal probability. I first describe

results for each task's questionnaire data, and then describe results of interview and observations for each task. Because this is an informal study with a limited number of participants (10), the statistical power of the experiment was low, and the a "Marginally Significant" level was set to be between .05 and .09.

5.3.1 Questionnaire Data

For each task, all questions are divided into the categories of comprehension, consciousness, control, and consent and a quick summary of the results is presented. However open-ended and interview questions will be discussed later in Section 5.3.2.

Task 1: Message Blurring

Table 5.2 shows the results of the data related to task 1. Participant responses to ease of finding the technique (Q2) were not significantly weighted towards ease or difficulty. On the other hand, participants reported that the blurring technique helped make them *conscious* of privacy threats in public settings, though this result was only marginally significant (Q3). Participants also reported that the blurring technique was helpful (i.e., was rated significantly higher than neutral) in *controlling* information theft in public settings (Q4).

Table 5.1 Task 1 questions

Q2	Did you find the "Blur Messages" option easy to find?
Q3	If you answered "Yes" to the above question, how much did this feature make you aware of privacy threats in a public place on a scale of 1 to 5?
Q4	How much do you think the invisible touch is helpful to avoid information theft in public places on a scale of 1 to 7?

Table 5.2 Task 1 test results

Core Concept	Question	Type	W	$\chi 2$	p	N	Distribution	Mdn	Max	Min
Comprehension	Q2	Yes/No/I didn't use it	-	1.4	.497	10	Yes=5, No=3, I Didn't use it=2	-	-	-
Consciousness	Q3	5-point scale	6	-	**.083**	5	Neutral=2, Made me aware=3	4	4	3
Control	Q4	7-point scale	45	-	**.006**	10	Neutral=1,Somewhat helpful=1,Helpful=5, Very helpful=3	6	7	4

*W= One-Sample Wilcoxon Signed Rank Test Statistic
** The bolded p-value means the test is significant or marginally significant.

Task 2: Pattern Consent

Table 5.4 shows the test results for task 2. The message in the consent page was helpful (i.e., rated significantly higher than neutral) for *comprehending* the possible privacy threat of switching to the classic Facebook page in public settings (Q7). Moreover, participants reported that the pattern consent feature made them significantly more *conscious* (Q8) and provided significantly more *control* (Q10) for avoiding information theft in public places.

Table 5.3 Task 2 questions

Q7	How much do you think the warning message was informative and helpful in understanding the situation on a scale of 1 to 7?
Q8	How much did this feature make you aware and conscious of being in a public place and anticipated consequences of your decision on a scale of 1 to 5?
Q10	How much do you think the Passgesture is helpful to avoid information theft in public places on a scale of 1 to 7
Q12	The type of user agreement being presented in Task 2 is a short targeted type of user agreement called Just-in-time-click-through-agreement. How effective did you find this comparing to long user agreements on a scale of 1 to 7

Table 5.4 Task 2 test results

Core Concept	Question	Type	W	$\chi 2$	p	N	Distribution	Mdn	Max	Min
Comprehension	Q7	7-p scale	36	-	**.01**	10	Neutral=2,Somewhat helpful=4, Helpful=4, Very helpful=1	5.5	7	4
Consciousness	Q8	5-p scale	25	-	**.05**	10	Little effect=1, Neutral=3, Good effect=4, Made me really aware=2	4	5	2
Control	Q10	7-p scale	38	-	**.05**	10	Unhelpful=1, Somewhat unhelpful=1, Neutral=1, Somewhat helpful=1, Helpful=5,Very helpful=1	6	7	2
Consent	Q12	7-p scale	21	-	.26	10	Neutral=4, Somewhat effective=1, Effective=3, Very effective=2	5.5	7	4

*W= One-Sample Wilcoxon Signed Rank Test Statistic
** The bolded p-value means the test is significant or marginally significant.

Task 3: Swipe Consent

In task 3, all questions had significant test results (see Table 5.6). Nine of ten participants reported that they felt they could *comprehend* what to do (Q14), and participants reported that the message in the consent page was helpful (i.e., rated significantly higher than neutral) for *comprehension* of the consequences of their actions (Q15). Participants also reported that the swipe consent technique was effective in making people *conscious* of privacy threats at a digital tabletop in a public setting (Q16). Also, participants indicated that the swipe consent technique was helpful in *controlling* information theft (Q18) and effective at allowing participants to give a clear, unambiguous *consent* (Q20).

Table 5.5 Task 3 questions

Q14	Was the little "Slide to right" note on the message bar helpful in understanding what to do?
Q15	How much do you think the warning message was helpful and informative about your decision and anticipated consequences on a scale of 1 to 7?
Q16	How effective was this feature in making you aware and conscious of being in a public place and the possible consequences of your decision on a scale of 1 to 5?
Q18	How helpful do you think the slide-to-reveal technique is to avoid information theft in public places on a scale of 1 to 7?
Q20	On a scale of 1 to 7, how effective was the slide-to-reveal technique to make you read the warning message as opposed to lengthy user agreements we normally see?

Table 5.6 Task 3 test results

Core Concept	Question	Type	W	$\chi 2$	p	N	Distribution	Mdn	Max	Min
Comprehension	Q14	Yes/No/ Not Sure	-	6.4	**.01**	10	Yes=9, Not sure=1	-	-	-
	Q15	7-p scale	45	-	**.006**	10	Neutral=1, Somewhat helpful=1, Helpful=3, Very helpful=5	6.5	7	4
Consciousness	Q16	7-p scale	55	-	**.004**	10	Somewhat effective=3, Effective=2, Very effective=5	6.5	7	5
Control	Q18	7-p scale	45	-	**.006**	10	Neutral=1, Somewhat helpful=5, Very helpful=4	5	7	4
Consent	Q20	7-p scale	45	-	**.006**	10	Neutral=1,Effective=3, Very effective=6	7	7	4

*W= One-Sample Wilcoxon Signed Rank Test Statistic

** The bolded p-value means the test is significant or marginally significant.

Task 4: Semantic Zoom

All task 4 questions were not significantly different than the neutral rating and so there is no clear indication that semantic zooming was effective for providing comprehension, consciousness, or control of privacy threats on a digital table in a public setting. On the other hand, there is also no evidence that this technique hindered privacy concerns in this context.

Table 5.7 Task 4 questions

Q21	How helpful were the arrows at the corner of the page in communicating that you can resize the page by pinching on a scale of 1 to 7?
Q23	How effective was this feature in making you aware and conscious of being in a public place and the possible consequences of your decision on a scale of 1 to 7?
Q24	How helpful do you think the Semantic Zoom for users to control their personal information in public places on a scale of 1 to 7?

Table 5.8 Task 4 test results

Core Concept	Question	Type	W	$\chi 2$	p	N	Distribution	Mdn	Max	Min
Comprehension	Q21	7-p scale	10.5	-	.27	10	Not helpful at all=2, Unhelpful=3, Neutral=2, Helpful=3, Helpful=3	3.5	6	1
Consciousness	Q23	7-p scale	14.5	-	.93	10	Not effective=1, Somewhat not effective=3, Neutral=3, Somewhat effective=1, Effective=2	4	6	2
Control	Q24	7-p scale	26.5	-	.22	10	Not helpful at all=1, Somewhat unhelpful=1, Neutral=2, Somewhat helpful=2, Helpful=3, Very helpful=1	5	7	1

*W= One-Sample Wilcoxon Signed Rank Test Statistic
** The bolded p-value means the test is significant or marginally significant.

Task 5: Managing Multiple People Using Facebook

Table 5.9 shows the results of analysis for task 5. The red triangle was not shown to be an effective indicator of the presence of another person at the table, with the number of people noticing vs. not noticing being statistically insignificant (Q28), leaving a small

number of responses for its effectiveness (Q29) at providing *consciousness* of the privacy threat of others being aware of one's actions. However, all participants reported that they noticed the "log off" button, rendering the statistical test for Q30 to be not technically possible to run due to lack of variation. Therefore, the deterministic result is that everyone noticed the log off button at the corner of the page. Furthermore, participants reported that the placement of the log off button was effective at making them *conscious* of the need to log off before leaving the digital table. Participants also reported that the the pop-up menu provided through the red triangle was effective at providing *control* over the sharing of personal information (Q32).

Table 5.9 Task 5 questions

Q28	Did you notice the red triangle appeared when I started using the table?
Q29	If you answered "Yes" to the above question, how effective do you think this technique is in making users more conscious when another person starts using the same table in a public setting on a scale of 1 to 7?
Q30	Did you notice the "Log off" button at the top right corner of the page?
Q31	If you answered "Yes" to the above question, how effective do you think the design and placement of the "Log off" button was in making the user more aware about logging off their Facebook account on the digital tabletop in a public setting on a scale of 1 to 7?
Q32	On a scale of 1 to7, how effective do you think the pop-up menu was in giving you control over how to share your personal information?

Table 5.10 Task 5 test results

Core Concept	Question	Type	W	χ^2	p	N	Distribution	Mdn	Max	Min
Consciousness	Q28	Yes/No/ Not Sure	-	.8	.67	10	No=4, Yes=4, Not Sure=2	-	-	-
	Q29	7-p scale	10	-	.66	4	Somewhat effective=1, Effective=1, Very effective=2	6.5	7	5
	Q30	Yes/No/ Not Sure	-	-	-	10	Yes=10	-	-	-
	Q31	7-p scale	45	-	**.006**	10	Neutral=1, Somewhat effective=1, Effective=6, Very effective=2	6	7	4
Control	Q32	7-p scale	45	-	**.006**	10	Neutral=1, Somewhat effective=6, Effective=2, Very effective=1	5	7	4

*W= One-Sample Wilcoxon Signed Rank Test Statistic
** The bolded p-value means the test is significant or marginally significant.

5.3.2 Observations, Open- Ended Questions and Interview Data

In this section, I report the results of the open-ended questions and semi-structured interviews conducted in between questions. A total of 5 interview questions and 8 open-ended questions were asked of participants each related to one a specific task. The interview questions were focused on the control element of each task and were intended to elaborate on the controllability of personal information.

Task 1: Message Blurring

Three participants (30%) reported that they did not quite understand what the technique was supposed to do (Q1). Two participants (20%) also did not understand the idea behind the blurring technique and thought it was annoying. The rest (50%) suggested that the technique could be used to protect information, especially when working in public. Overall, participants seemed to have a good understanding of the notion of this technique.

During interviews, although most of the participants found this technique beneficial for protecting their personal information in public places (Q5), many of them had difficulties finding the information they were asked to find and felt that because it was the first time they were using this technique they had difficulty locating the information. Even in instances where participants opened the message without blurring it, many tried to hide the information with their hands to protect their information. Many of them said that if they had a mechanism to search for specific text, it would be very helpful for them to control their information and possibly avoid using this feature

Task 2: Pattern Consent

Responses to open-ended questions (Q6) revealed that one participant was unable to complete task 2 and did not go through the page that included the pattern consent technique, another participant did not comprehend the notion of the technique (Q6) and thought it was instead access to her account, and a third participant clearly understood the purpose of

engaging in the act of gesturing to focus his attention on reading the warning message before giving consent. The six remaining participants recognized the feature as being like a password or passkey that needed to be unlocked to proceed. Finally, one participant said the feature was present to avoid accidentally pushing the button to switch to the classic Facebook page.

An important concept for providing control is to make sure the feature is designed to be natural and easy to control (affordance) (Patrick & Kenny, 2003), so the affordance of the pattern consent technique was examined in Q9. One of the ten participants did not accomplish task 2, and therefore did not use the pattern consent technique. Six participants realized that they had to read the message and draw the pattern while three others did not really understand what to do at first, and had to navigate back and forth through the pages until they did.

In response to how this technique can be improved to give users more control over their personal information (Q11) most participants said they did not read the message and focused entirely on making the gesture, so if there could be a way to make them pay more attention to the message it would be more efficient. Perhaps because the gesture was similar to Android's unlocking technique, they were familiar with what to do and did not pay attention to the warning.

Task 3: Swipe Consent

In task 3, in response to what participants think the swipe consent technique does (Q13), one participant said he thought the feature was intended to warn him about his actions, due to being in a public setting. Interestingly, two participants said this technique made them think more than the technique in task 2 about moving on to the next step and whether it was safe or not to do so. In other words, it was more effective at drawing their attention to the need to understand what was going on. Two participants said they thought they should unlock the page while it tried to warn them about something. One said it was a technique to force them to read something, while one of them said it was a kind of security measure. Two others said

it was to walk the user through a warning message. Also, one participant did not answer and just said they did not like it.

Five participants reported that they understood what they had to do when they saw the consent page (Q17) and that they were supposed to slide it to the right to reveal something. One participant stated that, since it was the first time he was seeing the swipe consent technique he wanted to make sure that he was in the right place before advancing to the next screen. Another participant said he thought this was a way to make sure no one was around, so that he could read the message in private. Also, one participant said that at first he thought it was a sort of security measurement, while another said she thought this was a private message and should not be read it in public.

In response to how the swipe consent technique can be improved to give users more control over their personal information (Q19), participants reported interest in sliding the bars to see what would happen. Because of their engagement in this task most of them read the whole warning message, unlike in task 2. However, a few of them stated that if they become used to this technique, they will probably slide the bars quickly and press the okay button without reading the text. Similarly, some of them reported that lengthy messages should be avoided because it makes the user tired. Lastly, one participant slid the bars from the bottom to the top and at the end suggested an order for the lines.

Task 4: Semantic Zoom

Among all participants, only one realized that the technique was useful for avoiding shoulder surfing and other privacy threats (Q22). Four of the participants stated that this technique was intended to ease zooming or was simply a different technique for zooming in and out. Two participants had no idea what the semantic zooming was for in the study. One participant thought that this was just a technique that demonstrated the multi-touch capabilities of the table. One participant stated the feature was to enable viewing of information from farther distances. Finally, one participant did not use the technique at all.

Responses to how the semantic zooming technique can be improved to give users more control over their personal information (Q25) showed that most participants were unfamiliar with the semantic zooming and had difficulty determining what to do. They hardly noticed the arrows at the corner of the surface; when asked how the technique and users' controllability can be improved they made suggestions such as making the arrows bigger, or replacing them with a hand icon doing pinching. Also it was recognized that if there were a message or notification letting the user know that pinching is available would be very beneficial, especially for the first-time users and would avoid revealing information by zooming in accidentally in a public setting.

Task 5: Multiple Simultaneous Uses

One participant (10%) realized that the red triangle was a sign of an activity happening elsewhere at the table (Q26). Most participants (70%) did not understand when and why the red triangle appeared, and instead thought it was something that provided more options. Two participants did not notice the red triangle at all.

Four of the participants wrote comments to the effect that they felt the red border was intended to show the border of the page and to separate the working areas (Q27). The remaining participants (6) did not notice the red border at all.

