EXPLORING EVERYDAY PRIVACY BEHAVIORS AND MISCLOSURES

A Dissertation
Presented to
The Academic Faculty

by

Kelly Caine

In Partial Fulfillment
of the Requirements for the Degree
Ph.D. in the
School of Psychology

Georgia Institute of Technology

EXPLORING EVERYDAY PRIVACY BEHAVIORS AND MISCLOSURES

Committee:

Dr. Dr. Arthur D. Fisk, Advisor
School of Psychology
Georgia Institute of Technology

Dr. Wendy A. Rogers
School of Psychology
Georgia Institute of Technology

Dr. Richard Catrambone
School of Psychology
Georgia Institute of Technology

Dr. James Foley
School of Interactive Computing
Georgia Institute of Technology

Dr. Robin Jeffries
Quantitative User Research
Google

Date Approved: December, 2009

To Mom and Dad

ACKNOWLEDGEMENTS

I would like to thank Dan Fisk and Wendy Rogers for supporting my research and teaching me how to be a researcher. I would also like to thank the other members of my committee, Robin Jeffries, Jim Foley, and Richard Catrambone for their guidance and encouragement. The members of the HFA lab, especially Anne Adams, Tim Nichols, Jamye Hickman, Aideen Stronge, Julian Sanchez, Travis Bowles, Anne McLaughlin, Rick Pak, Marita O'Brien, Alan Poole, Michelle Kwasny, Kaylee Burnham, and Rachael Stewart also deserve thanks. Many others have helped me during my time at Georgia Tech including Jan Westbrook, Anderson Smith, Mike Best, Dianne Leader, Fredda Blanchard-Fields, Beth Mynatt, Gregory Abowd, Bruce Walker, and Jack Feldman. From Google, where I learned to love my job, I would like to thank Antonella Pavese, Molly Stevens, Kathi Baxter, Richard Boardman, and Stephanie Jacobs.

I have also been fortunate to have been supported by many outside of my professional circle. I would especially like to thank my mother and father who have always encouraged and supported me. Other members of my family I would like to express special gratitude to are Cousin Ward, who helped copy edit this document, Uncle Woody, who helped me with my application to grad school, my brother Matt, my Stepmother Debbie, and my sisters Katie and RaeAnn. I also wish to thank a few of the friends who made grad school fun: Kurt Luther, Karen Williams, Nick Diakopoulos, Nikolaos Vasiloglou, Eugene Medynskiy, Lana Yarosh, Jennifer Ward, Jenn Thom-Santelli, Marc Grootjen, Caroline Korn, and Jamie Mneimneh. I would also like to thank Bill Russell, Boo Duncan and Janet Brown for coaching me in riding and in life. Finally, I would like to thank Jim Evans, Virginia Scotchie, David Clement, and Mac McClure for encouraging me to apply for graduate school and to Kay Connelly, for providing a delightful motivation to finish. Thank you all.

TABLE OF CONTENTS

Page

ACKNOWLEDGEMENTS iv

LIST OF TABLES viii

LIST OF FIGURES x

SUMMARY xi

CHAPTER

1 INTRODUCTION 14

Approaches to Preserving Privacy 15

Theories of Privacy 18

Interim Summary 29

Privacy in Human-Computer Interaction 30

Introducing Misclosure 35

Summary & Overview of Studies 42

2 METHOD FOR STUDY 1: ANALYSIS OF FOCUS GROUP DATA 44

Participants 45

Materials 46

Procedure 50

Data Analysis 51

3 RESULTS OF STUDY 1: PRIVACY BEHAVIORS 54

Qualitative Analysis of Privacy Behaviors 54

Summary of Qualitative Analysis of Privacy Behaviors 65

Quantitative Analysis of Privacy Behaviors 66

Summary of Quantitative Analysis of Privacy Behaviors 70

4 DISCUSSION OF FOCUS GROUP RESULTS 71

Theoretical Implications 72

Opportunities for Design 80

Summary and Interim Conclusions 88

5 METHOD FOR STUDY 2: CRITICAL MISCLOSURE INCIDENTS 90

Critical Incident Technique 90

Overview of Study 94

Participants 94

Materials 96

Procedure 97

Data Analysis Strategy 99

6 RESULTS OF STUDY 2: CRITICAL MISCLOSURE INCIDENTS 100

Number of Misclosures Reported 100

Type of Incidents Reported 101

Misclosure Type 101

Length of Time since Incident 102

Type of System 103

Experience with System 103

Familiarity 104

Attribution of Error 105

System Factors 105

Person Factors 107

Negative Consequences 107

Repeat Occurrences 108

Steps Taken to Prevent Future Occurrences 108

7 DISCUSSION OF CRITICAL MISCLOSURE INCIDENTS RESULTS 110

Design Implications 114

Theoretical Implications 119

8 CONCLUSION 121

Limitations 122

Future Work 124

Final Summary 125

APPENDIX A: MATERIALS FOR STUDY 1 128

APPENDIX B: MATERIALS FOR STUDY 2 144

APPENDIX C: MATERIALS USED FOR BOTH STUDIES 157

APPENDIX D: FINAL CODING SCHEME FOR FOCUS GROUP DATA 186

REFERENCES 187

LIST OF TABLES

Page

Table 1. Behavioral mechanisms used to regulate privacy. 26

Table 2. Information Privatness by Type 32

Table 3. Types of Misclosure 37

Table 4. Taxonomy of Error Types with Examples 37

Table 5. Focus Group Sample Description 46

Table 6. Privacy Scenarios 48

Table 7. Example Privacy Scenario with Probe 49

Table 8. Avoidance Behaviors 56

Table 9. Controlling the Outflow of Information 62

Table 10. Percentage of Reported Behaviors by Age 67

Table 11. Photo Sharing 67

Table 12. Identity Theft 68

Table 13. Health Disclosure 69

Table 14. Location Tracking 69

Table 15. Surveillance 70

Table 16. Self-Disclosure 70

Table 17. Behavioral mechanisms used to regulate privacy. 74

Table 18. Misclosure Sample Description 95

Table 19. Abilities Test Results 95

Table 20. Type of Misclosure 102

Table 21. Length of Time Since Misclosure Incident 102

Table 22. Type of System Used During Misclosure Incident 103

Table 23. Length of Time Using System Prior to Incident 104

Table 24. Primary Attribution of Error 105

Table 25. System Factors Contributing to Misclosure.. 106

Table 26. Self Factors Contributing to Misclosure 107

Table 27. Percentage of Misclosures With Negative Consequences 108

Table 28. Percentage of Misclosures With Repeat Occurrences 108

Table 29. Percentage of Misclosures When Additional Steps Were Taken to Prevent Future Occurrences 109

Table 30. Steps Taken to Prevent Future Misclosures.. 109

LIST OF FIGURES

Page

Figure 1. Information Type by Information Receiver Interaction 34

Figure 2. Conversation Available to all Dartmouth facebook Users 40

Figure 3. Screenshot of MAXqda coding interface 50

Figure 4. Hierarchical Coding of Privacy Behaviors... 55

Figure 5. Continuum of Sharing 64

Figure 6. Adaptation of Altman's Model of Privacy Regulation 76

Figure 7. Alternative Model of Privacy Regulation... 77

Figure 8. Information Type by Information Receiver Interaction 78

Figure 9. Example of Checking Facilitation 85

Figure 10. Traditional Age Input 86

Figure 11. Alternative "Vague" Age Input 87

Figure 12. Critical Incident Study Procedure 98

Figure 13. Percentage of Participants Reporting Misclosure... 100

Figure 14. Familiarity with System 104

Figure 15. Example similar to Facemail.. 115

Figure 16. Gmail undo feature.. 116

Figure 17. Sample facebook privacy settings 117

Figure 18. SelectiveShare Interface Sketch 118

SUMMARY

Critical Issues in Privacy and Technology

As access to information changes with increased use of technology, privacy becomes an increasingly prominent issue among technology users. Privacy concerns should be taken seriously because they influence system adoption, the way a system is used, and may even lead to system disuse. Threats to privacy are not only due to traditional security and privacy issues; human factors issues such as unintentional disclosure of information also influence the preservation of privacy in technology systems.

Approach

A dual-pronged approach was used to examine privacy. First, a broad investigation of younger and older adults' privacy behaviors was conducted. This investigation resulted in a categorization of privacy behaviors associated with technology. There were three high level privacy behavior categories identified: avoidance, modification, and alleviatory behavior. This categorization furthers our understanding about the psychological underpinnings of privacy concerns and suggests that 1) common privacy feelings and behaviors exist across people and technologies and 2) alternative designs which consider these commonalities may increase privacy. Second, I examined one specific human factors issue associated with privacy: disclosure error. This investigation focused on gaining an understanding of how to support privacy by preventing disclosure errors. Specifically, I explored instances where people made unintentional disclosures of private information when using technology.

Understanding Privacy Behaviors

From a psychological perspective, an important preliminary step to designing for privacy is to understand the behaviors with which privacy is associated. As a way to understand privacy behaviors in this dissertation, an archival analysis of previously collected focus group data was conducted. The existing focus group data covered a wide range of privacy intensive topics including health information, location tracking, surveillance, and identity theft. The goal of this study was to gain a better understanding of privacy across technologies, to discover the similarities, and identify the differences in what privacy means across contexts as well as provide a means to evaluate current theories of privacy.

Understanding Misclosure Occurrences

One important behavior identified in the privacy literature, and evidenced in the archival analysis is that users manage privacy by withholding information from some people while wanting to share the same information with specific others. Thus, an important implication is that for technologies to effectively support privacy, they need to support specific disclosure and prevent disclosure errors, or what I have termed misclosure. A misclosure is an error in disclosure. When information is disclosed in error, or misclosed, privacy is violated in that information not intended for a specific person(s) is nevertheless revealed to that person.

To understand the conditions under which misclosures are likely to occur I conducted a critical incident study. The critical incident technique is uniquely suitable to exploring misclosure because it allows the researcher to collect events of special significance (e.g., a misclosure incident) that have occurred in the past as well as explore the conditions surrounding each disclosure or misclosure. The goal of this study was to provide a psychological basis for design suggestions for improving privacy in technology which was grounded in empirical findings. The study furthers our understanding about privacy errors in the following ways: First, it demonstrates for the first time that both younger and older adults experience misclosures relatively frequently. Second, it suggests that misclosures occur even when technology is very familiar to the user. Third, it revealed that some misclosure experiences result in negative consequences, suggesting misclosure is a potential threat to privacy. Finally, by exploring the context surrounding each reported misclosure, I was able to propose potential design suggestions that may decrease the likelihood of misclosure.

Contributions

To summarize, the contributions of this dissertation include:

1. Identification and categorization of privacy behaviors across multiple technologies
    a. A critical examination of these behaviors resulting in suggestions for design improvements
    b. A discussion of the findings from this study in relation to existing theories of privacy
2. Identification of the (system and psychological) conditions under which misclosures are likely to occur
    a. An in-depth examination of misclosure occurrences resulting in suggestions for designs which may prevent misclosures.

CHAPTER 1

INTRODUCTION

Advances in computing and increasing use of technology may fundamentally change the conception of privacy because technology changes our ability to store, search, reproduce, and make information available to others (Sparck-Jones, 2003). While people were once able to easily determine who would have access to information about them, this is on longer the case. This fundamental change in the regulation of privacy threatens both users and businesses. For example, users report increased concerns about privacy (Karat, Karat, Brodie, & Feng, 2006; Sims Bainbridge, 2003; Westin, 2003) and increases in psychological and physiological stress due to these concerns (Webb, 1978). Businesses are affected by privacy because concerns about privacy influence system adoption (Herbsleb, Atkins, Boyer, Handel, & Finholt, 2002; Want, Hopper, Falc, & Gibbons, 1992) and trust of organizations (Karat, Karat & Brodie, 2008). Users cite privacy concerns as a reason they have not yet gone online, as well as a reason they have stopped using particular technologies (e.g., the internet; UCLA, 2003) altogether. When users are concerned about privacy, they may be less willing to use a technology; thus businesses developing those technologies suffer.

Privacy and security fears are considered major barriers to continued growth of specific technologies (Hoffman, Novak, & Peralta, 1999; Metzger, 2004), perhaps because they are considered to be among the most serious concerns (O’Neil, 2001; specifically among internet users). For example in e-commerce settings, purchasers are more willing to do business with companies that are perceived to protect privacy (Tsai, Egelman, Cranor, & Acquisti, 2007). Even when a user chooses to do business with a company, those consumers who are more concerned about privacy tend to want to limit access to their personal information (Phelps et al., 2000). When concerned about their privacy online, users may behave differently than they normally would. For example, they may become less likely to disclose information to websites, notify ISPs about unsolicited e-mail, request removal from mailing lists, respond angrily or 'flame' to unwanted email, and become less likely to use web sites that require registration (Sheehan & Hoy, 1999). Individuals are becoming more concerned about their privacy and are often taking action against what they perceive to be invasions of their privacy.

Approaches to Preserving Privacy

For the reasons outlined above, preserving privacy represents a major goal for information technology designers. However, protecting privacy is often a difficult challenge. From a technology perspective, protecting privacy is a multifaceted concept including physical security, internet security, software security, data handling, database design, policy, law, management, and human factors. Many approaches have proven successful in accomplishing specific sub-goals assumed to be required for protecting privacy. For example, information security has been improved, privacy policies have been re-written, the law is beginning to catch up with technology, and improved interface designs have been introduced. A brief review of a sample of these approaches is presented below.

Security Methods

Security methods are methods that focus on ensuring that data are not compromised once they have been disclosed. These approaches vary in terms of method and include relatively simple strategies like password protection to more intensive strategies like data encryption and data obfuscation. Encryption protects already disclosed data by transforming it using an algorithm into a form that is not decipherable by those who do not have the encryption key, while data obfuscation modifies a dataset by substituting pieces of data with similar data from the same set (Bakken, Parameswaran, Blough, Palmer & Franz, 2004; Parameswaran & Blough, 2005). Although security methods are often effective ways of protecting private information once it has been disclosed to an intended recipient, it will not protect against a number of threats to privacy (e.g., unintentional disclosure; phishing, etc.).

Legal & Policy Approaches

Contrary to conventional wisdom, there is no legal "right to privacy" mentioned in the bill of rights (Caudill & Murphy, 2000). Rather, Warren and Brandeis (1890), argued that individuals had a right "to be let alone" (p. 193), and that this right could be interpreted to mean that information collected about a person should be controlled by the individual. Thus, legal and policy approaches to preserving privacy typically focus on controlling how companies (and in some cases, governments) collect and disseminate personal information. In addition, some privacy policy (e.g., portions of informed consent) focuses on ensuring that users are aware of information being collected. The understanding of privacy used in these approaches is typically based on case law rather than psychological issues associated with privacy.

For example, users may consider information about them (e.g., social security number) to be “theirs”. From their perspective, they own it. However, third party information, or information that is collected about a person is not protected by the 4th Amendment (protection from unreasonable search and seizure). This means that information a bank, credit card company, or any other entity collects about a person is not necessarily legally protected, even though a person may “feel” as though they own the information because it is about them. Thus, legal approaches to privacy may not always reflect users understanding or attitudes about privacy.

Human Computer Interaction Approaches

Furthering an understanding of privacy is “central to the concerns of HCI (Human Computer Interaction)” (Karat, Karat, & Brodie, 2008, p. 646), thus HCI researchers have conducted investigations designed to contribute to our understanding about how to develop technologies that are privacy protective. From a design perspective, Palen and Dourish (2003), have argued that all designers of technology must consider users’ privacy at the beginning of the design process or risk that the system they develop will be privacy invasive. One method used at the beginning of the design process to understand the privacy issues involved in ubiquitous computing technologies is paratyping (Iachello, Truong, Abowd, Hayes & Stevens, 2006). Paratyping is a method of evaluation of a prototype of a specific technology set in a “real-world experience” (Iachello et al., 2006, p. 1011). In this method a researcher introduces a technological instance and then gathers participant feedback based on the interaction. In one study using paratyping, the authors concluded that algorithmic approaches (e.g., upfront privacy policy authoring) may not be a suitable approach to preserving privacy. Instead, they argue that gaining a better understanding of the social dynamics of privacy would be a more useful approach in terms of interface design (Iachello et al., 2006).

Reviewing the literature on social-psychological dynamics of privacy reveals two major theoretical treatments of privacy: Altman's (1975) theory of interpersonal interaction and Westin's (1967) theory of privacy and freedom.

Theories of Privacy

While both Altman's (1975) theory of interpersonal interaction and Westin's (1967) theory of privacy and freedom have "stood the test of time" and have "paved the way for others to follow" (Margulis, 2003), they are rarely referenced in HCI work on privacy (Caine, 2008; though see Palen and Dourish, 2003 for a notable exception). In the following sections I provide a brief overview of each theoretical approach and then explain how each approach can and cannot be applied to privacy in HCI.

Westin's Theory of Privacy and Freedom

Westin (1967) views privacy as the control over when, how, and to what extent information about an individual is communicated to others. He identifies 4 privacy states: solitude, intimacy, anonymity, and reserve, and 5 functions of privacy: personal autonomy, emotional release, self-evaluation, and limited and protected communication. Both classifications are supported by empirical studies.

The Basis of Westin's Theory

Westin identifies a number of "general aspects of privacy which apply… in virtually every society" (p. 61). First, Westin notes that across cultures there is what he terms the "universal privacy invading principle," that is, that there is a tendency for individuals to invade the privacy of others and for societies to want to know what is going on for the purpose of guarding against anti-social activities. Westin argues that there are two processes at work that invade privacy in this way: individual curiosity and societal surveillance. Of individual curiosity he argues that it is not the nature of people to ‘let everyone alone’ or ‘mind their own business’, but rather that people across societies have an “insatiable” (p. 20) craving to discover secrets. Of surveillance by authorities, he argues that society has mechanisms, namely watching an individual’s conduct and judging it against societal norms to enforce society’s rules. Despite the opportunity for greater privacy provided by modern society, Westin notes that density, bureaucracy, and surveillance are threats to modern notions of privacy.

Based on the analyses of privacy across cultures, Westin defines privacy as: “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others” (pg. 7). This definition highlights the idea of control over information. It also alludes to the states of individual privacy Westin identifies.

States of Individual Privacy

Westin classifies privacy into 4 distinct states: solitude, intimacy, anonymity and reserve. Solitude is a state of physical withdrawal where an individual is separated from all other people and believes he or she is free from observation. In a state of solitude, although the individual is separated from other people there may be noise or other stimuli present in the environment. Intimacy is a state where an individual is secluded with at least one other person. This small unit, which may consist of more than a dyad, is separate from others. Anonymity is the state of being in public with the knowledge of being observed, but only by strangers and without the risk of recognition. Importantly, Westin includes in his description of anonymity that the individual is free from identification and surveillance. By this description a member of a crowd in London, where video surveillance is ubiquitous, is NOT experiencing anonymity, even if they are surrounded by strangers. Westin states: "Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas" (pg. 31). The state of anonymity also includes publication of ideas anonymously. Finally, reserve is a psychological barrier where a person holds back some expression. Westin claims that reserve "expresses the individual's choice to withhold or disclose information" (p. 32) and that the state of reserve varies culture to culture.

Despite the intuitive sense Westin's classification of privacy states may make, Westin's states were developed ad hoc (Pedersen, 1979). To evaluate the appropriateness of Westin's classification, Pedersen conducted a factor analytic study to determine types of privacy. This factor analysis confirmed Westin's hypothesized states, with slight modification. Intimacy was identified to have two separate types: intimacy with friends and intimacy with family, and solitude was deconstructed into solitude and isolation. Pedersen's description of the 6 resultant states differs slightly from Westin's. For example, the description Pedersen offers of reserve, "unwillingness to be with and talk with others, especially strangers" differs from Westin's definition of reserve as, "a psychological barrier where a person holds back some expression" and "expresses the individual's choice to withhold or disclose some information."

Marshall (1974), independent of Westin and Pedersen, also conducted a factor analytic study of privacy states. Marshall classified six factors indicating six independent privacy states: intimacy, not neighboring, seclusion, solitude, anonymity, and low self-disclosure. Despite minor differences each classification arrives at similar conclusions that some states occur while alone, while others occur with people, and others indicate regulation of behavior such as disclosure.

Functions of Individual Privacy

In addition to identifying states of privacy, Westin also attempts a classification of the functions of individual privacy. According to Westin these are: personal autonomy, emotional release, self-evaluation and limited and protected communication. Personal autonomy is the "desire to avoid being manipulated or dominated wholly by others" (p. 33). Emotional release functions to provide relaxation from the various roles people play. Westin claims that people need moments off stage when they may "deviate temporarily from social etiquette", take "respite from emotional stimulation of daily life" (p. 35). Specifically, this function provides "protection [from]… minor non-compliance with social norms" (p. 35) and allows people to not be held responsible for venting to family or friendship circles. This function is similar to the idea of presentation of self, where different versions of the self are compared to actors on a stage; the self that is being portrayed at a moment is the actor on stage (Goffman, 1959).

Self-evaluation is the opportunity to integrate "experiences into meaningful patterns", to plan, and to process. Westin claims that "individuals need to process the information that is constantly bombarding them, information that cannot be processed while they are still 'on the go'" (p. 36). Self-evaluation also allows the opportunity to create and to evaluate the timing of making information known to the public. Finally, limited and protected communication involves choosing what to disclose to whom. This includes the idea of sharing information with certain people under the expectation that the information will not be repeated to others.