Most of the participants said that they did not notice when exactly the red triangle appeared (Q33)and once they discovered it, they were not sure about trying the options, as they were concerned that by mistakenly pressing one of the options, they would accidentally share their screen with a stranger.

5.4 General Discussion

In this section, I summarize the findings of my study by first relating the results back to each task's hypothesis, and then discuss implications for the design of digital tables in a public setting. The message blurring technique (used in task 1) was shown to improve *comprehension* and *consciousness* of threats to privacy, and to provide *control* of how much

information was shared (H_1 confirmed). Observations and interview responses, however, indicated that the comprehension element could be improved by using methods that notify users of the availability of such a technique.

The pattern consent technique (used in task 2) was effective at improving a person's ability to *comprehend* and be *conscious* of threats to privacy, to *control* how much of their information is shared with others, and to give informed and unambiguous *consent* to the processing of sensitive data in a public setting (H_2 confirmed). However, the interviews and observations showed that some people might skip reading messages as they become more familiar with the technique.

Perhaps the most promising technique was the swipe consent technique (used in task 3). It is clear from the analyses that H_3 can be confirmed. All responses were significant and indicated that the technique provided comprehension, consciousness, control, and consent. Results also showed that most participants understood what the technique does and is for. Moreover, the interview data showed that the technique used in task 3 was new to participants and engaged them in doing the task and consequently led them to read the whole warning message, whereas in task 2 a few of them skipped reading the warning message, and many indicated they would be more likely to do so with repeated use.

Contrary to H_4, there was no clear evidence that semantic zooming (used in task 4) was useful for improving comprehension, consciousness, control, or consent in public settings at a digital table (i.e., H_4 was not confirmed). Open-ended questions also revealed that only one person realized what the technique was supposed to do, and interview results showed that the main weakness of the technique was its lack of support for comprehension. Participants had difficulty noticing that this option was available and, when they did notice it, some of them were afraid of resizing the page and making private information more readable for people walking around or possibly shoulder surfing.

For the design that incorporated support for multiple simultaneous use of the table, comprehension was not effectively supported and consciousness and control were only

partially supported (H_5 was not confirmed). Most participants reported that they did not understand what either the red border or the red triangle was intended to indicate (comprehension). However, there was unanimous agreement on the noticeability of the log off button, and participants reported that this improved consciousness of this specific privacy threat. However, participants did report that the menu available when a second person was present provided suitable control of one's personal information. Nonetheless, the interview data and observations showed that the red border and triangle techniques used in task 5 had the potential to put users in an adverse condition of mistakenly sharing their page with strangers instead of helping them to control their information consciously. Participant did not realize when and why the red triangle appeared and some of them had difficulties finding options available for collaboration.

5.5 Limitations

The claims in this section are based on the findings of an informal study limited to the lab environment in the University of Waterloo with a small sample of participants with ages ranging from 24 to 31. Running a formal study with a larger number of participants from different age groups would complement the results of this study. Moreover, if this follow-up study were run in an actual public setting like a public library or a shopping mall, the data could be generalized further, as the participants would experience a more realistic feeling of being in a public place with unfamiliar people walking by as they explore the application.

In this study, I did not use the classic Facebook page as a baseline application. Instead, a newly designed Facebook prototype was used to test a set of different designs. Moreover, although we tested comprehension, consciousness, and control in all interface designs, consent was only tested in two of them. Having said that, the interface designs were not compared to one another and instead the data was analyzed on a self-report scale. In future research, the best result will be achieved if participants first use the classic Facebook website as a baseline and then use the redesigned version. Also it will be ideal to compare data from different designs with each other.

5.6 Summary

In this chapter, I presented a laboratory study to validate the designs presented in Chapter 4. Specifically, my study has shown that message blurring and the swipe consent technique are good candidates for addressing privacy concerns in this emerging environment. In addition, I have shown that the semantic zooming and multiple-person interface may require further design iterations before they could be effective at addressing issues of privacy on digital tables in public places.

Chapter 6. Conclusion and Future Work

This thesis demonstrates the design, implementation, and evaluation of privacy-enhanced interface designs for online social networks on digital tabletops in public settings. The motivation for this thesis was to shed light on circumstances and consequences of using online social networks on digital tabletops in public settings and also to embed information-privacy considerations into the design of systems and applications. The results of this research may provide knowledge and help for other researchers and system designers who work on digital tabletops in public settings.

This chapter concludes the thesis by summarizing the analyses and findings of the study. First the research contributions and final conclusions are discussed in Section 6.1 and then future work that this thesis may lead to and its implications are presented in Section 6.2.

6.1 Conclusion

Protection of personal information has become a critical issue in the digital world. The era of single-user desktop computers is changing to more sophisticated technologies such as digital tabletops. Digital tables are a promising new medium for the support of collaborative work. Instead of individuals working independently on their own devices or workstations, people can collaborate across a shared display through touch and gesture-based interaction while maintaining eye contact and engaging in conversation. Although digital tabletop displays offer many new possibilities for attracting the attention of passers-by in a public setting and offer the promise of new styles of interaction, they also introduce many potential threats to privacy.

In Chapter 3, three factors that affect privacy were discussed and two common threats to digital tabletops in public settings were identified to set the scene for analysing online social networks' privacy considerations using the Facebook privacy statement as an example of an

online social network. Ultimately several potential privacy threats were identified despite Facebook's privacy policy, judging from the privacy design framework introduced in Chapter 2. In Chapter 4, several interface designs were introduced to address the threats identified in Chapter 3. The motivation behind the designs is to improve personal information privacy according to the common requirements of widely-used privacy frameworks.

In Chapter 5, a study was run to evaluate the effectiveness of the designs and to investigate users' perception about their strengths and weaknesses. The main result of the study shows that users are sensitive to comprehension design elements. Therefore, among the five designs evaluated, the semantic zooming and collaboration feature used to manage multiple people uses were the least successful because participants could not figure out what is happening and what they should do to reach their goal and control the situation. On the other hand, the blurring technique, pattern consent, and swipe consent techniques were able to successfully communicate the potential privacy threats, and were seen as helpful by our participants.

The analyses of the interview data and findings based on observations also show that, in some cases, the level of control was not sufficient for participants and they started using their hands, for example, to protect their data. Such lack of control may result in people not using digital tabletops in public settings for information-sharing purposes.

Despite some of the limitations of the techniques that were introduced to participants, participants recognized the value of these designs and this work demonstrates the viability of addressing the privacy threats identified in earlier chapters through the design of a social networking interface. With further refinement and iteration, it is likely that these techniques could be improved and incorporated into designs of future social networking applications on this form of technology and in this type of environment.

6.2 Future Work

The result from this thesis can be used to inform the design of information-sharing websites (such as OSNs) for digital tabletops in public places. However, this research can also be used as a guide for a larger research project. The claims in this thesis are based on the findings of an informal study limited to the lab environment in the University of Waterloo with a small sample of participants with ages ranging from 24 to 31.

Running a formal study in a public place with a larger number of participants of more varied ages would be complementary to this study. Moreover, this thesis uses Facebook as a sample online social network (OSN) Future research can investigate other OSNs such as Twitter, Google+, My Space, and LinkedIn.

Glossary

OSN: Online Social Networks are websites such as Facebook, Twitter, etc., in which people share their information and interests and interact with friends in their profiles.

Digital Tabletop: Digital tabletops are horizontal computer displays with an interactive touch-sensitive area which serves as the surface of the table.

Privacy Policy: Privacy policy or sometimes called privacy law is a statement or legal document that defines the way a party collects, uses and disclosures personal information of users or clients.

PIPEDA: The Personal Information Protection and Electronic Documents Act is part of the federal privacy law that refers to the collection, use and disclosure of personal information in private sector organizations.

Privacy Act: is part of the federal privacy law which regulates public sector institutions.

HCI: Human-Computer Interaction is a field of study, mainly in Computer Science, that encompasses study, planning and design of interaction between people and computer.

CSCW: The term computer-supported cooperative work is used when collaborative works and activities are being supported by computer systems.

Microsoft Surface: Microsoft Surface is a computing platform made by Microsoft Corporation that enables user to interact with touch and other objects.

OSN: Online social networks are online web-based services that enable people to share interest and/or activities.

PII: Personally Identifiable Information is information which can be used to differentiate or locate and individual's identity either alone or when joint with other information that is linkable to a peculiar individual.

FTC: The Federal Trade Commission is an independent agency of the United States government concerned with the promotion of consumer protection and the elimination and prevention of anti-competitive business practices (Federal Trade Commission, 2012).

FIP: Fair Information Practices are guidelines representative of generally-accepted practices in an electronic marketplace.

OECD: The Organization for Economic Co-operation and Development are focused on helping governments in member countries and elsewhere to promote policies that will improve the economic and social well-being of people around the world (Development, Organization for Economic Co-operation and Development, 2012).

PET: Privacy-Enhancing Technologies is a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system (Blarkom, Borking, & Olk, 2003).

UBICOMP: Ubiquitous Computing refers to the third era of technology advised by Mark Weiser which is a model of human-computer interaction that computing technologies integrate with everyday objects and activities.

CAVE: A virtual reality environment in which projectors are directed to different walls of a room. The user walks around the room wearing a 3D glass to see 3D objects floating.

Virtual Reality: Is a form of technology that applies to a computer-simulated environment. People can interact with objects and explore different things that are generated by computer.

UI: User interface is the hardware and software components that exist between users and machine let the users manipulate the system.

JITCTA: A type of short and targeted user agreement that is being shown at the exact moment that user's consent is needed. If the user agrees with the term and gives consent, then he/she can continue working with application or system.

Permissions

Gmail by Google

Arezou Irannezhad <arezou.irannezhad@gmail.com>

Permission

2 messages

Arezoo Irannejad <airannej@uwaterloo.ca> Thu, Jan 17, 2013 at 2:49 PM
To: mchi@dgp.toronto.edu, ravin@dgp.toronto.edu

Dear Mike Wu and Ravin Balakrishnan,

My name is Arezoo Irannejad and I am perusing my master's degree in University of Waterloo under the supervision of Dr. Mark Hancock and Dr. Efrim Boritz.

I am writing my thesis about the use of online social networks on digital tabletops in public settings and referencing one of your papers (Multi-finger and whole hand gesture interaction techniques for multi-user tabletop displays).
I was wondering if I have the permission to use Figure 1 in your paper in my thesis document that shows two users making hand gestures on a digital tabletop.

Looking forward to hearing back from you.

Regards,
--
Arezoo Irannejad
MASc Student
Faculty of Engineering
Management Sciences Department
University of Waterloo
Telephone: +1-416-4199998
Email: airannej@uwaterloo.ca
Linkedin: http://www.linkedin.com/in/arezooirannejad

Mike Wu <mchi@dgp.toronto.edu> Thu, Jan 17, 2013 at 3:02 PM
To: Arezoo Irannejad <airannej@uwaterloo.ca>
Cc: ravin@dgp.toronto.edu

Hi Arezoo,

Unless Ravin has any objections, you have my permission to use the figure in your thesis document.

If you wouldn't mind, send me a digital copy of your thesis when you're all done. It sounds like interesting work!

And say hi to Mark for me!

Cheers,
Mike
[Quoted text hidden]

Gmail by Google

Arezou Irannezhad <arezou.irannezhad@gmail.com>

Permission for photo

2 messages

Arezoo Irannejad <airannej@uwaterloo.ca> Thu, Jan 17, 2013 at 1:33 PM
To: Frode-Eika.Sandnes@hioa.no, simenhag@ifi.uio.no

Dear Dr. Sandness and Dr. Hagen
My name is Arezoo Irannejad and I am perusing my master's degree in University of Waterloo under the supervision of Dr. Mark Hancock and Dr. Efrim Boritz.
I am writing my thesis about the use of online social networks on digital tabletops in public settings and referencing one of your papers (Visual scoping and personal space on shared tabletop surfaces).
I was wondering if I have the permission to use Figure 5 in your paper in my thesis document that shows one page of writing with two other red and blue lenses.
Looking forward to hearing back from you.

Regards,
--
Arezoo Irannejad
MASc Student
Faculty of Engineering
Management Sciences Department
University of Waterloo
Telephone: +1-416-4199998
Email: airannej@uwaterloo.ca
Linkedin: http://www.linkedin.com/in/arezooirannejad

Frode Eika Sandnes <Frode-Eika.Sandnes@hioa.no> Thu, Jan 17, 2013 at 2:52 PM
To: Arezoo Irannejad <airannej@uwaterloo.ca>

Dear Arezoo,

I am very happy that you are interrested in our work. We have no objections in you using the figure in your dissertation. However, note that we transfered copyright to Springer as part of the normal publication procedure. I suggest that you indicate Springer's copyright ownership in the figure caption together with the acknowledgement of our original paper.

I am writing on behalf of both me and Simen. Sadly, Simen passed away two years ago to this day.

I wish you good luck with the completion of your master degree. I would love to read your work once it is finished.

Best regards,

Works Cited

Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding.* Brooks/Cole Publishing Company.

Apted, T., & Kay, J. (2006). *Privacy and Remote Display Control on a Multi-user Pervasive table-top.* The University of Sydney.

Bardeesy, K. (2009). *Ottawa takes on social media giant for violating Canada's law*. Retrieved from The Globe and Mail: http://www.theglobeandmail.com/news/technology/ottawa-takes-on-social-media-giant-for-violating-canadas-law/article1220428/comments/

Bederson, B., & Hollan, J. (1994). Pad++:A Zooming Graphical Interface for Exploring Alternate Interface Physics. *ACM.*

Belloti, V. (1997). Design for privacy in multimedia computing and communications environments. In *Technology and Privacy.* MIT Press.

Beyer, H., & Holtzblatt, K. (1997). *Contextual Design: Defining Customer-Centered Systems (Interactive Technologies).* Morgan Kaufmann.

Blarkom, G. v., Borking, J., & Olk, J. (2003). Handbook of Privacy and Privacy-Enhancing Technologies. College bescherming persoonsgegevens.

Boritz, J. E., No, W. G., & Sundarraj, R. (August 25-27, 2009). Do Companies' Online Privacy Policy Disclosures Match Customer Needs? *Proceedings of the 2009 World Congress on Privacy, Security, Trust and the Management of e-Business.* Saint John NB.

Boritz, J., & No, W. (2011). E-Commerce and Privacy: Exploring What We Know and Opportunities for Future Discovery. *Journal of Information Systems*.

Brandeis, L., & Warren, S. D. (1890). The Right to Privacy.

Bringnull, H., & Rogers, Y. (2003). Enticing People to Interacti with Large Public Displays in Public Spaces. *INTERACT.* IOS Press.

Canada Department of Justice. (2012). *Personal information protection and electronic documents act (PIPEDA)*. Retrieved from http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-19.html#h-25

Carpendale, M., Inkpen, K., & Scott, S. (2004). Exploring Casual Tabletop Interactions.

Cavoukian, A. (2012). *Privacy by Design*. Retrieved from http://privacybydesign.ca/

Chan, L.-W., Hu, T.-T., Lin, J.-Y., Hung, Y.-P., & Hsu, J. (2008). On Top of Tabletop: a Virtual Touch Panel Display. *IEEE*.

Charters, D. (2002). Electronic monitoring and privacy issues in business-marketing: The ethics of the DoubleClick experience. *Journal of Business Ethics*.

Connolly, K. J. (2004). *Law of Internet Security and Privacy.* Aspen.

CSA. (n.d.). *Privacy Code*. Retrieved from Canadian Standard Association Group: http://www.csa.ca/cm/ca/en/privacy-code

D. Scott, S., D. Grant, K., & L. Mandryk, R. (2003). System Guidelines for Co-located,Collaborative Work on a Tabletop Display. *ECSCW*.

D. Scott, S., T. Carpendale, M., & M. Inkpen, K. (2004). Territoriality in Collaborative Tabletop Workspaces. *CSCW*.

De Luca, A., & Frauendienst, B. (2008). A Privacy-Respectful Input Method for Public Terminals. *CHI.*

Denning, D. E., & Branstad, D. K. (1996). A Taxonomy for Key Escrow Encyption System.

Department of Justice. (2012). *PRINCIPLES SET OUT IN THE NATIONAL STANDARD OF CANADA ENTITLED MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION.* Retrieved from Department of Justice: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-19.html#h-25

Development, O. f.-o. (2010). *OECD Privacy Principles*. Retrieved from http://oecdprivacy.org/

Development, O. f.-o. (2012). *Organization for Economic Co-operation and Development*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/OECD

Earp, J. B., Anton, A. I., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining Internet Privacy Policies Within the Context of User Privacy Values.

Facebook. (2012). *Facebook Privacy Policy*. Retrieved from Facebook: http://www.facebook.com/full_data_use_policy

Federal Trade Commission. (2012). *Federal Trade commission*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Federal_Trade_Commission

Federal Trade Commission. (2012). *FTC Issues Final Commission Report on Protecting Consumer Privacy*. Retrieved from http://www.ftc.gov/opa/2012/03/privacyframework.shtm

Federal Trade Commission. (n.d.). *Fair information Practice Principles*. Retrieved from Federal Trade Commission.

Goldie, L. (2009). *Twitter's rapid growth raises regulation issues*. Retrieved from Marketing week: http://www.marketingweek.co.uk/twitters-rapid-growth-raises-regulation-issues/2064439.article

Gross, R., & Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks (The Facebook Case). *ACM.*

Grubbs Hoy, M., & Phelps, J. (2003). Consumer Privacy and Security Protection on Church Web Sites: Reasons for Concern. *Journal of Public Policy & Marketing*.

Hagen, S., & Eika Sandes, F. (2011). Visual Scoping of Private Information Displayed on Shared Tabletop Surfaces. *Springer*.

Hagen, S., & Eika Sandnes, F. (2001). Visual scoping and personal space on shared tabletop surfaces. *Springer*.

Hancock, M., Vernier, F., Wigdor, D., Carpendale, S., & Shen, C. (2006). Rotations and Transitions for Tabletop Interactions. *IEEE*.

Harrison, C., Tan, D., & Morris, D. (2010). Skinput: Appropriating the Body as an Input Surface. *CHI*.

Incorporation, A. X. (2001). *The PIPEDA Privacy Principles.* Retrieved from Association Xpertise Incorporation: http://www.axi.ca/resdocs/privacy_guide.pdf

Kane, M., & Hines, M. (2005). *ChoicePoint faces inquiry, will curtail data sales*. Retrieved from CNet News: http://news.cnet.com/ChoicePoint-faces-inquiry,-will-curtail-data-sales/2100-1029_3-5599516.html

Kobsa, A. (2001). Tailoring Privacy to Users' Needs. Springer.

Kobsa, A. (2002). Personalized Hypermedia and International Privacy. ACM.

Krishnamurthy, B., & Wills, C. E. (2009). On the leakage of personnaly identifiable information via online social networks. *WOSN*. ACM.

Lee, J. C., Hudson, S. E., Summer, J. W., & Dietz, P. H. (2005). Moveable Interactive Projected Displays Using Projector Based Tracking. *UIST'05*. ACM.

Lippman, D. (2010). *Half of social networkers worried about privacy: poll*. Retrieved from Reuters: http://www.reuters.com/article/2010/07/15/us-internet-security-idUSTRE66E41820100715

Macavinta, C. (1999). *RealNetworks faced with second privacy suit*. Retrieved from CNet News: http://news.cnet.com/2100-1001-232766.html

Microsoft. (n.d.). *http://www.microsoft.com/presspass/presskits/surfacecomputing/gallery.mspx*. Retrieved from http://www.microsoft.com.

Norman, D. (1990). *The Design of Everyday Things.*

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. (n.d.). Retrieved from OECD: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html#part2

Office of the privacy commissioner of Canada. (2011). *Legal information related to PIPEDA*. Retrieved from Office of the privacy commissioner of Canada: http://www.priv.gc.ca/leg_c/p_principle_e.asp

Parker, J., Mandryk, R., & Inkpen, K. (2006). Integrating Point and Touch for Interaction with Digital Tabletop Displays. *IEE Computer Society*.

Patrick, A. S., & Kenny, P. (2003). From privacy legislation to internet design: Implementing information privacy in human-computer interaction. *PET*.

Peltonen, P., Kurvinen, E., Salovaara, A., Jacucci, G., Ilmonen, T., Evans, J., et al. (2008). "It's Mine, Don't Touch!": Interactions at a Large Multi-Touch Display in a City Centre. *CHI.*

Perlin, K., & Fox, D. (1993). Pad - An Alternate Approach to the Computer Interface. *ACM.*

Pinelle, D., Gutwin, C., & Greenberg, S. (2003). Task Analysis for Groupware Usability Evaluation: Modeling Shared-Workspace Tasks with the Mechanics of Collaboration. *TOCHI.* ACM.

Processing. (n.d.). *http://processing.org/*.

Scott, S. D., Grant, K. D., & Mandryk, R. L. (2003). System guidlines for co-located, collaborative work on a tabletop display. (pp. 159-178). ECSCW.

Scott, S. D., T. Carpendale, M. S., & Inkpen, K. M. (2004). *Exploring Casual Tabletop Interactions.* University of Calgary.

Seto, A. (2012). *Designing Discoverable Digital Tabletop Menus for Public Settings.*

Steel, E., & Vascellaro, J. (2010). *Facebook, MySpace Confront Privacy Loophole*. Retrieved from The Wall Street Journal: http://online.wsj.com/article/SB10001424052748704513104575256701215465596.html

Stutzman, F., & Kramer-Duffield, J. (2010). Friends Only: Examoning a Privacy-Enhancing Behavior in Facebook. *CHI.*

Thompson, J. J. (1973). In *Beyond Words: Nonverbal Communication in the Classroom.* MacMillan Publishing Company.

Weiser, M. (2002). The Computer for the 21st Century. *Pervasive Computing*.

Weiser, M., & Brown, J. S. (1996). The Coming Age of Calm Technology.

Westin, A. (1967). *Privacy and Freedom.* Atheneum.

Wickens, C. D., & Hollands, J. G. (2000). *Engineering Psychology and Human Performance.*

Wikiquote. (n.d.). *Privacy*. Retrieved from Wikiquote: http://en.wikiquote.org/wiki/Privacy

Won Gyun No, J. E. (August 25-27, 2009). Do Companies' Online Privacy Policy Disclosures Match Customer Needs? *Proceedings of the 2009 World Congress on Privacy, SEcurity, Trust and the Management of e-Business.* Saint John NB.

Wu, M., & Balakrishnan, R. (2003). Multi-Finger and Whole Hand Gestural Interaction. *UIST*.

Appendix I. Privacy Frameworks

OECD Privacy Framework[8]

Collection Limitation Principle

There should be limits to the collection of personal information with lawful and fair means and where possible with the consent of the data subject.

Data Quality Principle

Personal data that is being collected should be related to the specified purposes and to the extent sufficient for those purposes. It should be kept complete, accurate and up-to-date.

Purpose Specification Principle

The purpose of data collection should be specified before or at the time of data collection and the data usage should be limited to fulfilment of those specified purposes. If the purpose changed or expanded, first it should not be incompatible with the initial purposes and also it should be specifically mentioned what the changes are.

Use Limitation Principle

Collected personal data should not be disclosed to other parties or be used for purposes other than those specified except with the consent of the data subject or law authority.

Security Safeguards Principles

Reasonable security safeguards should be provided to protect personal data against destruction, unauthorized access or modification, loss etc.

[8] (Development, OECD Privacy Principles, 2010)

Openness Principle

There should be a general privacy policy available to the user about practices, policies with respect to personal information as well as the data controller's identity and usual residence.

Individual Participation Principle

An individual should have the right to challenge his or her personal information's existence and accuracy with no or minimal cost. If the challenge is successful his or her data should be erased, completed, or adjusted. If it is not successful and was denied there should be reasonable justifications and the user should have the right to challenge the denial as well.

Accountability Principle

A data controller should make necessary efforts to make sure the above principles are in effect.

PIPEDA Privacy Framework[9]

Accountability

An organization is responsible for the personal data in its possession including information transferred to a third party and shall protect this information with effective measures. There should be designated individual(s) accountable for the compliance of the organization with the following principles. Responding to complaints and inquiries are the organization's responsibility as well.

Identifying Purpose

[9] (Canada Department of Justice, 2012)

The purpose of the data collection shall be identified before or at the time of data collection and should be recorded for openness (Principle 8) and individual access (principle 9) policies. If a new purpose for the data is recognized, it should be identified before use and a new consent from the data subject is needed unless the new purpose is required by law.

Consent

For any collection, use and disclosure of personal data the knowledge and consent of the data subject is required unless there is law enforcement as in fraud protection programs. It should be in an understandable manner for the user and also clear about the purpose of data collection. Consent can have different forms depending on the type of information. An individual may withdraw consent at any time.

Limiting Collection

The collection of personal data shall be limited to the extent that is required for the identified purposes by fair and lawful means meaning that the user must not be misled and data collection should not be obtained through deception. The type of information being collected should be identified in privacy policy and practice that is available to the user to comply with openness (principle 8).

Limiting Use, Disclosure and Retention

Personal data shall not be used for purposes other than previously identified purposes or be disclosed to another party without the consent of the user as required by law. Personal data shall not be retained longer than the time required for fulfilling the purpose and there should be guidelines specifying the minimum and maximum retention period.

Accuracy

Personal Information should be as accurate, complete, and up-to-date as it is necessary to make appropriate decisions.

Safeguards

Depending on the sensitivity of the personal information, sufficient security safeguards should be provided against modification, unauthorized access, disclosure, etc. It might be in a form of physical methods such as restricting access to the office or organizational measures like security clearance or technological methods such as encryptions or passwords.

Also appropriate methods of protection should take place at the time of disposal or destruction of personal information.

Openness

An organization shall make its policies and practices regarding the management of personal information available to the users including type of information being kept and the means to access that information. This availability can be in different ways depending on some considerations such as having online access to it to be mailed to the requester.

Individual Access

Upon request, an individual should be informed about whether or not the organization holds, uses or disclosed any information about him or her and he or she should be able to challenge the accuracy and incompleteness of those data. If possible, any amendments made to the data, should be transferred to third parties having access to information in question.

Challenging Compliance

An individual should have the right to object to the compliance of the organization with the above principles and address the objection to the individual(s) accountable for it.

FTC Privacy Framework

Notice/Awareness

Notice means the entity's information practices should be made available to the user before collecting the information from them. The central principle of the FTC's FIP is Notice/Awareness because other principles are not meaningful if the user does not understand the policy and his or her rights. The types of information that the user must be given as part of the Notice/Awareness principle are as follows (Federal Trade Commission, Fair information Practice Principles):

- "Identification of the entity collecting the data;
- Identification of the uses to which the data will be put;
- Identification of any potential recipients of the data;
- The nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);
- Whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information; and
- The steps taken by the data collector to ensure the confidentiality, integrity and quality of the data. (Belloti, 1997)"

The entity's privacy policy should be easily available to the user (e.g. in a prominent location in the website) and should be understandable and clear.

Choice/Consent

Choice, as the second most important principle in this privacy framework, means giving the user options about how they want their personal information to be used especially in secondary uses other than those necessary for giving a complete service. For instance, giving users' information to third parties for marketing reasons is an external secondary use.

Traditionally there are two types of Choice/Consent methods: opt-in and opt-out. In opt-in the user gives his/her specific agreement about his/her information to be used for secondary purposes. Whereas, in opt-out the user takes affirmative steps to prevent the collection and use of his/her information. These options can be in the form of a general checkbox or more detailed specification regarding what information will be used for what other purposes.

Access/Participation

Access means a user's ability to review all the information collected about him/her as well as the ability to challenge incompleteness and inaccuracy of the information. Access should be reasonable time-wise and money-wise and there should be a mechanism to submit requests and objections.

Integrity/Security

Collectors must make sure that data are accurate and secure. As regards accuracy, they have to use reliable and cross-referencing sources against multiple sources and provide users access to data to verify their information. Regarding security, collectors should take managerial and technical measures to protect the data. They should limit the internal access to data and make sure no one can use the information for unauthorized purposes. They also must protect data against loss, unauthorized access, destruction, and unauthorized disclosure of data.

Enforcement/Redness

In order to make sure companies follow the FIP Principles, there should be enforcement measures. Without a firm enforcement mechanism, a privacy protection principle is merely suggestive rather that prescriptive. Among all enforcement approaches there are three redress mechanisms that are being used more commonly: self-regulation; legislations that create

private remedies for users; and government enforcements through civil and criminal sanctions.

a) Self-Regulation

Companies should have mechanisms to ensure compliance with the fair information practices such as external audits to ensure compliance, and membership in an industry association. Companies must assure there are means for users and consumers to complain and address their concerns. Also if any of the self-regulatory codes have been breached, there should be a solution for that such as a means for a user to correct the data or to be compensated for being harmed.

b) Private Remedies

The enactment of private remedies that provide private rights of action for users and consumers in case they are harmed by misuse of their personal information can be a strong motivation for data collectors to adopt fair information practices.

c) Government Enforcement

The third mechanism is government enforcement of fair information practices by means of civil or criminal penalties. To a certain extent this is the present state of enforcement in the US under US federal law. The US FTC imposes civil penalties including fine and imprisonment upon website operators who depart from their voluntarily adopted privacy policies (Connolly, 2004).