Similar to the privacy states, Westin proposes his classification of functions of privacy based on his understanding of the anthropological and sociological literatures but does not offer additional evidence that might test these claims. As with the privacy states, Pedersen (1997) followed up on Westin's ad hoc classification of privacy functions using a factor analysis. He identified 5 privacy needs/functions/purposes: contemplation, autonomy, rejuvenation, confiding and creativity. There is some overlap between Westin's classification of functions of privacy and Pedersen's, however, the overlap is not complete. Overall, Pedersen's (1979; 1982; 1997; 1999) work extends and empirically validates categories and relationships proposed by Westin (1967). However, all of Pedersen's work assumes Altman's theoretical stance (Pedersen, 1999), which we turn to next.

Altman's Theory of Social Interaction

Altman views privacy as an interpersonal boundary process by which people regulate (control) interactions with others. Using mechanisms including personal space and territoriality, individuals regulate toward a match between a desired and achieved level of privacy. When achieved privacy equals desired privacy, optimal privacy occurs. However, when a congruent state is impossible to reach, coping and/or negative consequences are hypothesized to occur.

Background

In addition to drawing on the work of numerous anthropologists and sociologists Altman (1975), also draws on Westin's (1967) work, recognizing and restating Westin's classification of four types of privacy: solitude, intimacy, anonymity, and reserve and four functions of privacy: personal autonomy, emotional release, self-evaluation, and limited and protected communication. Beyond recognition and unelaborated description, Altman does not offer a critique or extension of Westin's categories. Rather, it appears that Altman accepts the categorizations, but does not find them of use. Instead, Altman (1975, p. 12) claims the functions of privacy are, "(a) control and management of interpersonal interaction, (b) plans, roles, and strategies for dealing with others, and (c) features of self-identity" (cf., Pedersen, 1997; Westin, 1967).

Overview of Theory

Altman's is essentially a theory about environment and behavior, specifically, social behavior and its relation to the physical environment. His theory is broad enough to be considered a theory of social interaction (Margulis, 2003) rather than merely a theory of privacy and includes conceptualizations of privacy, crowding, territory, and personal space. He examines, "how people are affected by the physical environment in face-to-face interaction and how they actively use the environment to shape social interaction with others" (Altman, 1975, pgs. 2-3). Altman views the physical environment as a behavioral extension of the self, thus components in the environment are considered parts of the theory, in the same way as psychological components.

For Altman (1975), privacy is central to the other concepts he discusses (i.e., crowding, territoriality, and personal space). He proposes that privacy is, "a central regulatory process by which a person (or group) makes himself more or less accessible and open to others and that the concepts of personal space and territorial behavior are mechanisms that are set in motion to achieve desired levels of privacy" (Altman, 1975, p. 3). This definition emphasizes privacy as control over interaction.

Conceptualization of Privacy

Privacy, to Altman, is a process. He describes a hypothetical personal boundary that may be more open—where it is more receptive to interaction with others—or more closed where the "self" is less open to interaction. Altman argues that this regulation is dynamic, meaning an individual, influenced by changing conditions, opens or closes themselves to others resulting in a desired level of interaction. Privacy is considered an optimizing process where people seek to interact not too much or too little, but at an optimal level. Both inputs (incoming stimuli from others) and outputs (disclosing) are regarded as being involved in privacy regulation. Altman, Vinsel, & Brown (1981) hypothesize that a period of openness will eventually be followed by a period of closedness. Relationships may move toward closedness or openness as time progresses (see pg. 144).

Selective control

Selective control is the idea that people regulate their interaction by making themselves more or less accessible to others. Ideas of openness and closedness, availability and unavailability, passable and not passable, and where a person falls at a certain time on these are all dependent on unmentioned circumstances.

Because of the dynamic nature of Atlman's conceptualization of privacy, the desired level of privacy (contact with others at a particular moment) may not equal the level of achieved privacy. The desired level of privacy is, "an internal, personal state in which a person or group develops momentary desires for certain levels of input and output to and from others" (Altman, 1975, pg, 6). Although the theory does not explain when desired levels of interaction might be high or low, it allows for the full range of preferred interaction levels. Altman states that this interaction level may shift over time. When there is a mismatch between desired privacy and achieved privacy a person or group will adjust by altering interpersonal control mechanisms until the achieved level of privacy equals the desired level of privacy. It is hypothesized that people engage in privacy regulation to ensure that achieved privacy equals desired privacy. These privacy-regulation mechanisms include personal space, territory, verbal behavior and nonverbal behavior.

Mechanisms for the Regulation of Privacy

If a person recognizes that they have less privacy than they want, they may engage in behaviors designed to lessen their interaction; alternatively, if a person recognizes they have more privacy than they want, they may engage in behaviors to increase their interaction. To describe this notion, Altman introduces the ideas "interpersonal control" and "interpersonal boundary regulation," both of which refer to the notion of a person "maintaining an appropriate and desired level of interaction between itself and the external physical and social environment," (Altman, 1975, pgs. 3-4). To maintain the appropriate level of interaction, people regulate privacy to a desired level by using behavioral mechanisms. Behavioral mechanisms (see Table 1) used to achieve privacy goals include verbal behavior, paraverbal behavior, nonverbal behavior, personal space, territoriality and culture (Altman & Chemers, 1980; Altman, 1975).

Behavioral mechanisms that are used to regulate privacy include increasing physical distance from another person and communicating, verbally or non-verbally,

Table 1. Behavioral mechanisms used to regulate privacy.

Behavioral Mechanism	Definition	Examples
Verbal	the contents of what a person says	Saying: • “Let’s talk” • “Can I raise an issue with you” • “Sorry, I’m too busy now” • “No, I can’t make it this evening”
Para Verbal	way of speaking, how someone says something	Speaking in a cool or warm tone
Non Verbal	communication without words including posture, gaze, facial expressions and gestures	• body orientation • turning away • smiling • grimacing • frowning • looking away • fidgeting with own clothing • rubbing own hands together • looking at our watches • assuming rigid, symmetrical body positions
Personal Space	"the space within an invisible boundary around people that is with them everywhere they go." (Altman & Chemers, 1980, p. 102)	• increase or decrease physical distance between self and another person o by backing away o by moving closer
Territory	control and ownership of a place by a person or group	• invite someone into a territory they occupy • closing a door • use signs saying keep out or welcome • offering a chair • providing refreshments • not inviting in
Culture	customs, rules and norms which communicate availability to other members in the same culture	• not dropping by a friend’s house at dinner time • too early in the morning or too late at night avoiding • coming to parties too early and leaving at a reasonable hour • not opening shut doors (at least without knocking) etc.)

(Altman & Chemers, 1980; Altman, 1975)

dissatisfaction with the level of interaction, among many others. All behavioral mechanisms incur some cost (expending physical and/or psychological energy) to the person or group who is engaging in them. Altman claims that “after repeated failures to achieve a balance between achieved and desired levels of privacy, a person may accept the fact of inevitable and uncontrolled intrusion and/or separation.” Accepting an inevitable and uncontrolled intrusion is hypothesized to have detrimental consequences: “psychological viability or well-being of people and groups centers on the successful management of privacy. That is, success or failure at privacy regulation may well have implications for self-identity, self-esteem, and self-worth – or the very well-being and survival capability of people and groups” (pg. 81, Altman & Chemers).

Comparison of Theories of Privacy

In the preceding sections, two theories of privacy were reviewed. Both theories posited that privacy is about controlling interaction and information disclosure. The first, Westin’s theory, views privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” The second, Altman’s theory, postulates that privacy is a boundary regulation process. A fundamental difference between Westin’s and Altman’s views of privacy is definitional. Whereas Westin’s concept of privacy focuses on control over information, Altman’s concept of privacy focuses on regulation of interaction.

An additional distinction is that for Westin, privacy is related to withdrawal, whereas for Altman privacy includes the spectrum of interaction (from closedness to openness). Repeatedly in his writing, Westin pits social stimulation/interaction/communication against privacy: “social stimulation… exists…

alongside… needs for privacy." (pg 10), but is not a part of privacy. On the other hand, for Altman, the need for stimulation is also a privacy need; states of too little interaction are considered cases where achieved privacy is more than desired privacy. Most studies of privacy in HCI discuss privacy in the way Westin approaches privacy, as a state of isolation, rather than as one of various states of interaction.

A strength of Westin's theory is that the states and functions proposed are clear and well defined; hypotheses are easily drawn from these classifications. For example, when privacy is violated we may expect autonomy or creativity to decrease. Similarly, Altman offers hypotheses about what happens if achieved privacy does not equal desired privacy: behavioral mechanisms will be engaged until optimal privacy is achieved. However, Altman's theory does not offer predictions about when privacy may be desired, or why.

Both Westin and Altman's theoretical approaches are useful in furthering our understanding of privacy in HCI. Because Westin's theory focuses on control over information, his theory may be particularly useful in assessing information privacy (i.e., data privacy). On the other hand, Altman's theory focuses on regulation of interaction and may therefore be suited for understanding privacy of systems that allow/encourage online interaction (e.g., online communities).

However, despite the potential usefulness of these theories in HCI a number of problems plague their adoption as principles that may be used to guide further research. First, the field has yet to agree on a singular or multi-themed definition of privacy (Leino-Kilpi et al., 2001; Caine, 2008). This lack of an agreed upon definition has left privacy as, "a concept disarray" (Solove, 2006), with multiple papers on privacy introducing the topic of their paper by saying, “the concept [of privacy] and its definition often remain ambiguous,” (Acquisti, Friedman, & Telang, 2006). Second, neither theory addresses the use of technology; there is a need to evaluate each theory against current research that explores privacy and technology. Finally, designers find it difficult to apply either theoretical approach in their work with technology: “It is by no means an easy task to apply Altman’s theory of privacy to the problem of designing a privacy-supporting video media space... Altman’s theory largely ignores the privacy-technology relationship…. Altman’s description of the process is extremely abstract: both the boundaries and the mechanisms by which they are controlled are purposefully left ambiguous,” (Boyle, 2005, p. 152). Therefore, for current theories of privacy to be useful in HCI they need to be evaluated and clarified.

Interim Summary: Need for Study 1

To summarize, despite various approaches, privacy continues to be a major concern among technology users (Karat, Karat, Brodie, & Feng, 2006; Sims Bainbridge, 2003; Westin, 2003). Users “flame, complain and abstain” (Sheehan & Hoy, 1999) when technology does not appropriately protect privacy, make their dissatisfaction known publicly, and even refuse to begin using new technologies because of privacy concerns (Herbsleb, Atkins, Boyer, Handel, & Finholt, 2002; Want, Hopper, Falc, & Gibbons, 1992). Current theories of privacy are ill-equipped to provide guidance about privacy as it relates to technology. Therefore, what is left to understand is the nature of privacy concerns, how they influence behavior, and how we can provide technology solutions to allay such concerns. Gaining this broad understanding is the first goal of the proposed research and will be addressed in Study 1, an archival analysis.