Appendix II. Facebook Statement Analysis

OECD & PIPEDA & FTC's FIP

Privacy Principles	Related Quotes From Facebook Privacy Policy[10]	
Collection Limitation/ **Limiting Collection/** **Notice and Awareness**	1.1	If you tag someone, that person and their friends can see your post no matter what audience you selected. The same is true when you approve a tag someone else adds to your post.
	1.2	When you comment on or "like" someone else's post, or write on their wall, that person gets to select the audience.
	1.3	Some types of posts are always public posts. As a general rule, you should assure that if you do not see a sharing icon, the information will be publicly available.
	1.4	Some types of posts are always public posts. As a general rule, you should assure that if you do not see a sharing icon, the information will be publicly available.
	1.5	Choose the public icon if you want to make something public. Choosing to make something public is exactly what it sounds like.it means that anyone, including people off of Facebook, will be able to see or access it.
	1.6	If you select "Only Me" as the audience for your friend list, but your friend sets her friend list to "Public", anyone will be able to see your connection on your friend's profile.
	1.7	If you choose to hide your gender, it only hides it on your profile.
	1.8	To make it easier for your friends to find you, we allow anyone with contact information (such as your email address and mobile number), to find you through Facebook search, as well as other tools we provide,

[10] (Facebook, 2012)

such as contact importers.

1.9 If you share your contact information (such as your email address or mobile number) with your friends, they may be able to use third party applications to sync that information with other address books, including ones on their mobile phones.

1.10 Some things (like your name and profile picture) do not have sharing icons because they are always publicly available. As a general rule you should assume that if you do not see sharing icon, the information will be publicly available.

1.11 If you do not want someone to tag you and they refused not to do so, you can block them. This will prevent them from tagging you going forward.

1.12 If you are tagged in a private space (such as a message or a group) only the people who can see the private space can see the tag. Similarly, if you are tagged in a comment, only the people who can see the comment can see the tag.

1.13 Because pages are public, information you share with a page is public information. This means, for example, that if you post a comment on a page, that comment can be used by the page owner off of Facebook, and anyone can see it.

1.14 When you “like” a page, you create a connection to that page. That connection is added to your profile and your friends may see it in their News Feeds.

1.15 Some pages contain content that comes directly from the page owner. Because this content comes directly from the page owner, that page may be able to collect information about you, just like any website.

1.16 We may receive information about you from the games, applications, and websites you use, but only when you have given the permission.

1.17 Facebook games, applications and websites are created and maintained by other business and developers who are not part of Facebook, so you should always make sure to read their term of service and privacy policies.

1.18 If the application needs additional information other than your public

		information and those you choose to make public, it will have to ask you for specific permission.
	1.19	Applications get your age range, locale, and gender when you and your friends visit them.
	1.20	Sometimes a game console, mobile phone, or other device might ask for permission to share specific information with the games and applications you use on that device (such as your public information). If you say okay, those applications will not be able to access any other information about you without asking specific permission from you or your friends.
	1.21	Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social.
	1.22	When you log in to a website using your Facebook, we give the site your User ID, but we do not share your email address or password with that website.
	1.23	If you make something public using a plugin, such a posting a public comment on a newspaper's website, then that website can access your comment (along with your User ID) just like everyone else.
	1.24	Websites that use social plugins can sometimes tell that you have engaged with the social plugin. For example, they may know that you clicked on a Like button in a social plugin.
	1.25	We receive data when you visit a site with a social plugin. We keep this data for 90 days. After that, we remove your name or any other personally identifying information from the data, or combine it with other people's data in a way that it is no longer associated with you.
	1.26	When you visit a site using instant personalization, it will know some information about you and your friends the moment you arrive. This is because instant personalization sites can access your User ID, your friends list, and your public information.
	1.27	The first time you visit an instant personalization site, you will see a notification letting you know that the site has partnered with Facebook to provide a personalized experience.

1.28 Instant personalization when you first visit the site. It also prevents from accessing any information about you until you or your friends visit the site.

1.29 If you turn public search setting off and then search for yourself on a public search engine, you may still see a preview of your profile. This is because some search engine cache information for a period of time.

1.30 When an advertiser creates an ad on Facebook, they are given the opportunity to choose their audience by location, demographics, likes, keywords, and any other information we receive or can tell about you and other users.

1.31 Many of the things you do on Facebook (like "liking" a Page) are posted to your Wall and shared in News Feed. But there's a lot to read in News Feed. That's why we allow people to "sponsor" your stories to make sure your friends see them. For example, if you RSVP to an event hosted by a local restaurant, that restaurant may want to make sure your friends see it so they can come too. If they do sponsor a story, that story will appear in the same place ads usually do under the heading "Sponsored Stories" or something similar. Only people that could originally see the story can see the sponsored story, and no personal information about you (or your friends) is shared with the sponsor.

1.32 We like to tell you about some of the features your friends use on Facebook to help you have a better experience. For example, if your friend uses our friend finder tool to find more friends on Facebook, we may tell you about it to encourage you to use it as well. This of course means you friend may similarly see suggestions based on the things you do. But we will try to only show it to friends that could benefit from your experience.

1.33 We may share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally

	recognized standards. 1.34 If you give us your password while using Facebook friend finder, we will delete it after you upload your friends' contact information. 1.35 Cookies are small pieces of data that we store on your computer, mobile phone or other device to make Facebook easier to use, make our advertising better, and to protect you (and Facebook). For example, we may use them to know you are logged in to Facebook, to help you use social plugins and share buttons, or to know when you are interacting with our advertising or Platform partners. We may also ask advertisers to serve ads to computers, mobile phones or other devices with a cookie placed by Facebook (although we would not share any other information with that advertiser) 1.36 Unless we make a change for legal or administrative reasons, or to correct an inaccurate statement, we will give you seven (7) days to provide us with comments on the change. If we receive more than 7000 comments concerning a particular change, we will put the change up for a vote. The vote will be binding on us if more than 30% of all active registered users as of the date of the notice vote.
Data Quality/ **Accuracy/** **Notice and Awareness**	2.1 Registration information are editable through "Account Setting". 2.2 Information shared by you can be edited or removed through the "Edit/Remove" button at the top-right corner of the story box. 2.3 You can control who can send you messages using your "How You Connect" settings. 2.4 You can control whether we suggest that another user tag you in a photo using the "How Tags work" setting. 2.5 You can control who can see the Facebook Pages you've "liked" by visiting your profile and clicking "Edit Profile". 2.6 Whenever you add thing to your profile you can select a specific audience, or even customize your audience. To do this, simply click on the sharing icon and choose who can see it. 2.7 The "Apps you use" setting lets you control the applications you use. You can see the permissions you have given these applications, as well

		as the last time an application accessed your information. You can also remove applications you no longer want, or turn off all platform application.
	2.8	You can download a copy of everything you've put into Facebook by visiting our "Account Setting" and clicking on "Download a copy of your Facebook data".
	2.9	We may send you notifications and other messages using the contact information we have for you, like your email address. You can control most of the notifications you receive, including ones from pages you like and applications you use, using your "Notifications" setting.
	2.10	If someone tags you in a post you can choose whether you want that post to appear on your profile. If you approve a post and later change your mind, you can remove it from your profile.
	2.11	Your Public Search setting controls whether people who enter your name on a public search engine may see your public profile (including in sponsored results). You can find your Public Search setting on the "Apps and Websites" setting page.
	2.12	If you decide that you do not want to experience instant personalization for all partner sites, you can disable instant personalization from the "Apps and Websites" settings page.
Purpose Specification/ Identifying Purpose/ Notice and Awareness	3.1	We use the information we receive about you with connection with the services and features we provide to you and other users like your friends, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use.
	3.2	Sometimes we get data from our advertising partners, customers and other third parties that help us (or them) deliver ads, understand online activity, and generally make Facebook better.
	3.3	Your birthday allows us to do things like show you age-appropriate content and advertisements.
	3.4	We may get your GPS location so we can tell you if any of your friends are nearby.
	3.5	An advertiser may tell us how you responded to an ad on Facebook or on

		another site in order to measure the effectiveness of-and improve the quality of those ads.
	3.6	We may put together data about you to determine which friends we should show you in your News Feed or suggest you tags in the photos you post.
	3.7	We may put together your current city with GPS and other location information we have about you to, for example, tell you and your friends about people or events nearby, or offer deals to you that you might be interested in.
	3.8	We may also put together data about you to serve you ads that might be more relevant to you.
	3.9	Granting us the permission to use the information we receive about you not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information.
	3.10	If you choose to hide your gender, it only hides it on your profile. This is because we just like the applications you and your friends use; need to use your gender to refer to you properly on the site.
	3.11	When you go to a game or application, or connect with a website using Facebook Platform, we give the game, application or website your User ID, as well as your friends' User IDs (or your friend list). Your friend list helps the application make your experience more social because it lets you find your friends on that application.
	3.12	Your User ID helps the application personalize your experience because it can connect your account on that application with your Facebook account, and it can access your public information. This includes information you choose to make public, as well as information that is always publicly available.
	3.13	Age range lets applications provide you with age-appropriate content. Locale lets applications know what language you speak. Gender lets applications refer to you correctly.
	3.14	One of your friends might want to use a music application that allows them to see what their friends are listening to. To get the full benefit of

that application, your friend would want to give the application her friend list that includes your User ID so the application knows which of her friends is also using it.

3.15 Instant personalization is a way for Facebook to help partner sites such as Bing and Rotten Tomatoes create a more personalized and social experience than a social plugin can offer.

3.16 When you visit and instant personalization site, we provide the site with your User ID and your friend list (as well as your age range, locale, and gender). The site can then connect your account on that site with your friends' accounts to make the site instantly social. The site can also access public information with any of the User IDs it receives, which it can use to make the site instantly personalized.

3.17 For example, if the site is a music site, it can access your music interests to suggest songs you may like, and access your friends' music interests to let you know what they are listening to. Of course it can only access you or your friends' music interests if they are public.

3.18 We like to tell you about some of the features your friends use on Facebook to help you have a better experience. For example, if your friend uses our friend finder tool to find more friends on Facebook, we may tell you about it to encourage you to use it as well. This of course means your friend may similarly see suggestions based on the things you do. But we will try to only show it to friends that could benefit from your experience.

3.19 Cookies are small pieces of data that we store on your computer, mobile phone or other device to make Facebook easier to use, make our advertising better, and to protect you (and Facebook). For example, we may use them to know you are logged in to Facebook, to help you use social plugins and share buttons, or to know when you are interacting with our advertising or Platform partners. We may also ask advertisers to serve ads to computers, mobile phones or other devices with a cookie placed by Facebook (although we would not share any other information with that advertiser).

3.20 We give your information to the people and companies that help us

	provide the services we offer. For example, we may use outside vendors to help host our website, serve photos and videos, process payments, or provide search results. In some cases we provide the service jointly with another company, such as the Facebook Marketplace. 3.21 Some types of posts are always public posts. As a general rule, you should assure that if you do not see a sharing icon, the information will be publicly available. 3.22 Your public information can show up when someone does a search on Facebook or on a public search engine 3.23 Your public information will be accessible to the games, applications, and websites you and your friends use. 3.24 Your public information will be accessible to anyone who uses our APIs such as our Graph API. 3.25 We give your information to the people and companies that help us provide the services we offer. For example, we may use outside vendors to help host our website, serve photos and videos, process payments, or provide search results. In some cases we provide the service jointly with another company, such as the Facebook Marketplace. 3.26 If you give us your password while using Facebook friend finder, we will delete it after you upload your friends' contact information. 3.27 We may also share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves and you from violations of our Statement of Rights and Responsibilities; and to prevent death or imminent bodily harm. 3.28 If the advertiser chooses to run the ad, we serve the ad to people who meet the criteria the advertiser selected, but we do not tell the advertiser who any of those people are. e ad runs, we provide advertisers with reports on how their ads performed. For example we give advertisers reports telling them how many users saw or clicked on their ads. But these reports are anonymous. We do not tell advertisers who saw or clicked on their ads.
Use Limitation/	4.1 We don't share information we receive about you with others unless we

Limiting Use, Disclosure and Retention/ **Choice and Consent**		have: received your permission, given you notice, such as by telling you about it in this policy; or removed your name or any other personally identifying information from it.
	4.2	If you tag someone, that person and their friends can see your post no matter what audience you selected. The same is true when you approve a tag someone else adds to your post.
	4.3	When you comment on or "like" someone else's post, or write on their wall, that person gets to select the audience.
	4.4	We only provide data to our advertising partners or customers after we have removed your name or any other personally indemnifying information from it, or have combined it with other people's data in a way that it is no longer associated with you.
	4.5	When others share information about you, they can also choose to make it public.
	4.6	Choose the public icon if you want to make something public. Choosing to make something public is exactly what it sounds like.it means that anyone, including people off of Facebook, will be able to see or access it.
	4.7	Choose "Friends" icon if you want things you added to your profile to be shared with your Facebook friends.
	4.8	Choose "Customize" icon if you want to customize your audience. You can also use this to hide the item on your profile from specific people.
	4.9	Your friend list is always available to the games, applications and websites you use no matter what audience you have chosen for your friend list. Your friendship may also be visible elsewhere such as your friends' profiles or searches.
	4.10	If you select "Only Me" as the audience for your friend list, but your friend sets her friend list to "Public", anyone will be able to see your connection on your friend's profile.
	4.11	If you share your contact information (such as your email address or mobile number) with your friends, they may be able to use third party applications to sync that information with other address books, including ones on their mobile phones.

	4.12	Some things (like your name and profile picture) do not have sharing icons because they are always publicly available. As a general rule you should assume that if you do not see sharing icon, the information will be publicly available.
	4.13	If you do not want someone to tag you and they refused not to do so, you can block them. This will prevent them from tagging you going forward.
	4.14	If you are tagged in a private space (such as a message or a group) only the people who can see the private space can see the tag. Similarly, if you are tagged in a comment, only the people who can see the comment can see the tag.
	4.15	Because pages are public, information you share with a page is public information. This means, for example, that if you post a comment on a page, that comment can be used by the page owner off of Facebook, and anyone can see it.
	4.16	If the application needs additional information other than your public information and those you choose to make public, it will have to ask you for specific permission.
	4.17	If you do not want applications to receive information about you, you can turn off all Facebook applications using your “Privacy Settings”.
	4.18	Sometimes a game console, mobile phone, or other device might ask for permission to share specific information with the games and applications you use on that device such as your public information). If you say okay, those applications will not be able to access any other information about you without asking specific permission from you or your friends.
	4.19	Instant personalization sites receive your User ID and friend list when you visit them.
	4.20	Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social.
	4.21	Your friends might want to share the music you “like” on Facebook. If you have made that information public, then the application can access it just like anyone else. But if you have shared your likes with just your friends, the application could ask your friend for permission to share

them.

4.22 You can control most of the information other people can share with application s from the “Apps and Website” settings page. But these controls do not let you limit access to your public information and friend list.

4.23 When you log in to a website using your Facebook, we give the site your User ID, but we do not share your email address or password with that website.

4.24 If you make something public using a plugin, such a posting a public comment on a newspaper’s website, then that website can access your comment (along with your User ID) just like everyone else.

4.25 When you visit a site using instant personalization, it will know some information about you and your friends the moment you arrive. This is because instant personalization sites can access your User ID, your friend list, and your public information.

4.26 The first time you visit an instant personalization site, you will see a notification letting you know that the site has partnered with Facebook to provide a personalized experience. The notification will give you the ability to disable or turn off instant personalization for that site. If you do that, that site is required to delete all of the information about you it received from Facebook. In addition, we will prevent that site from accessing your information in the future, even when your friends use that site.

4.27 If you turn off an instant personalization site after you have been using it or visited it a few times (or after you have given it specific permission to access you data, it will not automatically delete your data. But the site is contractually required to delete your data if you ask it to.

4.28 The partner is also contractually required not to use your User ID for a purpose (other than associating it with your account) until you and your friends visit the site.

4.29 If the instant personalization site wants any additional information, it will have to get your specific permission.

4.30 We do not share any of your information with advertisers (unless, of

course, you give us permission.)

4.31 Facebook Ads are sometimes paired with social actions your friends have taken. For example, an ad for a sushi restaurant may be paired with a news story that one of your friends likes that restaurant's Facebook page.

4.32 When you show up in one of these news stories, we will only pair it with ads shown to your friends. If you do not want to appear in stories paired with Facebook ads, you can opt out using your " Edit social ads" setting.

4.33 We may serve ads with social context (or serve just social context) on other sites. These work just like the ads we serve on Facebook-the advertisers do not receive any of your information.

4.34 We sometimes allow business or anyone else to sponsor stories like the ones that show up in your news Feed, subject to the audience set for that story. While these are sponsored, they are different from ads because they don't contain a message from the person that sponsored them. Your friends will see these stories even if you have opted out of the "Show my social actions in Facebook Ads" setting.

4.35 Your "Show my social action in Facebook Ads" setting does not control ads about Facebook's services and features.

4.36 Games, applications and websites can serve ads directly to you if they have your User ID.

4.37 Many of the things you do on Facebook (like "liking" a Page) are posted to your Wall and shared in News Feed. But there's a lot to read in News Feed. That's why we allow people to "sponsor" your stories to make sure your friends see them. For example, if you RSVP to an event hosted by a local restaurant, that restaurant may want to make sure your friends see it so they can come too. If they do sponsor a story, that story will appear in the same place ads usually do under the heading "Sponsored Stories" or something similar. Only people that could originally see the story can see the sponsored story, and no personal information about you (or your friends) is shared with the sponsor.

4.38 We like to tell you about some of the features your friends use on Facebook to help you have a better experience. For example, if your

		friend uses our friend finder tool to find more friends on Facebook, we may tell you about it to encourage you to use it as well. This of course means your friend may similarly see suggestions based on the things you do. But we will try to only show it to friends that could benefit from your experience.
	4.39	We may share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards.
	4.40	Unless we make a change for legal or administrative reasons, or to correct an inaccurate statement, we will give you seven (7) days to provide us with comments on the change. If we receive more than 7000 comments concerning a particular change, we will put the change up for a vote. The vote will be binding on us if more than 30% of all active registered users as of the date of the notice vote.
	5.1	If you do not want your information to be accessible through out APIs, you can turn off all platform applications from your Privacy Settings.
	5.2	Choose “Friends” icon if you want things you added to your profile to be shared with your Facebook friends.
	5.3	Choose “Customize” icon if you want to customize your audience. You can also use this to hide the item on your profile from specific people.
	5.4	Your friend list is always available to the games, applications and websites you use no matter what audience you have chosen for your friend list. Your friendship may also be visible elsewhere such as your friends’ profiles or searches.
	5.5	If you select “Only Me” as the audience for your friend list, but your friend sets her friend list to “Public”, anyone will be able to see your connection on your friend’s profile.
	5.6	If you choose to hide your gender, it only hides it on your profile.

Security Safeguard/ **Safeguards/** **Integrity and Security**	5.7	If someone tags you in a post you can choose whether you want that post to appear on your profile. If you approve a post and later change your mind, you can remove it from your profile.
	5.8	To make it easier for your friends to find you, we allow anyone with contact information (such as your email address and mobile number), to find you through Facebook search, as well as other tools we provide, such as contact importers.
	5.9	If you share your contact information (such as your email address or mobile number) with your friends, they may be able to use third party applications to sync that information with other address books, including ones on their mobile phones.
	5.10	Some things (like your name and profile picture) do not have sharing icons because they are always publicly available. As a general rule you should assume that if you do not see sharing icon, the information will be publicly available.
	5.11	If you do not want someone to tag you and they refused not to do so, you can block them. This will prevent them from tagging you going forward.
	5.12	If you are tagged in a private space (such as a message or a group) only the people who can see the private space can see the tag. Similarly, if you are tagged in a comment, only the people who can see the comment can see the tag.
	5.13	Your friends can add you to the groups they are in. you can always leave a group, which will prevent others from adding you to it again.
	5.14	When you “like” a page, you create a connection to that page. That connection is added to your profile and your friends may see it in their News Feeds.
	5.15	You can remove the pages you have “liked” from your profile.
	5.16	Some pages contain content that comes directly from the page owner. Because this content comes directly form the page owner, that page may be able to collect information about you, just like any website.
	5.17	Facebook games, applications and websites are created and maintained by other business and developers who are not part of Facebook, so you should always make sure to read their term of service and privacy

		policies.
	5.18	When you go to a game or application, or connect with a website using Facebook Platform, we give the game, application or website your User ID, as well as your friends' User IDs (or your friend list). Your friend list helps the application make your experience more social because it lets you find your friends on that application.
	5.19	If the application needs additional information other than your public information and those you choose to make public, it will have to ask you for specific permission.
	5.20	The "Apps you use" setting lets you control the applications you use. You can see the permissions you have given these applications, as well as the last time an application accessed your information. You can also remove applications you no longer want, or turn off all platform application.
	5.21	When you turn all platform applications off, your User ID is no longer given to applications, even when your friends use those applications. But you will no longer be able to use any games, applications or websites through Facebook.
	5.22	If you do not want applications to receive information about you, you can turn off all Facebook applications using your "Privacy Settings".
	5.23	Instant personalization sites receive your User ID and friend list when you visit them.
	5.24	Your friends and the other people you share information with often want to share your information with applications to make their experiences on those applications more personalized and social.
	5.25	Your friends might want to share the music you "like" on Facebook. If you have made that information public, then the application can access it just like anyone else. But if you have shared your likes with just your friends, the application could ask your friend for permission to share them.
	5.26	You can control most of the information other people can share with application s from the "Apps and Website" settings page. But these controls do not let you limit access to your public information and friend

list.

5.27 If you want to completely block applications from getting your information, you will need to turn off all platform applications. This means that you will no longer be able to use any games, applications or websites.

5.28 If an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission and no one else.

5.29 If you already have an account on a website, the site may be able to connect that account with your Facebook account. Sometimes it does this using what is called an “email hash”, which is similar to searching for someone on Facebook using an email address. Only the email addresses in this case are encrypted so no email addresses are actually shared between Facebook and the website.

5.30 When you log in to a website using your Facebook, we give the site your User ID, but we do not share your email address or password with that website

5.31 We receive data when you visit a site with a social plugin. We keep this data for 90 days. After that, we remove your name or any other personally identifying information from the data, or combine it with other people’s data in a way that it is no longer associated with you.

5.32 When you visit a site using instant personalization, it will know some information about you and your friends the moment you arrive. This is because instant personalization sites can access your User ID, your friend list, and your public information.

5.33 The first time you visit an instant personalization site, you will see a notification letting you know that the site has partnered with Facebook to provide a personalized experience. The notification will give you the ability to disable or turn off instant personalization for that site. If you do that, that site is required to delete all of the information about you it received from Facebook. In addition, we will prevent that site from accessing your information in the future, even when your friends use that site.

	5.34	If you decide that you do not want to experience instant personalization for all partner sites, you can disable instant personalization from the "Apps and Websites" settings page.
	5.35	If you turn off an instant personalization site after you have been using it or visited it a few times (or after you have given it specific permission to access you data, it will not automatically delete your data. But the site is contractually required to delete your data if you ask it to.
	5.36	To join the instant personalization program, a potential partner must enter into an agreement with us designed to protect your privacy. For example, this agreement requires that the partner delete your data if you turn off instant personalization when you first visit the site. It also prevent from accessing any information about you until you or your friends visit the site.
	5.37	Instant personalization partners sometimes use an email hash process to see if any of their users are on Facebook and get those users' User IDs. This process is similar to searching for someone of Facebook using an email address, except in this case the email addresses are encrypted so no actual email addresses are exchanged.
	5.38	The partner is also contractually required not to use your User ID for an purpose (other than associating it with your account) until you and your friends visit the site.
	5.39	When you visit and instant personalization site, we provide the site with your User ID and your friend list (as well as your age range, locale, and gender). The site can then connect your account on that site with your friends' accounts to make the site instantly social. The site can also access public information with any of the User IDs it receives, which it can use to make the site instantly personalized.
	5.40	For example, if the site is a music site, it can access your music interests to suggest songs you may like, and access your friends' music interests to let you know what they are listening to. Of course it can only access you or your friends' music interests if they are public.
	5.41	Your Public Search setting controls whether people who enter your name on a public search engine may see your public profile (including in

		sponsored results). You can find your Public Search setting on the "Apps and Websites" setting page.
	5.42	In the advertiser chooses to run the ad, we serve the ad to people who meet the criteria the advertiser selected, but we do not tell the advertiser who any of those people are.
	5.43	After the ad runs, we provide advertisers with reports on how their ads performed. For example we give advertisers reports telling them how many users saw or clicked on their ads. But these reports are anonymous. We do not tell advertisers who saw or clicked on their ads.
	5.44	We take safety issues very seriously, especially with children, and we encourage parents to teach their children about safe internet practices. To learn more visit our Safety Center.
	5.45	To protect minors, we may put special safeguards in place (such as placing restriction on the ability of adults to share and connect with them),, recognizing this may provide minors with a more limited experience on Facebook.
	5.46	Facebook complies with the EU Safe Harbor framework as set forth by the Department of Commerce regarding the collection, use and retention of data from European Union. As part of our participation in the safe Harbor, we agree to resolve all disputes you have with us in connection with our policies and practices through TRUSTe.
	5.47	If you give us your password while using Facebook friend finder, we will delete it after you upload your friends' contact information.
	5.48	We do our best to keep your information secure, but we need your help. For more detailed information about staying safe on Facebook, visit the Facebook Security page.
	5.49	Unless we make a change for legal or administrative reasons, or to correct an inaccurate statement, we will give you seven (7) days to provide us with comments on the change. If we receive more than 7000 comments concerning a particular change, we will put the change up for a vote. The vote will be binding on us if more than 30% of all active registered users as of the date of the notice vote.
	5.50	You can always remove or block cookies (such as by using the settings

		in your browser), but it may affect your ability to use Facebook. Learn more at: https://www.facebook.com/help/?page=176591669064814 .
	5.51	We offer tools to help you upload your friends' contact information so that you can find your friends on Facebook, and invite friends who do not use Facebook to join. If you do not want us to store this information, visit this help page at: https://www/facebook.com/contact_importer/remove_uploads.php
	5.52	If a user deceases we may close an account if we receive a formal request from the person's next of kin.
Openness/ **Openness /** **Access and Participation**	6.1	If you want to see information available about you throughout Graph API, just type https://graph.facebook.com/ [User ID or Username]?metadata=1 into your browser.
	6.2	Facebook games, applications and websites are created and maintained by other business and developers who are not part of Facebook, so you should always make sure to read their term of service and privacy policies.
	6.3	You can preview your public profile at: http://www.facebook.com/[Your Username or UserID]?p
	6.4	You can learn more about how to request a search engine to remove you from cached information at: http://www.facebook.com/help/?faq=13323
	6.5	Try this tool to see one of the was advertisers target ads and what information they see at: http://www.facebook.com/ads/create/
	6.6	Advertisers sometimes place cookies on your computer in order to make their ads more effective. Learn more at: http://networkadvertising.org/managing/opt_out.asp.
	6.7	Learn what happens when you click "Like" on an advertisement or an advertiser's Facebook Page at: https://www.facebook.com/help/?faq=19399
	6.8	We take safety issues very seriously, especially with children, and we encourage parents to teach their children about safe internet practices. To learn more visit our Safety Center.
	6.9	To view our certification of compliance with the EU Safe Harbor

		framework, visit the U.S Department of Commerce's Safe Harbor website at: https://safeharbor.export.gov/list.aspx.
	6.10	You can report a deceased person's profile at: https://www.facebook.com/help/contact.php?show_form=deceased .
	6.11	If we make changes to this Privacy Policy we will notify you by publication here and on the Facebook Site Governance Page. If the changes are material, we will provide you additional, prominent notice as appropriate under the circumstances. You can make sure that you receive notice directly by liking the Facebook Site Governance Page.
Individual Participation / Challenging Compliance/ Access and Participation	7.1	If you have given a game, application, or website permission to post information on your wall, you can remove it from your "Apps you use" setting.
	7.2	You can control who can send you messages using your "How You Connect" settings.
	7.3	You can control who can see the Facebook Pages you've "liked" by visiting your profile and clicking "Edit Profile".
	7.4	We provide initial responses to access requests within a reasonable period of time, typically within thirty days.
	7.5	You can download a copy of everything you've put into Facebook by visiting our "Account Setting" and clicking on "Download a copy of your Facebook data".
Accountability/ Accountability/ Notice and Awareness	8.1	If the ownership of our business changes, we may transfer your information to the new owner so they can continue to operate the services. But they will still have to honor the commitments we have made in this privacy policy.
	8.2	If you are a resident of or have your principal place of business in the US or Canada, this Statement is an agreement between you and Facebook, Inc. Otherwise, this Statement is an agreement between you and Facebook Ireland Limited. References to "us," "we," and "our" mean either Facebook, Inc. or Facebook Ireland Limited, as appropriate.
	8.3	This Statement makes up the entire agreement between the parties regarding Facebook, and supersedes any prior agreements.

Appendix III. Study Questionnaire

Pre-Study Questions

1. I am: ☐ Female ☐ Male

2. What is your age? Age_____

3. What discipline are you in?

□ Management Sciences □ Computer Science

□ Mechanical Other (Specify): _____

4. Do you have a Facebook account?

☐ Yes ☐ No

5. How familiar are you with privacy policies (Privacy regulations about gathering, use and disclosure of personal information)?

Very Unfamiliar	**Unfamiliar**	**Somewhat Unfamiliar**	**Neutral**	**Somewhat Familiar**	**Familiar**	**Very Familiar**
☐	☐	☐	☐	☐	☐	☐

6. Have you ever read the Facebook's privacy policy?

□ 1 - I have never read it before

□ 2 - I have glanced at it

□ 3 - I have read some parts of it

□ 4 - I have read it all

7. If you answered "Yes" to the above question, what was the level of your understanding?

□ I have not understood any of it.