From a psychological perspective, an important preliminary step to designing for privacy is to understand the feelings and behaviors with which privacy is associated. As a first step toward understanding privacy feelings and behaviors, an archival analysis of a set of transcripts obtained from multiple focus groups was conducted. The scenarios in the focus covered a wide range of privacy intensive topics, including health information, location tracking, surveillance, and identity theft thus providing a rich data set from which to obtain reports of feelings and behaviors associated with privacy across technologies. In the next section I provide a more focused introduction to a specific problem in privacy in HCI: supporting privacy by preventing disclosure errors.

Privacy in Human-Computer Interaction

Although widely considered an important topic in psychology, privacy has received little scholarly attention in the psychological literature (Altman, 1975; Berscheid, 1977; Iachello & Abowd, 2005; J. Karat, Karat, & Brodie, 2008; Ludford, Priedhorsky, Reily, & Terveen, 2007; Margulis, 2003; Palen & Dourish, 2003; Patil & Lai, 2005; Webb, 1978; Westin, 1967, 2003). However, research on privacy is flourishing is the field of HCI. HCI designers have realized that the systems they are currently developing may threaten the privacy of their users if privacy is not taken into account at the beginning of the design process (Palen & Dourish, 2003).

Within the HCI literature most research has been atheoretical, centering around groupings of technologies and features, rather than fundamental psychological aspects of privacy. Two features that have received attention are: information type and information receiver.

Information Type

Different pieces of information have different levels of overall “privateness” (Metzger, 2004) or sensitivity (Hawkey & Inkpen, 2006). Privateness ranges from “very private” to “not really private,” while sensitivity is associated with willingness to disclose such that individuals are less willing to disclose sensitive than non-sensitive information (Singer, von Thurn, & Miller, 1995). For example, location has been found to be a particularly sensitive piece of information (Kaasinen, 2005; Patil & Lai, 2005) that users are often unwilling to disclose. In other studies participants reported preferring to keep early work drafts, phone numbers, personal statistics (e.g., SSN, marital status, salary), history of performance reviews, and health related information out of the hands of others (Olson, Grudin & Horvitz, 2005).

It may be that the possession of a piece of information by another leaves the discloser vulnerable to the power of others, thereby increasing the degree of risk of disclosure (Burgoon, 1982). Specifically, stigmas which refer to “a stable characteristic or attribute of an individual that is perceived as damaging to the individual’s reputation” (Montgomery & Baxter, pg. 13) increase the risk of disclosure. Stigmas include information items such as physical disability, homosexuality, sexual abuse, drug addiction, alcoholism, and diseases such as mental illness, epilepsy and HIV-positive status. Individuals tend to be stigmatized when they posses or display characteristics of a stigma, or are associated with someone who is stigmatized. Importantly, stigmas tend to continue to be associated with a person over time so those who have in the past been stigmatized, tend to continue to be stigmatized.

Table 2. Information Privatness by Type

	Type of Information
Less Private	Sex
	First name
	Education level
	Age
	Favorite TV show
	Favorite snack food
	Time spent online per week
	Marital status
	Interests/hobbies
	Product preferences
	Race/ethnicity
	Occupation
	Email address
	Number of people in household
	Political party affiliation
	Recent online purchases
	Last name
	Religion
	Health
	Postal address
	Income
	Telephone number
	Drafts of work projects
	Salary
	Child's name
	Credit card number
	Banking information
More Private	Social security number
	Location

Note. Adapted from Metzger (2004) with additional data from Ludford, Priedhorsky, Reily, & Terveen, 2007; Olson, Grudin & Horvitz (2005); Hawkey & Inkpen, (2006); Ackerman, Cranor & Reagle (1999)

Although no one study has compared all types of information, Table 2 presents a conceptual summary compiled from multiple studies of types of information by level of general privateness. While the simplicity and potential usefulness of this table is appealing, it should be viewed with a cautious eye; it is likely that type of information in isolation is poor predictor of privacy preference.

Information Receiver

In addition to type of information, perceived privacy of a request is also dependent on the relationship of the information discloser to receiver (Adams, 1999; Consolvo et al., 2005; Hawkey & Inkpen, 2005; Khalil & Connelly, 2006; Lederer, Mankoff, & Dey, 2003; Muller, Smith, Shoher, & Goldberg, 1991; Olson, Grudin, & Horvitz, 2005; Patil & Lai, 2005). Although across studies different groups were identified (e.g. colleagues, family, friends, etc.), the common finding across groups was that participants perceived different levels of privacy for different groups (whether these be self-defined or researcher imposed). Overall, the supervisor/manager/boss was associated with the most privacy concern while the spouse/ significant other was associated with the least (Consolvo et al., 2005; Hawkey & Inkpen, 2005; Lederer et al., 2003).

Information Type by Information Receiver

Although there may be types of information and certain receivers that influence perceived privacy independently, many studies reveal a more complex information type by information receiver interaction (see Figure 1). That is, neither the type of information, nor the information receiver alone predicts the level of perceived privacy of an event. Rather, it is both of these variables in combination that predict the perceived privacy of an event. For example, a high privacy information type (e.g. location information) may not be considered highly private when the information receiver is a spouse or significant other. However, if the information receiver is a stranger then location information will be considered highly private (e.g., Khalil & Connelly, 2006).

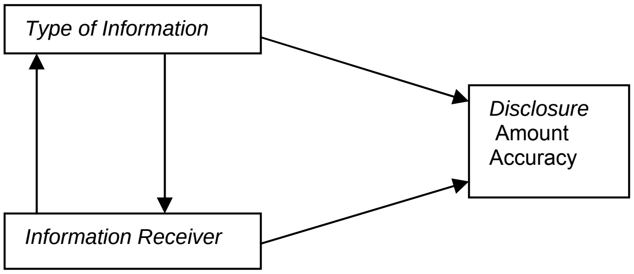


Figure 1. Information Type by Information Receiver Interaction

In studies where both variables have been examined in combination, the relationship of perceived privacy (often operationalized as privacy comfort level or sharing preference) differed based on both information type and information receiver. For instance, in a study of web browser use, privacy comfort level was influenced by a combination of viewer (information receiver) and sensitivity of content (information type; Hawkey & Inkpen, 2006). Similarly, for a project management groupware system, users who engaged in participatory design wanted to restrict sharing different aspects of projects with a variety of potential information receivers (Mueller, Smith, Shoher & Goldberg, 1991).

Even when studied in combination the patterns of privacy preferences are not simple: some information types are variable across people in terms of sharing preferences while others are consistent. For example, while some participants are willing to share personal items with co-workers, others are less willing to do so. Items that tend to be less variable across people include a general preference for sharing work email address and work phone number with co-workers, and never giving credit card information to the public (Olsen et. al, 2005). However, it may not be that both information type and receiver variables are equally important; the identity of the inquirer has been shown to be a stronger determinant of information disclosure than the situation (Leaderer, Mankoff & Dey, 2003).

If these variables truly interact then it may not be appropriate to examine either in isolation as the results may appear contradictory, leading to the conclusion that "privacy means different things to different people" (Karat, Karat & Brodie, 2008, p. 642). To appropriately assess which types of information people consider the most private we need to specify an intended recipient or else risk that each participant imagines a different potential receiver of such information. It is likely that participants would perceive an invasion of privacy if we ask about giving out SSN, credit card information and birth date to "the public". However, if we specify "your credit card company" as the receiver of such information, participants are less likely to claim an invasion of privacy.

In summary, what is clear from these studies is that users have specific and complex privacy and disclosure preferences. One way to support privacy in these systems therefore, is to ensure that no errors of disclosure occur.

Introducing Misclosure

One clear result that can be gleaned from the review of findings from studies of privacy in HCI presented above is that an important aspect of preserving privacy is the ability to withhold information from some people while sharing with specific others.

Thus, for technologies to effectively support privacy, they need to support specific disclosure and prevent disclosure errors.

A wide variety of computer mediated systems ranging from cell phones to online health communities are used by millions of people each day. Despite the frequency with which many people uses these technologies, people tend to lack awareness of what information they disclose to online systems (Ahern, Eckles, Good, King, Naaman, & Nair, 2007) and therefore may be disclosing information in error. Though research in human factors has a comprehensive theory of human error (e.g., Reason, 1984), this theory has received little attention in the context of privacy in HCI.

In psychological terms, a disclosure can be defined as "the act of revealing personal information to others" (Jourard, 1971, p. 2). A counterpart to the intentional act of disclosure is the act of revealing information in error. When information is disclosed in error, or a *misclosure* occurs, privacy is violated in that information not intended for a specific person(s) is nevertheless revealed to that person.

Misclosures can occur in multiple ways (See Table 3 for types of misclosure). For example, an individual may disclose intended information to unintended recipients by accident. This type of misclosure is labeled as a recipient misclosure. An information misclosure is when an individual discloses unintended information to the intended recipient. A final type of misclosure, a combination misclosure, is when an individual discloses unintended information to an unintended recipient. Each type of misclosure may be related to different psychological variables. To explore the type of variables associated with each type of misclosure a critical incident study was used in this dissertation.

Table 3. Types of Misclosure

		Recipient	
		Intended	Unintended
Information	Intended	Disclosure	Recipient Misclosure
	Unintended	Information Misclosure	Combination Misclosure

Misclosure Examples

Designing for privacy does not mean keeping all information away from everyone. Rather, in most cases privacy means keeping some information away from some people. When people choose to disclose private information through technology systems, they engage in behaviors to attempt to ensure two things: 1) that the information reaches only those for whom it was intended, and 2) that the information remains hidden from any others. However, because of errors in disclosure, this is often difficult to accomplish.

Table 4. Taxonomy of Error Types with Examples

Error	Description	Example
Recipient Misclosure	Correct information to unintended recipient	Phishing (sending financial information to a criminal who poses as a trusted institution)
Information Misclosure	Incorrect information to intended recipient	Attach a different photo to an MMS (e.g., text message) than one you meant to attach
Combination Misclosure	Incorrect information to unintended recipient	Forwarding an email to a listserv when you meant to delete the email

Table 4 provides a summary of three types of disclosure errors, as well as an example of each. Phishing is an example of a recipient misclosure because the user sends the intended information (e.g., password to bank account) to an unintended person (phisher instead of the bank). In this case the misclosure occurred for two reasons a) because the phisher is stealing information and b) because the technology did not provide enough information to the user to become aware that the recipient of the information would be the phisher and not the bank. An example of an information misclosure is an event where a user attaches a photo of themselves on the beach to their boss, rather than a photo of them standing dutifully by their conference poster. In this case, the user intended (and was successful) in sending information to the boss, however, the information was not the information the user meant to send. In the final case, the user commits a combination misclosure. An example of this mistake which combines a recipient misclosure and an information misclosure is when a user forwards an email to a listserv when they actually meant to delete that email.