□ I understood most of it but not all.

□ I have understood all of it.

8. Do you ever use Facebook collaboratively with your friends in public places (An example would be browsing pictures and checking news or events with your friends in a coffee shop or in a public library)?

☐ Yes ☐ No ☐Depends. Explain: _____

9. Has someone ever looked over your shoulder while you were using Facebook?

☐ Yes ☐No ☐Maybe, but I haven't noticed.

10. If you answered "Yes" to question 8, how many times per day/week/month/year (circle one) do you think you get shoulder-surfed? _____

Interview and Post-Task Questions

Task 1

Q1) What do you think the blurring technique you just used does?

_____

_____

Q2) Did you find the “Blur Messages” option easy to find?

☐ Yes ☐No ☐ I didn’t use it

Q3) If you answered “Yes” to the above question, how much did this feature make you aware of privacy threats in a public place on a scale of 1 to 5?

It had no effect on me ☐ ☐ **Neutral** ☐ ☐ ☐ **Made me Really Aware**

Q4) How much do you think the invisible touch is helpful to avoid information theft in public places on a scale of 1 to 7?

Not Helpful at all	Unhelpful	Somewhat Unhelpful	Neutral	Somewhat Helpful	Helpful	Very Helpful
□	□	□	□	□	□	□

Q5-Interview) How do you think this technique can be improved to give users more control over their personal information?

_____

_____

Task 2

Q6) What do you think the Passgesture does?

_____

_____

Q7) How much do you think the warning message was informative and helpful in understanding the situation on a scale of 1 to 7?

Not Helpful at all	Unhelpful	Somewhat Unhelpful	Neutral	Somewhat Helpful	Helpful	Very Helpful
□	□	□	□	□	□	□

Q8) How much did this feature make you aware and conscious of being in a public place and anticipated consequences of your decision on a scale of 1 to 5?

It had no effect on me ☐ **It had a little effect on me** ☐ **Neutral** ☐ **It had good effect on me** ☐ **Made me Really Aware** ☐

Q9) What did you think you have to do when you first saw the Passgesture area? (Affordance)

_____

_____

Q10) How much do you think the Passgesture is helpful to avoid information theft in public places on a scale of 1 to 7?

Not Helpful at all ☐ **Unhelpful** ☐ **Somewhat Unhelpful** ☐ **Neutral** ☐ **Somewhat Helpful** ☐ **Helpful** ☐ **Very Helpful** ☐

Q11-Interview) How do you think this technique can be improved to give users more control over their personal information?

_____

_____

Q12) The type of user agreement being presented in Task 2 is a short targeted type of user agreement called Just-in-time-click-through-agreement. How effective did you find this comparing to long user agreements on a scale of 1 to 7?

Not Effective at all	**Not Effective**	**Somewhat not Effective**	**Neutral**	**Somewhat Effective**	**Effective**	**Very Effective**
☐	☐	☐	☐	☐	☐	☐

Task 3

Q13) What do you think the slide-to-reveal message does?

_____

_____

Q14) Was the little “Slide to right” note on the message bar helpful in understanding what to do?

☐ Yes ☐No ☐Not Sure

Q15) How much do you think the warning message was helpful and informative about your decision and anticipated consequences on a scale of 1 to 7?

Not Helpful at all	**Unhelpful**	**Somewhat Unhelpful**	**Neutral**	**Somewhat Helpful**	**Helpful**	**Very Helpful**
☐	☐	☐	☐	☐	☐	☐

Q16) How effective was this feature in making you aware and conscious of being in a public place and the possible consequences of your decision on a scale of 1 to 5?

Not Effective at all	**Not Effective**	**Somewhat not Effective**	**Neutral**	**Somewhat Effective**	**Effective**	**Very Effective**
☐	☐	☐	☐	☐	☐	☐

Q17) What did you think you have to do when you first saw the slide-to-reveal technique area?

_____

_____

Q18) How helpful do you think the slide-to-reveal technique is to avoid information theft in public places on a scale of 1 to 7?

☐ **Not Helpful at all**

☐ **Unhelpful**

☐ **Somewhat Unhelpful**

☐ **Neutral**

☐ **Somewhat Helpful**

☐ **Helpful**

☐ **Very Helpful**

Q19-Interview) How do you think this technique can be improved to give users more control over their personal information?

_____

_____

Q20) On a scale of 1 to 7, how effective was the slide-to-reveal technique to make you read the warning message as opposed to lengthy user agreements we normally see?

☐ **Not Effective at all**

☐ **Not Effective**

☐ **Somewhat not Effective**

☐ **Neutral**

☐ **Somewhat Effective**

☐ **Effective**

☐ **Very Effective**

Task 4

Q21) How helpful were the arrows at the corner of the page in communicating that you can resize the page by pinching on a scale of 1 to 7?

☐ **Not Helpful at all**

☐ **Unhelpful**

☐ **Somewhat Unhelpful**

☐ **Neutral**

☐ **Somewhat Helpful**

☐ **Helpful**

☐ **Very Helpful**

Q22) What do you think the Semantic Zoom does?

_____

_____

Q23) How effective was this feature in making you aware and conscious of being in a public place and the possible consequences of your decision on a scale of 1 to 7?

☐ **Not Effective at all**

☐ **Not Effective**

☐ **Somewhat not Effective**

☐ **Neutral**

☐ **Somewhat Effective**

☐ **Effective**

☐ **Very Effective**

Q24) How helpful do you think the Semantic Zoom for users to control their personal information in public places on a scale of 1 to 7?

Not Helpful at all	Unhelpful	Somewhat Unhelpful	Neutral	Somewhat Helpful	Helpful	Very Helpful
☐	☐	☐	☐	☐	☐	☐

Q25-Interview) How do you think this technique can be improved to give users more control over their personal information?

_____

_____

Task 5

Q26) What do you think the red triangle does?

_____

_____

Q27) What do you think the red border does?

_____

_____

Q28) Did you notice the red triangle appeared when I started using the table?

☐ Yes ☐No ☐Not Sure

Q29) If you answered “Yes” to the above question, how effective do you think this technique is in making users more conscious when another person starts using the same table in a public setting on a scale of 1 to 7?

Not Effective at all	**Not Effective**	**Somewhat not Effective**	**Neutral**	**Somewhat Effective**	**Effective**	**Very Effective**
☐	☐	☐	☐	☐	☐	☐

Q30) Did you notice the “Log off” button at the top right corner of the page?

☐ Yes ☐No ☐Not Sure

Q31) If you answered “Yes” to the above question, how effective do you think the design and placement of the “Log off” button was in making the user more aware about logging off their Facebook account on the digital tabletop in a public setting on a scale of 1 to 7?

Not Effective at all	**Not Effective**	**Somewhat not Effective**	**Neutral**	**Somewhat Effective**	**Effective**	**Very Effective**
☐	☐	☐	☐	☐	☐	☐

Q32) On a scale of 1 to7, how effective do you think the pop-up menu was in giving you control over how to share your personal information?

Not Effective at all	**Not Effective**	**Somewhat not Effective**	**Neutral**	**Somewhat Effective**	**Effective**	**Very Effective**
☐	☐	☐	☐	☐	☐	☐

Q33-Interview) How do you think this technique can be improved to give users more control over their personal information?

_____

_____

Appendix IX. Statistical Calculations

Q2)

Descriptive statistics for Q2

	N	Minimum	Maximum	Mean	Std. Deviation
Q2	10	0	2	.90	.738
Valid N (listwise)	10				

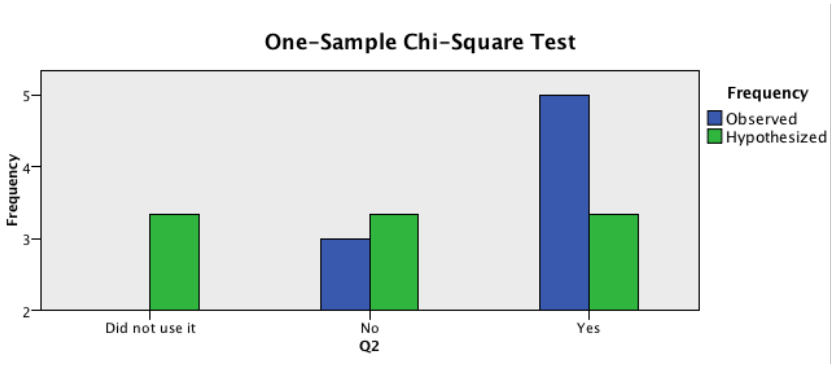
Frequency statistics for Q2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	3	30.0	30.0	30.0
	Yes	5	50.0	50.0	80.0
	Did not use it	2	20.0	20.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q2

	Null Hypothesis	Test	Sig.	Decision
1	The categories of Q2 occur with equal probabilities.	One-Sample Chi-Square Test	.497	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Chi-Square test for Q2

Q3)

Descriptive statistics for Q3

	N	Minimum	Maximum	Mean	Std. Deviation
Q3	5	3	4	3.60	.548
Valid N (listwise)	5				

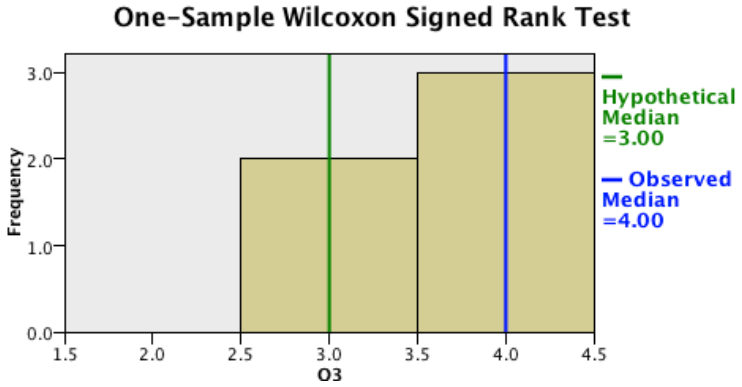
Frequency statistics for Q3

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	2	20.0	40.0	40.0
	Good Effect	3	30.0	60.0	100.0
	Total	5	50.0	100.0	
Missing	System	5	50.0		
Total		10	100.0		

Hypothesis test summary for Q3

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q3 equals 3.00.	One-Sample Wilcoxon Signed Rank Test	.083	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q3

Q4)

Descriptive analysis for Q4

	N	Minimum	Maximum	Mean	Std. Deviation
Q4	10	4	7	6.00	.943
Valid N (listwise)	10				

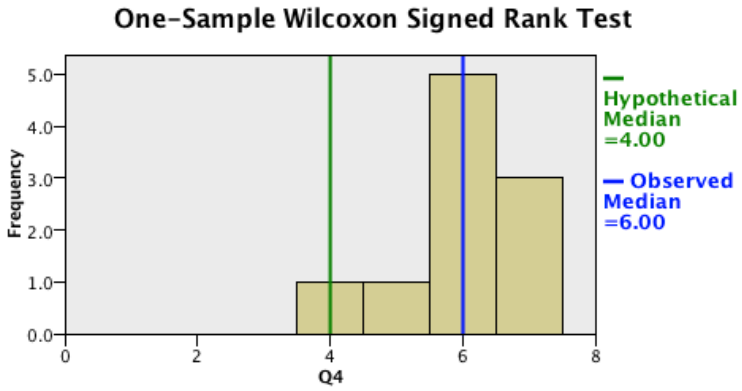
Frequency analysis for Q4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	1	10.0	10.0	10.0
	Somewhat helpful	1	10.0	10.0	20.0
	Helpful	5	50.0	50.0	70.0
	Very helpful	3	30.0	30.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q4

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q4 equals 4.00.	One-Sample Wilcoxon Signed Rank Test	.006	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q4

Q7)

Descriptive analysis for Q7

	N	Minimum	Maximum	Mean	Std. Deviation
Q7	10	4	7	5.30	.949
Valid N (listwise)	10				

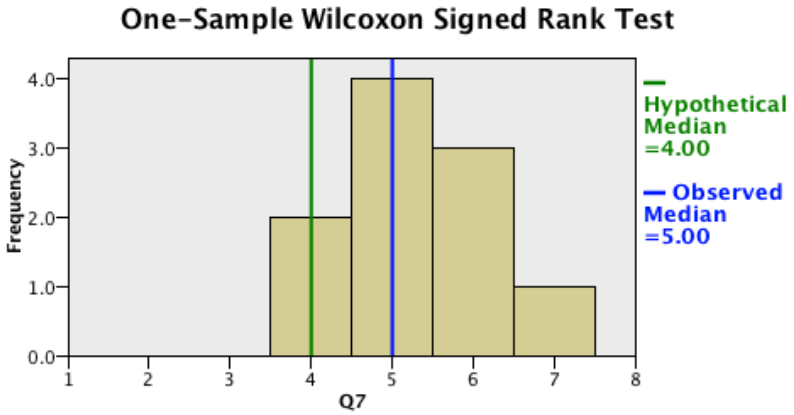
Frequency analysis for Q7

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	2	20.0	20.0	20.0
	Somewhat helpful	4	40.0	40.0	60.0
	Helpful	3	30.0	30.0	90.0
	Very helpful	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q7

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q7 equals 4.00.	One-Sample Wilcoxon Signed Rank Test	.010	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q7

Q8)

Descriptive analysis for Q8

	N	Minimum	Maximum	Mean	Std. Deviation
Q8	10	2	5	3.70	.949
Valid N (listwise)	10				

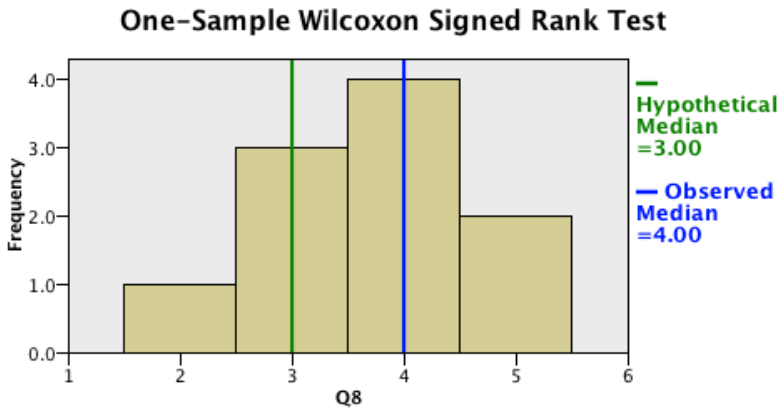
Frequency analysis for Q8

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Little Effect	1	10.0	10.0	10.0
	Neutral	3	30.0	30.0	40.0
	Good Effect	4	40.0	40.0	80.0
	Made really aware	2	20.0	20.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q8

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q8 equals 3.00.	One-Sample Wilcoxon Signed Rank Test	.053	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Chi-Square test for Q8

Q10)

Descriptive analysis for Q10

	N	Minimum	Maximum	Mean	Std. Deviation
Q10	10	2	7	5.10	1.595
Valid N (listwise)	10				

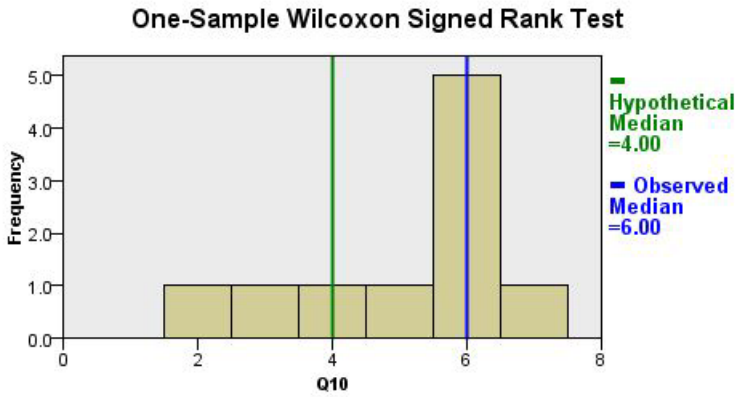
Frequency analysis for Q10

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Unhelpful	1	10.0	10.0	10.0
	Somewhat unhelpful	1	10.0	10.0	20.0
	Neutral	1	10.0	10.0	30.0
	Somewhat helpful	1	10.0	10.0	40.0
	Helpful	5	50.0	50.0	90.0
	Very helpful	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q10

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q10 equals 4.00.	One-Sample Wilcoxon Signed Rank Test	.058	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q10

Q12)

Descriptive analysis for Q12

	N	Minimum	Maximum	Mean	Std. Deviation
Q12	10	4	7	5.30	1.252
Valid N (listwise)	10				

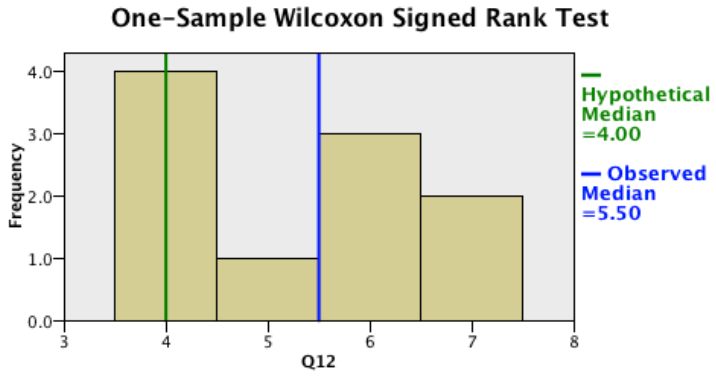
Frequency analysis for Q12

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	4	40.0	40.0	40.0
	Somewhat Effective	1	10.0	10.0	50.0
	Effective	3	30.0	30.0	80.0
	Very Effective	2	20.0	20.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q12

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q12 equals 4.00.	One-Sample Wilcoxon Signed Rank Test	.026	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q12

Q14)

Descriptive analysis for Q14

	N	Minimum	Maximum	Mean	Std. Deviation
Q14	10	1	3	1.20	.632
Valid N (listwise)	10				

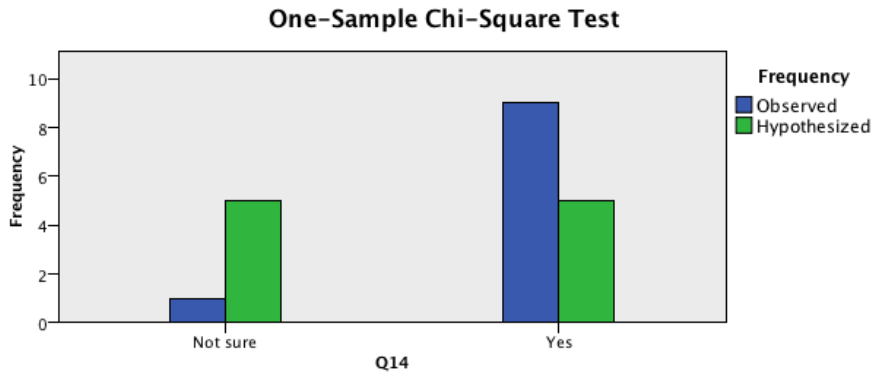
Frequency analysis for Q14

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	9	90.0	90.0	90.0
	Not sure	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q14

	Null Hypothesis	Test	Sig.	Decision
1	The categories of Q14 occur with equal probabilities.	One-Sample Chi-Square Test	.011	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Chi-Square test for Q14

Q15)

Descriptive analysis for Q15

	N	Minimum	Maximum	Mean	Std. Deviation
Q15	10	4	7	6.20	1.033
Valid N (listwise)	10				

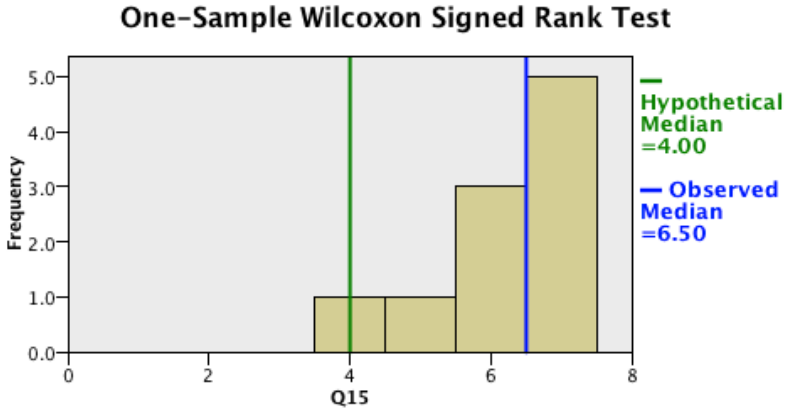
Frequency analysis for Q15

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	1	10.0	10.0	10.0
	Somewhat helpful	1	10.0	10.0	20.0
	Helpful	3	30.0	30.0	50.0
	Very helpful	5	50.0	50.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q15

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q15 equals 4.00.	One-Sample Wilcoxon Signed Rank Test	.006	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q15

Q16)

Descriptive analysis for Q16

	N	Minimum	Maximum	Mean	Std. Deviation
Q16	10	5	7	6.20	.919
Valid N (listwise)	10				

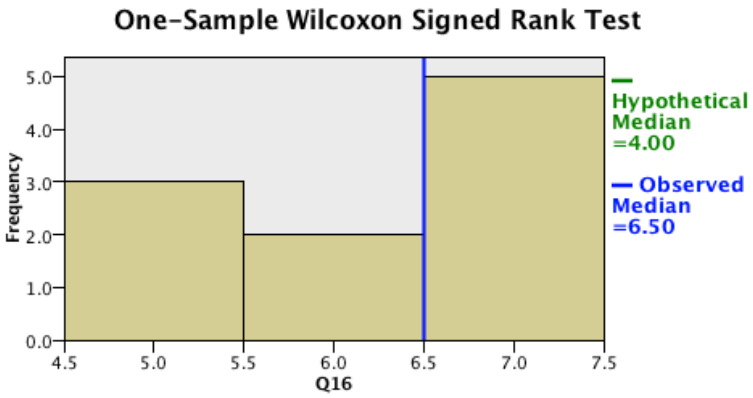
Frequency analysis for Q16

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somewhat Effective	3	30.0	30.0	30.0
	Effective	2	20.0	20.0	50.0
	Very Effective	5	50.0	50.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q16

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q16 equals 4.00.	One-Sample Wilcoxon Signed Rank Test	.004	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q16

Q18)

Descriptive analysis for Q18

	N	Minimum	Maximum	Mean	Std. Deviation
Q18	10	4	7	5.70	1.160
Valid N (listwise)	10				

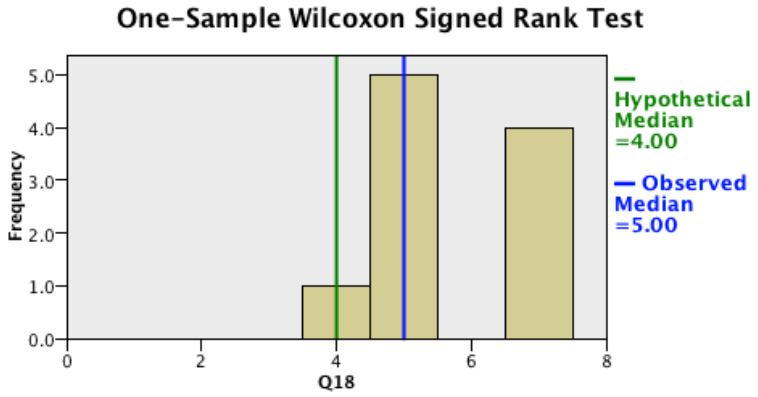
Frequency analysis for Q18

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	1	10.0	10.0	10.0
	Somewhat helpful	5	50.0	50.0	60.0
	Very helpful	4	40.0	40.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q18

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q18 equals 4.00.	One-Sample Wilcoxon Signed Rank Test	.006	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q18

Q20)

Descriptive analysis for Q20

	N	Minimum	Maximum	Mean	Std. Deviation
Q20	10	4	7	6.40	.966
Valid N (listwise)	10				

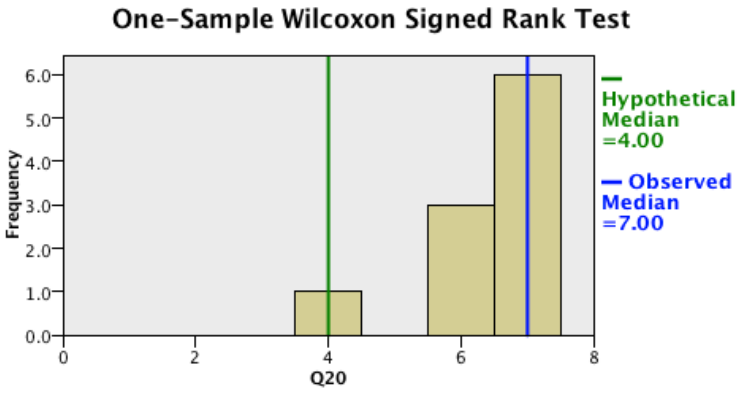
Frequency analysis for Q20

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	1	10.0	10.0	10.0
	Effective	3	30.0	30.0	40.0
	Very Effective	6	60.0	60.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q20

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q20 equals 4.00.	One-Sample Wilcoxon Signed Rank Test	.006	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q20

Q21)

Descriptive analysis for Q21

	N	Minimum	Maximum	Mean	Std. Deviation
Q21	10	1	6	3.40	2.066
Valid N (listwise)	10				

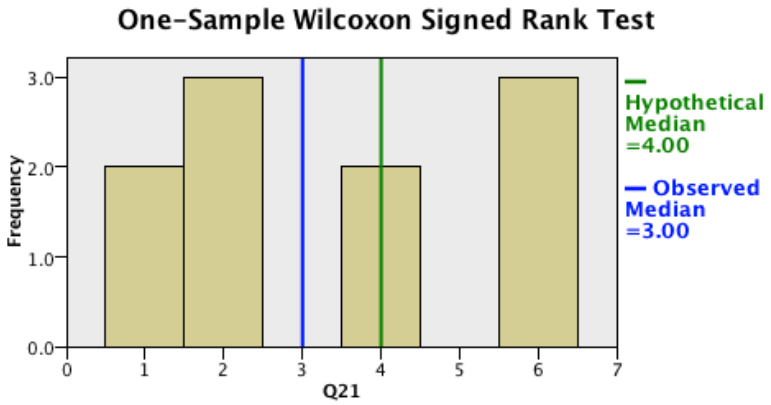
Frequency analysis for Q21

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No helpful at all	2	20.0	20.0	20.0
	Unhelpful	3	30.0	30.0	50.0
	Neutral	2	20.0	20.0	70.0
	Helpful	3	30.0	30.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q21

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q21 equals 4.00.	One-Sample Wilcoxon Signed Rank Test	.271	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q21

Q23)

Descriptive analysis for Q23

	N	Minimum	Maximum	Mean	Std. Deviation
Q23	10	2	6	4.00	1.333
Valid N (listwise)	10				

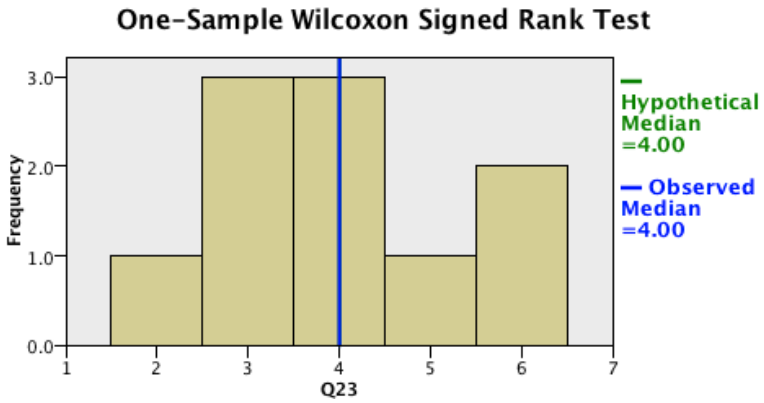
Frequency analysis for Q23

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not Effective	1	10.0	10.0	10.0
	Somewhat not effective	3	30.0	30.0	40.0
	Neutral	3	30.0	30.0	70.0
	Somewhat effective	1	10.0	10.0	80.0
	Effective	2	20.0	20.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q23

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q23 equals 4.00.	One-Sample Wilcoxon Signed Rank Test	.931	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q23

Q24)

Descriptive analysis for Q24

	N	Minimum	Maximum	Mean	Std. Deviation
Q24	10	1	7	4.70	1.767
Valid N (listwise)	10				

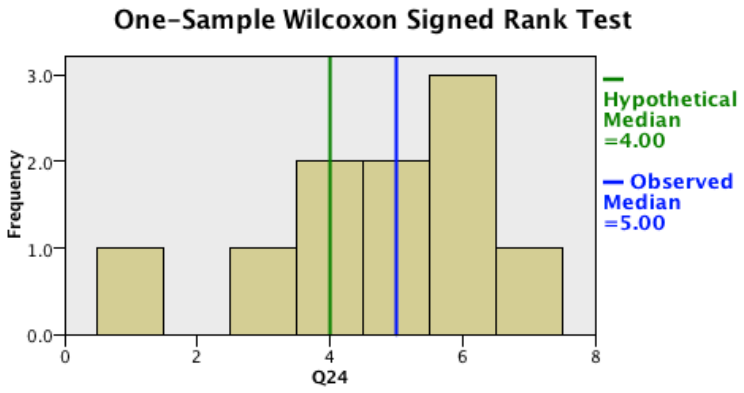
Frequency analysis for Q24

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No helpful at all	1	10.0	10.0	10.0
	Somewhat unhelpful	1	10.0	10.0	20.0
	Neutral	2	20.0	20.0	40.0
	Somewhat helpful	2	20.0	20.0	60.0
	Helpful	3	30.0	30.0	90.0
	Very helpful	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q24