While the examples presented above are only for the sake of explanation, in the next section I present an actual case study of a misclosure incident.

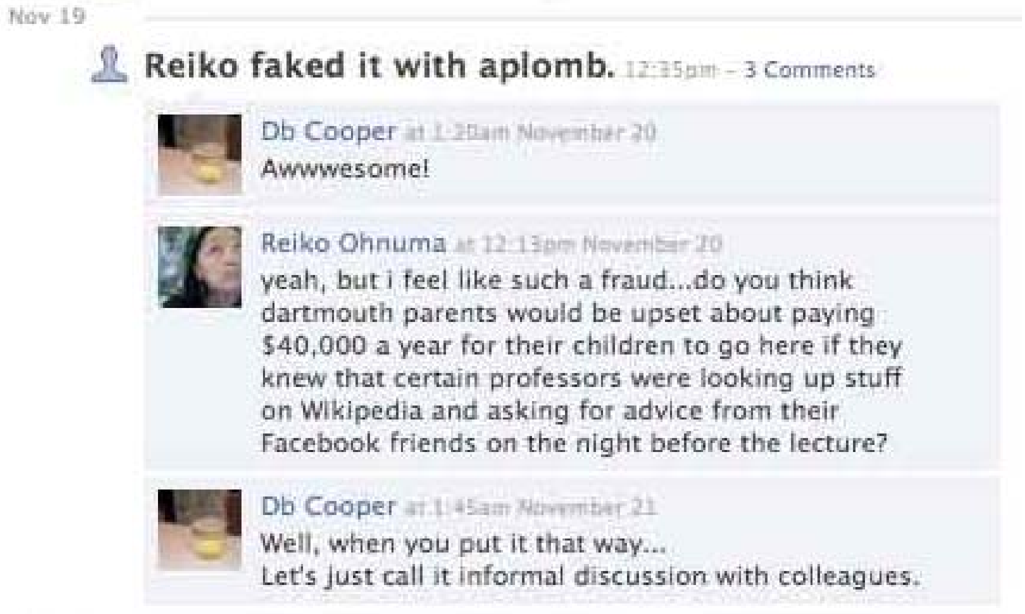
Misclosure Case Study

Reiko Ohnuma, PhD is a professor of Religion at Dartmouth College. She is the author of both journal articles and a book and teaches classes regularly as part of her professorship. Dr. Ohnuma began using facebook; she set up her profile, uploaded a profile photo, and set her privacy settings so that only her friends (i.e., people she specifically approved) could see most information about her, including her status updates. She also joined the Dartmouth network.

Reiko virtually interacted with her friends on facebook, making regular status updates. Sometimes Reiko would vent about her duties as professor. For example, on November 3rd, Reiko posted a status update that read, “Reiko has nothing interesting to say about these damn papers, but better think of something quick,” apparently referring to papers she had to grade for a class she was teaching. It is likely that Reiko did not want students in her class to know she had nothing interesting to say about the papers the students wrote.

Sometimes Reiko’s friends would respond to her status updates with helpful information, a joke, or a comforting remark. For example, on November 17th, while preparing to give a lecture the following morning, Reiko complained that she, “doesn’t know how to explain what ‘modernity’ is & isn’t entirely clear herself.” A helpful colleague offered his take on modernity, to which Reiko replied that she would, “shamelessly plagiarize” the language the colleague used in his description in her class.

After teaching the class on modernity, Reiko posted another status update: “Reiko pulled it off with aplomb,” referring to her successful lecture. The colleague who offered his take on modernity congratulated Reiko on the social networking site. Reiko then replied, “yeah, but i feel like such a fraud…do you think dartmouth parents would be upset about paying $40,000 a year for their children to go here if they knew that certain professors were looking up stuff on Wikipedia and asking for advice from their facebook friends on the night before the lecture?” (see Figure 2 for screen shot of the conversation).



Nov 19

Reiko faked it with aplomb. 12:35pm – 3 Comments

Db Cooper at 1:20am November 20
Awwwesome!

Reiko Ohnuma at 12:13pm November 20
yeah, but i feel like such a fraud...do you think dartmouth parents would be upset about paying $40,000 a year for their children to go here if they knew that certain professors were looking up stuff on Wikipedia and asking for advice from their Facebook friends on the night before the lecture?

Db Cooper at 1:45am November 21
Well, when you put it that way...
Let's just call it informal discussion with colleagues.

Figure 2. Conversation Available to all Dartmouth facebook Users

Obviously Reiko did not understand that other people besides her facebook friends would be able to see her status updates. Specifically, I assume she did not expect *her students*, many of whom are members of the Dartmouth facebook network (anyone with an @dartmouth.edu email address can join the Dartmouth network), to be able to see her status updates. The problem is that Reiko's understanding of the privacy settings on facebook did not match with the way the system functions. By joining the Dartmouth network, Reiko made her profile information and status updates available to all other Dartmouth network members, even though she thought she set her privacy settings so that only her "friends" could see this information.

In this case, no amount of additional security, encryption, or policy would have protected Reiko's privacy. The problem was with an interface that did not support Reiko being able to disclose information to those she wanted to disclose to while keeping the same information from others. Thus, Reiko misclosed.

Critical Issues

While a privacy error on facebook such as the one committed by Reiko might be viewed by many as merely a social blunder (perhaps even humorous), few would argue that committing a similar mistake when using a Personal Health Record (PHR), for example is a laughing matter. Privacy of health information is a major concern among designers, patients, and health care providers (Thede, 2008). Besides increasing concerns about using potentially beneficial technologies such as PHRs, a misclosure of health information could have even more far reaching consequences. Consider a recipient misclosure incident where a patient accidentally disclosed his or her cancer diagnosis to their employer instead of to their general practitioner. In the best case, the patient might get sympathy earlier than expected, but in the worse case an employer might look the person over for a promotion, or even fail to renew a contract if the person is not a salaried employ.

Interim Summary: Need for Study 2

Many technical solutions have been developed that address issues of privacy and security of already disclosed information. However, disclosure errors are as threatening as data breeches and lapses in internet security, yet no research has addressed the human factors issues associated with this threat to privacy. A misclosure is the act of unintentionally revealing information when using technology. This type of error can have serious consequences on privacy. There is a need to understand the types of misclosures that occur and identify the factors precipitating misclosure occurrences.

Summary & Overview of Studies

From this review of human factors issues associated with privacy in HCI, two things become clear. First, there is a need for a better understanding of the variety of behaviors associated with privacy and technology. Second, there is a need to support users in the specific goal of keeping certain information from certain people, as this one of the human factors issues associated with preserving privacy.

In this dissertation I examined privacy from two complementary perspectives to better understand why privacy issues remain a barrier in the design and use of technology. The objectives of studies were to identify, categorize and critically examine privacy behaviors across multiple technologies and determine which were related to design factors, and uncover the system and psychological conditions under which misclosures were likely to occur. Results from the studies in combination provide a broad understanding of many of the privacy issues facing technology users, as well as an in-depth exploration of one threat to privacy: disclosure error.

Study 1 was an archival analysis of existing focus group data about younger and older adults' privacy-related behaviors. The primary goal of this study was to identify and categorize privacy behaviors that are associated with technology use.

Study 2 was a critical incident investigation of disclosure errors among younger and older adults. The goal of this study was to understand the factors that surround misclosure incidents. Specifically, this investigation explored system and psychological characteristics that led to misclosure incidents as well as examined consequences of those misclosures. The knowledge gained provides a psychological basis for design suggestions grounded in empirical findings (e.g., suggestions for technology instruments to avoid misclosures).

To summarize, the contributions of this dissertation include:

1. Identification and categorization of privacy behaviors across multiple technologies
    a. A critical examination of these behaviors resulting in suggestions for design improvements
    b. A discussion of the findings from this study in relation to existing theories of privacy
2. Identification of the (system and psychological) conditions under which misclosures are likely to occur
    a. An in-depth examination of misclosure occurrences resulting in suggestions for designs which may prevent misclosures.

CHAPTER 2

METHOD FOR STUDY 1: ANALYSIS OF FOCUS GROUP DATA

The academic study of privacy has a relatively short history, and there is agreement that relatively little is known about the topic (e.g., Altman, 1975; Berscheid, 1977; Iachello & Abowd, 2005; Karat, Karat, & Brodie, 2008). Specifically, there is a lack of understanding of the psychological variables related to privacy (Caine, 2008). From a psychological perspective, an important preliminary step to further study is to understand the behaviors with which privacy is associated.

In this study I attempted to gain a better understanding of privacy behaviors across a broad range of interactions and technologies. A goal of this study was to identify reported privacy behaviors across multiple technologies. Specifically, I gathered privacy related experiences from a range of participants by conducting an archival analysis of previously collected focus group data.

Choosing a focus group as a research method can be justified at many points throughout the examination of a particular research question (Stewart & Shamdasani, 1990). For example, focus groups may be useful after an experimental study to help explain seemingly confusing quantitative findings. However, focus group methodology may be particularly useful in the exploratory phase of research because of the flexibility of the method and the opportunity to obtain data in the participant's own words (Stewart & Shamdasani, 1990). One of the goals of this study was to understand users' conceptions of privacy, thus a focus group method was particularly useful in this exploratory phase of research on privacy.

This type of data provides a basis of understanding about "everyday privacy behaviors" as described by participants. Once we better understand the types of behaviors people engage in with respect to privacy, we can explore the behaviors more deeply.

Specifically, we are now able to better understand what behaviors participants report and how they describe privacy related behaviors.

The focus groups described in this section were conducted during the Fall of 2007 and Spring of 2008 as part of Michelle Kwasny's MSHCI project. Thus, this chapter is separated into 2 major sections: a section that explains how data were collected (including participants, materials, and procedure) and a section that describes the method for analyzing the 500+ pages of data that were generated from the focus groups.

Participants

Participants were 34 older adults (20 female) between the ages of 60 and 80 (*M* = 69.45, *SD* = 4.95) and 26 younger adults (13 female) between the ages of 18 and 26 (*M* = 20.88, *SD* = 2.03). Older adult participants were recruited from a database of people that had previously expressed interest in participating in studies in the Human Factors and Aging Lab and from a local senior center (Maggie Russell Tower). Younger adult participants were drawn from the student participant pool at Georgia Tech.

As shown in Table 5, participants were well educated and diverse in terms of ethnicity. Participants were fluent English speakers. Younger adults received class credit for participation whereas older adult participants were remunerated for their time at a rate of $10 per hour. Approval for the study was given by the Georgia Institute of Technology Institutional Review Board.

Table 5. Focus Group Sample Description

	Younger Adults (N = 26)	***Older Adults (N = 34)***
Age: *M (SD*)	20.88 (2.03)	69.45 (4.95)
Gender: *% (N*)		
Male	50% (13)	41% (14)
Female	50% (13)	59% (20)
Education: *% (N*)		
≤ High school	15% (4)	36% (12)
Vocational training, some college, Associate's degree	62% (16)	33% (11)
Bachelor's, Master's Doctoral Degree	23% (6)	32% (11)
Ethnicity: *% (N*)		
Hispanic	11 % (3)	3 % (1)
Non-Hispanic White	58 % (15)	41 % (14)
Non-Hispanic Black	8 % (2)	47 % (16)
Other	23 % (6)	9 % (3)

Note: Percentages were rounded.

Materials

Materials for the study included questionnaires and a focus group script (described below), as well as audio recording equipment. The focus group script can be found in Appendix A; all questionnaires can be found in Appendix C.

Demographic and Health Questionnaire

The demographic questionnaire (see Czaja et al., 2006a) gathered broad characteristics of the sample including age, gender, ethnicity, and work status; the health questionnaire gathered self-reported health status, satisfaction with health, and number of medical problems.

Technology Experience Questionnaire

The technology experience questionnaire (see Czaja et al., 2006b) gathered information about technology experience, usage, and attitudes.

Focus Group Script

The focus group script was designed to elicit in-depth discussion of privacy and related topics. The script began by introducing the moderator and assistant moderator / note taker, and welcoming participants to the study. Next, purposes of the study and ground rules for polite participation were explained (e.g., there are no right or wrong answers, please do not interrupt others while they are speaking). Third, the script addressed the use of voice recorders during the focus group and explained how and to what extent the discussion would be kept confidential. This included instructions to participants that they should keep the contents of the discussion to themselves after leaving the study setting. Finally, after a brief ice breaker question to get people talking, the script moved on to the focus of the study: a discussion of privacy across technologies.

Definition questions were designed to gather individual definitions of privacy as well as group-generated definitions of privacy. Participants were first asked to provide their own individual definition of privacy in written form. Then, participants were asked to discuss their definitions of privacy and list the different aspects of privacy from each of their definitions. Groups were not instructed to come to a consensus, rather they were asked to explore and acknowledge differences between definitions. Discussion questions were open ended questions about general thoughts and opinions about privacy. For example, one question asked participants to reflect back to the last time they thought about privacy before the current session.

Table 6. Privacy Scenarios

Category	Scenario
1. Photo Sharing	You have a lifetime of photos you are thinking of storing on a website.
2. Identity Theft	You are using your credit card to buy dinner in your favorite restaurant. When the waiter picks up the bill with your card in it, he takes the card in the other room for 5 minutes.
3. Health Disclosure	You have the symptoms of an illness that have lasted for over a week. You call your doctor's office and describe your symptoms to a nurse.
4. Location Tracking	You are using a cell phone with a locating device (such as GPS). You find out that there is a way for anyone in the world to find out your exact location.
5. Surveillance	Atlanta is trying to crack down on traffic violations by installing traffic cameras on every stop light. These cameras monitor traffic and then take a snapshot of anything out of the ordinary, such as someone running a red light. (Red-light camera)
6. Self Disclosure & Relationship Building	You are having a conversation with friends at home.

The scenario questions covered six main topics: photo sharing, identity theft, health disclosure, location tracking, surveillance, and self-disclosure/relationship building. The scenarios are presented in Table 6. Each scenario was discussed for approximately 20 minutes and included discussion of standard probes (probes that were given after each scenario) and scenario-specific probes. An example of questions asked after Scenario 1 is given in Table 7.

Table 7. Example Privacy Scenario with Probe

Scenario
You have a lifetime of photos you are thinking of storing on a website. a. Standard Probes i. Do you have any privacy issues or concerns with this situation? ii. What about this situation makes it concerning? iii. Why? b. Additions to this scenario i. What if you used a scrapbook? ii. What about an online photo album (like Flickr, Picasa, Snapfish, etc - Only say these if participants ask for examples.)? iii. What about if they were just photos from a recent trip? iv. What if there were sensitive photos included in your set? v. What if you could pick exactly who saw the photos?

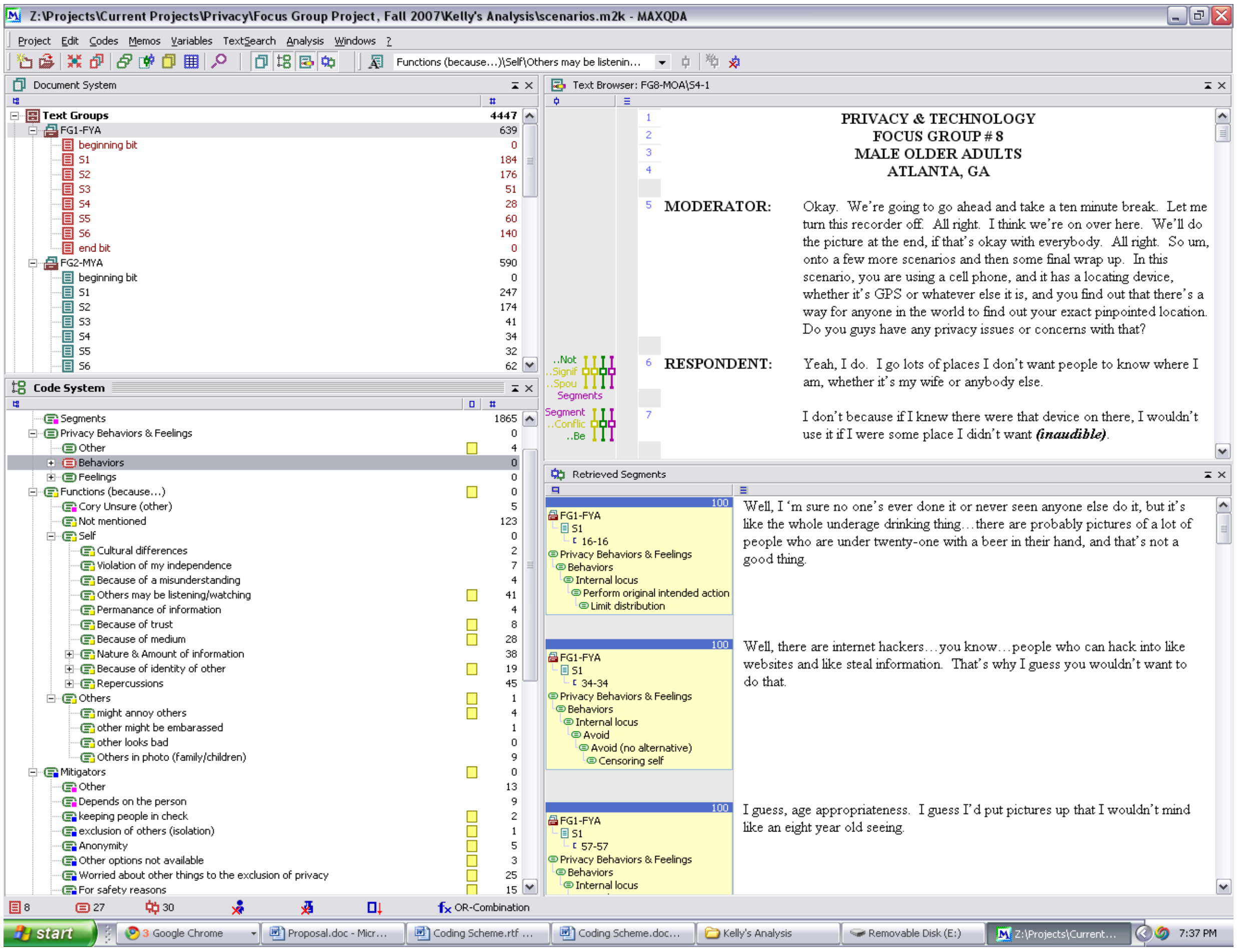
Equipment

Voice Recording Device

All focus group interviews were recorded using an Olympus DM-20 or Olympus DS-30 voice recorder. Interviews were transferred to PC and converted to mp3 format for transcription.

Qualitative Data Analysis Software

Focus group transcripts were coded using MAXqda (version 2k3), a software tool designed for qualitative data analysis. A screen shot of the MAXqda interface is shown in Figure 3.



Document System	#
Text Groups	4447
FG1-FYA	639
beginning bit	0
S1	184
S2	176
S3	51
S4	28
S5	60
S6	140
end bit	0
FG2-MYA	590
beginning bit	0
S1	247
S2	174
S3	41
S4	34
S5	32
S6	62

Code System	□	#
Segments		1865
Privacy Behaviors & Feelings		0
Other	□	4
Behaviors		0
Feelings		0
Functions (because…)	□	0
Cory Unsure (other)		5
Not mentioned		123
Self		0
Cultural differences		2
Violation of my independence		7
Because of a misunderstanding		4
Others may be listening/watching	□	41
Permanance of information		4
Because of trust	□	8
Because of medium	□	28
Nature & Amount of information		38
Because of identity of other	□	19
Repercussions		45
Others	□	1
might annoy others	□	4
other might be embarassed		1
other looks bad		0
Others in photo (family/children)		9
Mitigators	□	0
Other		13
Depends on the person		9
keeping people in check	□	2
exclusion of others (isolation)	□	1
Anonymity	□	5
Other options not available	□	3
Worried about other things to the exclusion of privacy	□	25
For safety reasons	□	15

1 PRIVACY & TECHNOLOGY
2 FOCUS GROUP # 8
3 MALE OLDER ADULTS
4 ATLANTA, GA

5 **MODERATOR:** Okay. We're going to go ahead and take a ten minute break. Let me turn this recorder off. All right. I think we're on over here. We'll do the picture at the end, if that's okay with everybody. All right. So um, onto a few more scenarios and then some final wrap up. In this scenario, you are using a cell phone, and it has a locating device, whether it's GPS or whatever else it is, and you find out that there's a way for anyone in the world to find out your exact pinpointed location. Do you guys have any privacy issues or concerns with that?

6 **RESPONDENT:** Yeah, I do. I go lots of places I don't want people to know where I am, whether it's my wife or anybody else.

7 I don't because if I knew there were that device on there, I wouldn't use it if I were some place I didn't want ***(inaudible)***.