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q24 equals 4.00.	One-Sample Wilcoxon Signed Rank Test	.229	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q24

Q28)

Descriptive analysis for Q28

	N	Minimum	Maximum	Mean	Std. Deviation
Q28	10	0	2	.80	.789
Valid N (listwise)	10				

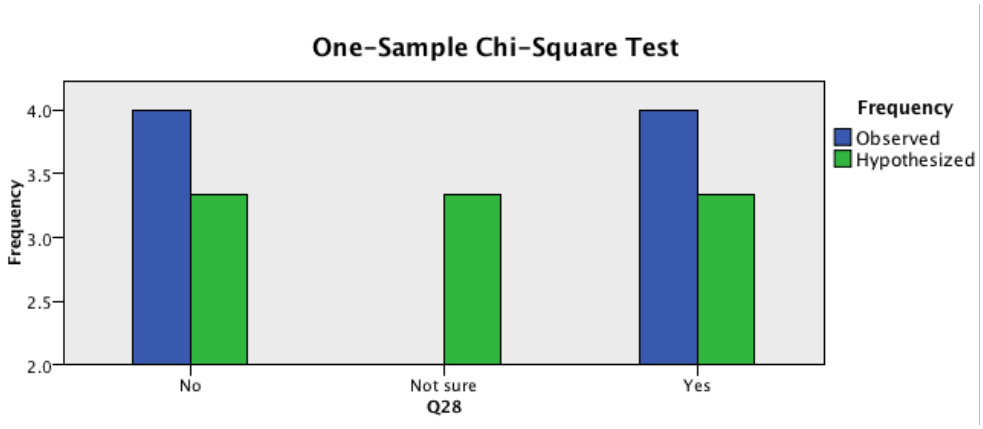
Frequency analysis for Q28

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	4	40.0	40.0	40.0
	Yes	4	40.0	40.0	80.0
	Not sure	2	20.0	20.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q28

	Null Hypothesis	Test	Sig.	Decision
1	The categories of Q28 occur with equal probabilities.	One-Sample Chi-Square Test	.670	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Chi-Square test for Q28

Q29)

Descriptive analysis for Q29

	N	Minimum	Maximum	Mean	Std. Deviation
Q29	4	5	7	6.25	.957
Valid N (listwise)	4				

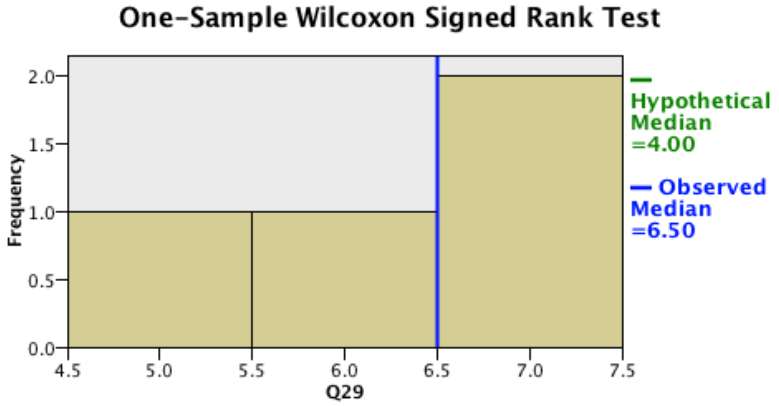
Frequency analysis for Q29

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Somewhat Effective	1	10.0	25.0	25.0
	Effective	1	10.0	25.0	50.0
	Very Effective	2	20.0	50.0	100.0
	Total	4	40.0	100.0	
Missing	System	6	60.0		
Total		10	100.0		

Hypothesis test summary for Q29

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q29 equals 4.00.	One-Sample Wilcoxon Signed Rank Test	.066	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q29

Q30)

Descriptive analysis for Q30

	N	Minimum	Maximum	Mean	Std. Deviation
Q30	10	1	1	1.00	.000
Valid N (listwise)	10				

Frequency analysis for Q30

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	10	100.0	100.0	100.0

Q31)

Descriptive analysis for Q31

	N	Minimum	Maximum	Mean	Std. Deviation
Q31	10	4	7	5.90	.876
Valid N (listwise)	10				

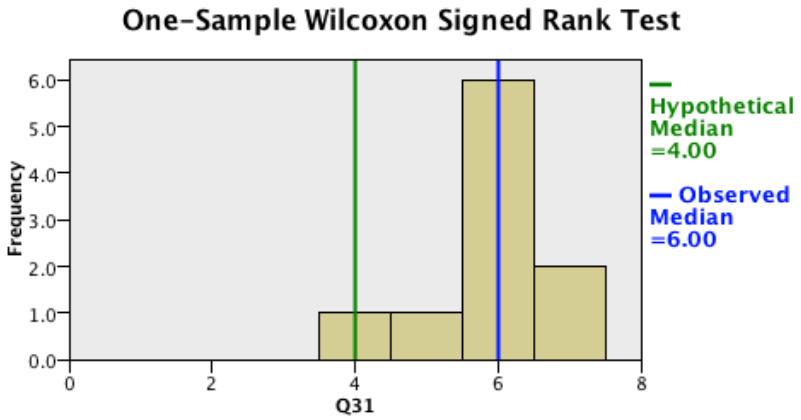
Frequency analysis for Q31

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	1	10.0	10.0	10.0
	Somewhat Effective	1	10.0	10.0	20.0
	Effective	6	60.0	60.0	80.0
	Very Effective	2	20.0	20.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q31

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q31 equals 4.00.	One-Sample Wilcoxon Signed Rank Test	.006	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q31

Q32)

Descriptive analysis for Q32

	N	Minimum	Maximum	Mean	Std. Deviation
Q32	10	4	7	5.30	.823
Valid N (listwise)	10				

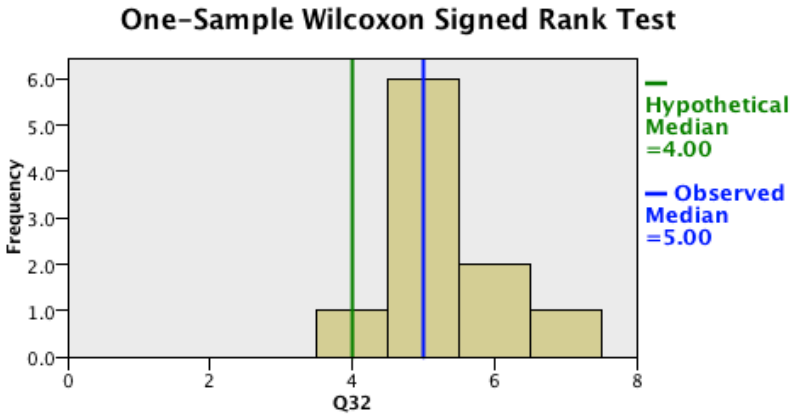
Frequency analysis for Q32

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Neutral	1	10.0	10.0	10.0
	Somewhat effective	6	60.0	60.0	70.0
	Effective	2	20.0	20.0	90.0
	Very Effective	1	10.0	10.0	100.0
	Total	10	100.0	100.0	

Hypothesis test summary for Q32

	Null Hypothesis	Test	Sig.	Decision
1	The median of Q32 equals 4.00.	One-Sample Wilcoxon Signed Rank Test	.006	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.



Descriptive chart for One-Sample Wilcoxon Signed Rank test for Q32

Appendix X. Interview Scripts

Participants 1:

Task 1: A smart feature that can identify and search for words such as telephone number. If the first time we search for the message the whole message is blurry, there might be difficulties finding the information we are looking for. An algorithm to find some non-confidential words and make them visible so that we can easier find the needed information

Task 2: Instead of the passgetsure pattern we could ask user to write the word Cautious or Warning for example so that even if the user skipped reading the warning message, there will be still a good chance they become more aware about what they are doing.

Task 3: It did its job very well. It made me read the whole message. The fact that I had to reveal the message line by line made me read all of it. But we have to make sure it does not take a long time otherwise users' will be frustrated especially users that are not familiar with these types of techniques.

Task 4: It is hard for user to know what to do. Although I have noticed the arrows at the corner I didn't think doing gestures like pinching will change the level of presentation because I was not familiar with it before. If user can be informed about it, it may become more common in different applications.

Task 5: I didn't know what to do exactly and it could have been nice if some information were available about each of those option so that user does not press them accidently. For example it can be that when you keep your finger on any of the options a message appears

explaining thing and then when we pushed it, it asks whether we are sure to do that. Also it would have been good to be able to only share specific things like only a picture instead of the whole page.

Participant 2:

Task 1: I didn't know about the feature and if there were a warning message for example that such an option is available it would have been easier for me to locate the option. Also pop-up message can be frustrating some times but it would be more beneficial.

Task 2: The only thing I can say is that because I was familiar with this technique similar to Android phones, I just made the pattern without reading the message.

Task 3: The font of the text was not eye-catching but the technique was new for me and attracted me more. I read the whole message whereas the first one I just skipped it.

Task 4: I noticed the arrows but I didn't wan to use it because I thought it is going to make the screen bigger and I didn't wan to do that because the small screen was giving me more privacy.

Task 5: I only think options can be visible from the beginning and not to be that I have to discover them

Participant 3:

Task 1: I think it should have been activated by default so that user won't enter into the message accidently with having everything revealed. And if the user didn't want to blur the message they can deactivate the feature. This would be safer.

Task 2: Making that gesture made me read the text and if it was only an Okay button I would possibly won't read the message. It could be also that instead of making the gesture the user has to write a word. Because if users get used to it they can skip reading the message and just make a gesture.

Task 3: The problem was that the lines didn't have any order and I started reading form the last line. Or something like the first line is darker and it gets lighter from line to line. It gets more user-friendly that way.

Task 4: At first place it wasn't clear for me there is a zooming feature. There should be a message or something telling the user there is such an option available. The arrows were small and were not noticeable. Again I think there should be a message saying there is a zooming option available for you.

Task 5: I didn't notice when the red triangle appeared and I didn't use it. Again I think a message or a sound would be beneficial to notice. Although the message might be bothering but it can be an option to be shown only the first time and the user can set it not to appear the next time.

Participant 4:

Task 1: I think the main problem is that if you blur the text how you can find the information. If there was a fast way of revealing the message user can search for the information easier.

Task 2: I think this task was totally okay and I had no problem with it.

Task 3: At the beginning it was a little bit confusing but then I liked it and made me read the whole message. Whereas in task 2 I did not read the whole message.

Task 4: If there were some hints available to tell the user what option is available and how to use it would have been better especially for the user who is not familiar with this technique. The arrows were too small.

Task 5: Actually nothing comes to my mind

Participant 5:

Task 1: This technique was very interesting for me. Because I am very worried about my information and if I were to use it in a shopping mall I definitely wanted to have such a

feature available.

Task 2: I read the message. It was a little confusing for me and I prefer putting the password of my account rather having challenging stuff.

Task 3: It was time-consuming and I like the previous technique although I read the message in both tasks.

Task 4: I noticed the arrows but I didn't know what that means. I don't have experience using these devices. Normally if I have something very confidential, I would not check it in public and rather go to a private place.

Task 5: I think having a hardware shelter around the table would be beneficial so that not every one can easily see my information and I prefer not to use my sensitive information in public.

Participant 6:

Task 1: It would be better to have a message or comment to give some idea what to do like "Touch any sentence to see it". Because many users like me are typical people with not so much technology experience.

Task 2: I am a conservative person and don't want my information to be visible. Therefore this technique was not advantageous to me because I never choose to for example switch to classic Facebook website.

Task 3: Because it was the first time I read the whole message but if I get used to it I may just slide the bars rapidly and press okay.

Task 4: When I started using this technique because I did not know what to do the arrows meant nothing for me. If the figure of the arrows would change to something else such as a picture of 2 fingers, it would be more informative.

Task 5: About the log of button, I saw it but I did not pay attention or thought about using it. I also did not notice the red border. When you joined me and I shared my page with you at

the table I was worried about you seeing my information and the first thing came to my mind was retrieving the page instead of logging off. It would be better to make it more noticeable somehow.

Participant 7:

Task 1: I saw the whole message before blurring it. If I haven't seen it would be difficult for me to find the information and had to go back and forth to figure it out.

Task 2: When I saw that page I felt like I am in a wrong place and it is going to ask me to log in again. It would have been nice if as soon as I entered the page a message pops up saying you are entering into a new area and we need another authentication or consent.

Task 3: I think that this method was new made me read the whole message for the first time. But if I am going to use it in future I won't read it any more and will know I just have to slide bars. Maybe coming up wit a new idea every time would be a solution.

Task 4: If the arrows were in different color or bigger it would be better. Also a small notice that you can pinch to zoom in or zoom back will also be helpful.

Task 5: I did not notice the border but I did notice the red triangle and when it appeared and made me curious. The log off button I noticed but it was not eye-catching. It was better if it was in different color. However, I still don't think I would work with my sensitive information in public places because I still think people cans see it. Also I really liked to be able to resize my page.

Participant 8:

Task 1: It would be better to have a search tool so that if the user searches the telephone number, the number appears.

Task 2: It is easier to put in a pin code instead of a pattern.

Task 3: I really liked this technique better than the previous one and it made me read the whole message.

Task 4: I first thought it would change the font size and make it harder for people to see it.

Task 5: I didn't notice the red triangle. If it had something like an exclamation mark it would be more noticeable.

Participant 9:

Task 1: The problem was that if I had not seen the message I could not locate the telephone number. If there was a option to differentiate letters form numbers it would be helpful.

Task 2: No specific suggestion comes to my mind.

Task 3: The warning was stronger so I was not sure to press the okay button. I think if it had a back button it would be useful.

Task 4: I like the technique a lot but I really did not get how it is going to help.

Task 5: My concern is that what if I choose one of the options unintentionally. I was curious to see what it happens but you may not have been my friend. If it were a describing message about the feature it would be better.

Participant 10:

Task 1: Since I assumed I am in a public place I think the message should have been blurred by default but then I would have some problem finding information. Maybe having a search option looking up for numbers or keywords would be helpful.

Task 2: I didn't read the message and I do have Android cellphone. I normally click on buttons automatically and okay it and skip the message.

Task 3: In this task I read the whole message. I am not very worried about privacy stuff and I found these technologies annoying. Also the sliding bar was a little tricky because it didn't go all the way to the back and the okay button didn't become activated although I read the whole message.

Task 4: It took me a while to notice the arrows. If they were a little bit bigger it would be better. Also it might have been because I have never seen it before. I needed some transition to tell me the page is changing. It was not obvious to me.

Task 5: I noticed the triangle appeared when you joined the table. If someone sitting there I knew they can see my stuff and I didn't need a notifier. If it is really confidential it shouldn't be accessed in a public device.