100
FG1-FYA
S1
16-16
Privacy Behaviors & Feelings
Behaviors
Internal locus
Perform original intended action
Limit distribution

Well, I 'm sure no one's ever done it or never seen anyone else do it, but it's like the whole underage drinking thing…there are probably pictures of a lot of people who are under twenty-one with a beer in their hand, and that's not a good thing.

100
FG1-FYA
S1
34-34
Privacy Behaviors & Feelings
Behaviors
Internal locus
Avoid
Avoid (no alternative)
Censoring self

Well, there are internet hackers…you know…people who can hack into like websites and like steal information. That's why I guess you wouldn't want to do that.

100
FG1-FYA
S1
57-57
Privacy Behaviors & Feelings
Behaviors
Internal locus

I guess, age appropriateness. I guess I'd put pictures up that I wouldn't mind like an eight year old seeing.

Figure 3. Screenshot of MAXqda coding interface

Procedure

After giving informed consent, participants filled out the demographics and health and technology experience questionnaires. Next, participants completed the individual privacy definition task and then participated in a group discussion of privacy definitions. Following the discussion of privacy definitions, participants were asked to describe the last time they had thought about privacy and asked to share these stories with the group.

The scenario questions represented the majority of time and deep discussion. First, each scenario was read from the focus group script. Sometimes the scenario generated discussion without the need for a probe, however, most often the first general probe was presented as a way to encourage participants to express their reactions to the scenario. Once the discussion following a probe ran its course (i.e., topics were repeated or participants became quiet indicating the conclusion of a specific topic for discussion) or the time allowed (generally regulated by the moderator) for a topic was up, the moderator moved on to the next probe. If a topic covered by a subsequent probe was brought up by a participant and thus discussed out of turn, the moderator either skipped the probe later in the script, or followed up if specific items required further discussion. This procedure was repeated for each of the six scenarios.

After all scenarios were discussed, participants were asked to repeat the individual definition exercise. At the end of the session, participants were debriefed, remunerated via check or experimetrix credit and thanked.

Data Analysis

To assess privacy behaviors and feelings, participants' verbatim transcribed responses were coded using a qualitative coding scheme.

Segmentation & Category Development

First, all transcripts were segmented. A segment is a section of text to be analyzed. Each segment serves as one unit to be analyzed. For the purposes of this analysis, a segment is defined as, "a feeling or behavior related to privacy". Each segment may only contain one behavior or feeling. A *privacy behavior* is defined as an action or reaction of a person, more specifically, "activities in response to external or internal stimuli" (VandenBos, 2007, p. 107), whereas a *privacy feeling* is defined as, as the conscious subjective experience of emotion, or more specifically, "a self-contained phenomenal experience" (VandenBos, 2007, p. 371).

After all texts were segmented, an iterative category generation strategy was applied to construct a final coding scheme. Using this approach, one of four coders who were working simultaneously assigned a label describing the general idea of the segment.

Then, the next segment was either a) assigned the same label as the first segment if that label was appropriate (i.e., accurately describes the idea of the segment, at a higher level than the segment itself), or b) given a *new* label that describes the general idea of that segment. The same decision criterion was applied to all following segments: either label the segment with an existing code, or create a new code. After the initial coding scheme was developed, a grouping and pruning process was applied where similar categories were combined (and renamed when appropriate) and those categories containing very few segments were eliminated. This process was done collaboratively with all coders involved. Segments from these categories were reassigned to alternative categories where appropriate. When an alternative category did not exist, remaining segments were placed in an "other" category. Thus, each segment was grouped naturally by label. Discrepancies in the labeling of a particular segment were resolved through discussion until a consensus could be reached.

Coding Procedures

The coding scheme was organized hierarchically. Behaviors served as the parent code for hierarchically organized sub codes. These sub codes serve as more specific labels for each segment. For example, a segment was first coded at the highest level behavior category (avoidance, modification, alleviatory), then coded at the lowest level (e.g., be vague).

For maximum understandability, each segment was kept in context during coding. This means that although segments had already have been identified as distinct from non-segmented text, they were presented to the coder within the original surrounding text during coding so that the coder could easily examine contextual cues.

Within each dimension, segments were categorized at the lowest hierarchical level possible. For example, the segment, "When I bring my laptop to school to use… I have wireless but I always plug it in here just to sort of reduce that, that potential for stealing various information.," was coded as:

- Behavior
    - Avoidance
        - Avoid using device/system AND use alternative medium

because the segment was a *behavior* where the respondent *avoided performing some action* (in this case, use a wifi network) then *used an alternative medium* to perform the intended action (i.e., use a network cable instead of wifi). A complete version of the coding scheme is provided in Appendix D.

Intercoder Agreement

Final intercoder agreement was calculated using Cohen's Kappa, a method of calculating observer agreement of categorical data that accounts for agreements due to chance. Kappas of .61 - .80 are considered "substantial" where the only category above "substantial" is "almost perfect" (Kappas of . 81 – 1.00; Landis & Koch, 1977). Overall intercoder agreement (between the author and one other coder) at the highest behavior category level was Cohen's Kappa = .89 (i.e., almost perfect) suggesting strong agreement between coders. The authors' coding was used for data analysis.

CHAPTER 3

RESULTS OF STUDY 1: PRIVACY BEHAVIORS

In the following section I describe results from two separate but related analyses. First I present a qualitative analysis of privacy behaviors. In this analysis I identify, categorize and describe privacy behaviors across technologies and age groups. Following this analysis, I present a quantitative analysis of privacy behaviors and show how reported behaviors differ across type of technology and age group. Following the results chapter, I present a general discussion of these results in light of existing theories of privacy and how these results may influence design.

Qualitative Analysis of Privacy Behaviors

Three high level privacy behavior categories emerged from the data: avoidance, modification, and alleviatory behavior. Beneath each of these higher level categories, behaviors were grouped into lower level codes that represented more specific descriptions of types of behaviors (see Figure 4 for conceptual representation). For the purpose of discussion, there were 5 avoidance behavior categories, 5 modification behavior categories, and 5 alleviating behavior categories (though, at a different level of analysis there were arguably more sub-categories identified). In the following section I provide a description of each of the higher level groupings of behaviors (i.e., avoidance, modification, and alleviatory) as well as descriptions of the lower level groups. Direct, representative quotes, exemplifying each low level category are provided.

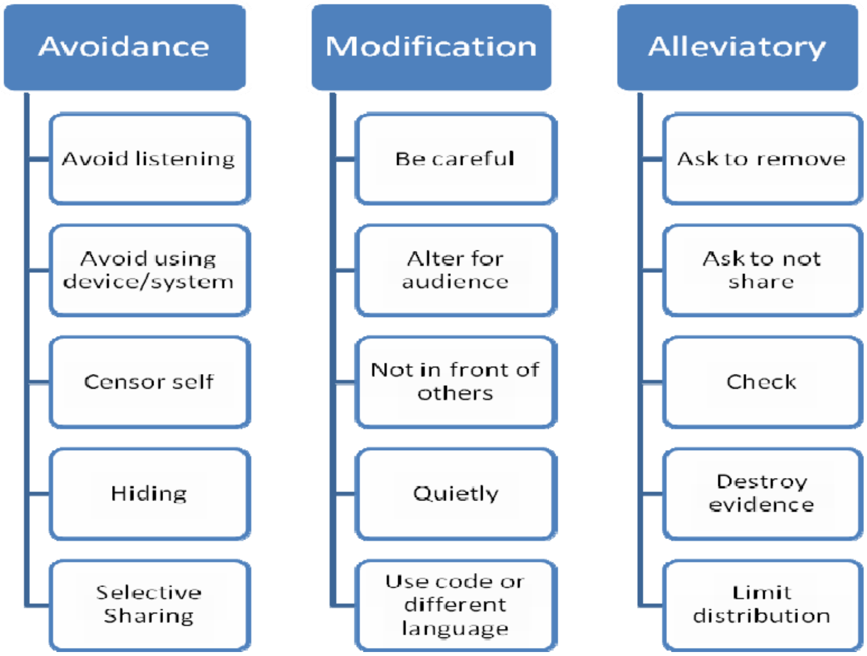


Figure 4. Hierarchical Coding of Privacy Behaviors

Behaviors clustered into three high level categories: avoidance, modification, and alleviatory. Avoidance behaviors included not performing an originally intended action because of privacy concerns and engaging in a behavior to avoid a situation where privacy would be an issue. Modification behaviors included performing an action but not in the originally intended manner. Alleviatory behaviors involved taking actions to prevent the spread of information, reduce consequences, and determine whether further (mitigating) steps needed to be taken.

Avoidance Behaviors

Participants discussed a variety of behaviors designed to avoid situations where privacy would be a concern or would be violated. For example, participants hid private information so that it was not available to others (thus avoiding the spread of information), avoided using devices/systems when they thought use of the system would result in a breach of privacy, and avoided behaving in the way the originally intended by censoring their actions and words when they thought their privacy was at risk. The most commonly reported avoidance behaviors were: avoiding using a device/system, censoring the self, and selective sharing. Each of these behavior categories is described in detail below; a summary of avoidance behaviors is presented in Table 8.

Table 8. Avoidance Behaviors

Category	***Description***	***Examples***
Avoid listening to someone else	Try not to listen to other people's conversations	"Turn a deaf ear and forget about it."
Avoid using device/system	Avoid using a system because of privacy-invasive features	"I remember seeing a commercial where your friends could pull out their cell phone and they could see you as a dot on that. And when I saw that, I thought there is no way I'd ever get that cell phone."
Avoid using device/system AND use alternative medium	Avoid using a system because of privacy-invasive features AND use an alternative system to accomplish same task	"If I'm ordering something from Gap, I'll just go and get it from Gap."
Avoid those devices/systems where security assurance not provided	Avoid using a system specifically because security assurance is not provided	"Maybe just same difference for a wireless network, some are secured and some are not. If it's not secured then I might not want to even access my e-mail through that."
Censor self (by not doing something or not saying something)	Refrain from performing an action or saying something	"If I feel uncomfortable telling it to them, I won't tell it to them."
Hiding	Hide self or some information	"Well, I would just make sure that I keep it somewhere very safe, and not just like put it anywhere in my house where people could just pick it up and look through it. I would keep it somewhere hidden."
Selective Sharing (content & recipient)	Refrain from sharing content or by selecting recipients	"You could choose what you want to say, too."

Avoiding using a device/system

Participants reported having avoided using devices/systems in the past because of privacy concerns and also that they would avoid devices/systems they had not used before, but that were mentioned during the focus group discussion. As an example of the former, one participant reported that he had stopped using one instant messaging system in exchange for a different system because of experiences he had where he unintentionally disclosed information to an unintended recipient:

> "The old AIM, I use Trillian now, but the old AIM right when someone messages you, then it becomes, that window gets the focus. So, if you're typing something to someone else or going to a website and then right when they IM you and that screen comes up, and then you're, you have to go directly there, you press enter. Then they see exactly what you were typing to someone else or for someone else... That's why I got out of AIM and I started using Trillian."
> -YA Male

In this case, the participant was unhappy with his ability to control what information was transmitted to which recipient. He decided to avoid this system in the future, and chose to use a different system where this control was easier to maintain instead.

Participants also reported that they would avoid using certain devices/systems if they felt the device/system collected, stored, or transmitted information about them to someone they did not want to have this information. For example, participants reported that they would avoid cell phones that tracked and transmitted their location, refuse to use a credit card in an online purchase, and refuse to share photos online because these technologies would provide information to unintended or unknown entities. Other participants mentioned that they would only use such systems if given security assurance such as the "little lock at the bottom right" (Male, YA) referring to SSL encryption icon in some internet browsers (e.g., Firefox), or only using a secured wifi network (vs. an unsecured network).

Censoring the Self

Another commonly reported behavior was self censoring. In this category of behavior, participants avoided taking certain actions or saying things because of privacy concerns. For example, one participant described how her concerns about privacy led her to behave in a way that is different from how she would have otherwise behaved:

> "you know…when you're in an elevator and you see there's a security camera and like… if it's really obvious you get kind of conscious about like…how you're standing or what you're doing. Like you're not going to scratch your butt in front of the camera."
> -YA Female

In this case, the participant becomes aware that she is under observation from a security camera, begins to feel self-conscious, and refrains from performing an action that she feels would be inappropriate for (unspecified) other people to observe.

Similarly, participants reported censoring themselves with respect to speech. Participants avoided certain topics (e.g., religion, politics) altogether, and also reported that they would avoid discussing topics that were "sensitive", "serious", or "touchy". This behavior is distinct from selective sharing in that comments categorized as self censoring were behaviors where topics were avoided altogether, whereas in selective sharing participants choose to share some pieces of information, while refraining from sharing others.

Selective Sharing

Selective sharing took two distinct, albeit related, forms: content restriction and recipient restriction. Both forms of selective sharing involve withholding information. In content restriction, a person refrains from sharing some pieces of information while sharing other pieces of information. In recipient restriction, a person refrains from sharing with some people, while sharing with others.

Content restriction

Content restriction behaviors are those behaviors where a person withholds certain information, but shares other information. This is different from censoring the self in that censoring the self involves completely avoiding performing an action or discussing a certain topic, while content restriction involved limiting what is shared. For example, in a medical context if a participant was engaged in censoring behavior, they would completely avoid a topic they considered embarrassing. On the other hand, if they were engaged in content restriction behavior they would share certain parts of the embarrassing information but avoid mentioning the most embarrassing parts. As a specific example, one participant described a situation where they engaged in content restriction behavior:

> "And some of the symptoms, if I did have them I might not necessarily put them on [the paperwork] because it's a little, it might be, it might come across a little awkward."
> -YA Male

Recipient restriction

Recipient restriction is where a person withholds information from some people, but shares the same information with other people. In recipient restriction, similar to censoring the self, whole topics may be avoided, but notably, only avoided in the presence of certain people; here the *person* rather than the topic is the focus of the comment (i.e., segment). In recipient restriction, the focus of the restricting behavior is on the person who would receive the information. The intent of the behavior is to withhold information from some people, but not others. For example, one participant described a situation where they were interested in discussing something with their family but had to wait for a friend to leave the conversation before they could speak freely:

> "Or it could be a family, a whole family, sitting down with one friend. And you don't want that one friend to hear that, you let the friend go, then you start the conversation over again."
> -OA Female

In this case, the recipient is the focus of the avoidance behavior, rather than the topic per se.

Summary of Avoidance Behaviors

Avoidance behaviors are ones where a participant engages in behaviors to avoid situations when privacy would be a concern. These include refusing to perform certain actions, discuss whole topics, discuss certain parts of a topic, or disclose information to certain people. Avoidance behaviors are related yet distinct from modification behaviors and alleviatory behaviors, both of which are introduced below.

Modification Behaviors

When participants chose to engage in a situation rather than avoid it, they often modified their behaviors for privacy reasons. These modification behaviors included taking extra care ("being careful"), being vague and/or limiting the depth of the things they said, otherwise modifying what they said so as to be appropriate for a particular audience, not doing/saying something in front of others, doing/saying quietly, and using a code or different language. The most commonly reported modification behaviors were being careful, not [doing/saying something] in front of others, and being vague. Each of these modification behaviors is described in detail below.

Being Careful

Across scenarios, participants reported that there were times when they had to exert effort to be careful, take extra care, or be cautious. Often participants reported that they needed to be careful with respect to what they said. For example, one participant explained that when talking to a friend, "the wisest thing is be careful with your conversation" (OA Male). Other participants noted that they needed to be careful with their behaviors: "It is something [others taking photos of you] you need to be careful of because, like you [another participant] said, I mean you don't necessarily want everybody know what it is that you were doing" (YA Female).

Not in Front of Others

Often participants would modify their behavior to ensure that they were not within earshot or line of sight of other people. Here, participants explicitly described behaviors intended to put physical distance between them and others. This could include behaviors where a dyad or group moved to be out of range of others, or an individual who moved to be out of range of everyone else. For example, one participant explained how she moved to a location where she could not be heard by others when she received a call from her physician:

> "I had an appointment like last week and they called me to like confirm my appointment, or they called me back so I could make an appointment. I was at work, and there was like three guys in the room. I definitely like went like out in the hallway."
> - YA Female

In addition to being out of earshot or line of sight of other people, participants also described that they took steps to be out of range of some technologies. For example, one participant described that he made attempts to try to "get away from any recording device" (YA Male) when he discussed "work deals" he did not want others to know about.

Being Vague

Another way participants modified their verbal behavior, in particular, was by being "vague." This could include being purposefully unclear, using double entendre (i.e., making meaning ambiguous), or simply leaving out details. Often participants explicitly described their behavior as "being vague" (verbatim quote), but also included in this category are quotes that express similar meaning. For example, "be general about it" (YA Male), don't "go into any detail" (OA Female), explain things "not in full detail" (YA Male). Being vague is similar to content restriction and censoring self in that the idea behind all three is to limit the outflow of information. However, each accomplishes this goal in a different way (see Table 9). In being vague, participants take actions to make the meaning of what they are saying ambiguous, except, perhaps, to someone who already has preexisting knowledge. In content restriction, participants are clear in what they say, but they limit what they say, and in censoring the self, participants avoid discussing topics altogether. In "limiting distribution" which is an alleviatory behavior described in the next section, participants describe how they limit the ways information that has already been collected is disbursed.

Table 9. Controlling the Outflow of Information

Censor Self	Content Restriction	Being Vague	Limit Distribution
Avoid discussing entire topics (e.g., "sensitive" topics, religion, politics)	Avoid sharing some content, but share other content fully (e.g., leave out embarrassing details)	Be purposefully ambiguous, use double entendre, leave out details so that only one someone with prior knowledge may understand (e.g., "I'm not feeling wel.l" vs. "My arm is oozing."	After information has flowed out and collected, limit how much further information is transmitted (e.g., "don't post it [a photo] on facebook")

Alleviatory Behaviors

The final group of reported behaviors was alleviatory behavior. Alleviatory behaviors occur only after information has been collected and involve actions taken to prevent the spread of information, reduce consequences, and determine whether further (mitigating) steps need to be taken. Alleviatory behaviors fell into one of two broad categories: external locus and internal locus. External locus meant that someone besides the participant had control over the piece of information in question, whereas internal locus meant that the participant had direct control over the information. Both categories of behavior are described in detail below.

External Locus

External locus alleviatory behaviors are behaviors that involve asking a person (other than the participant) who was in control of the participant's information to take some action on behalf of the participant. These included asking the person not to share information in the first place or asking the person to remove information, or "un-share", information that was currently shared. For example, one participant explained how he would ask someone not to share a photo of him with others: “I’d just say hey do you mind not showing that one?” (YA Male). If information had already been shared but sharing was not desired, participants reported that they would ask others to take down the information. For example, also with respect to a photo, one participant stated that they would ask the person who posted the photo to simply “untag it” (YA Female), referring to the tagging feature on the social networking site facebook that allows the owner of a photo to “tag” people in the photo associating the image with the name and identity of the person in the photo.

External locus alleviating behaviors were behaviors that, by nature, involved asking someone else (besides the participant) to take some action because at that point in the information cycle, the other person was the one who had control over the information. In Internal locus behaviors, on the other hand, participants themselves had control over their information.

Internal Locus

Internal locus alleviating behaviors were behaviors that involved information that the participant was in control of. These behaviors included limiting distribution, destroying evidence, checking, requesting permission, altering information/images, and claiming innocence. Of these behaviors, limiting distribution, destroying evidence, and checking were the most common.

Limiting Distribution

Limiting distribution has to do with limiting the transmission of information that has already been collected. After an act has been committed, whether modified or not, and collected by some means it can either be transmitted or not transmitted (distributed or not distributed). Along this continuum of transmission from not shared with anyone to shared with everyone, there are countless (though perhaps reasonable categories of) points in between (see Figure 5). Limiting distribution includes limiting the transmission of information by attempting to ensure that sharing falls somewhere short of "shared with everyone."

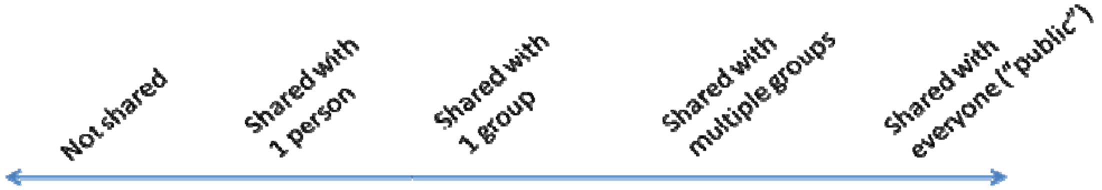


Figure 5. Continuum of Sharing

When participants described limiting distribution, the topic they most often discussed was photo sharing. Participants described how after photos of them had been taken they would limit the distribution of those photos by not sharing them with others. They reported that they would not share them online, on facebook, or by showing hard copies to others. In some ways limiting distribution mirrors selective sharing of content, however a key difference is that selective sharing of content occurs before an act is committed, and limiting distribution only occurs (and can only occur) after an act is committed *and* recorded. As with selective sharing, when participants described limiting distribution, they not only talked about limiting distribution of content, sometimes they also discussed limiting distribution to certain others. One participant described how he "would just make it [a set of photos] so my friends could see it," (Male YA) while another participant framed sharing in terms of who could *not* see the photos: "but definitely I wouldn't want certain people, like my parents, seeing [all my photos]" (Male YA).

Destruction of Evidence

Related, but worth discussing separately, is destruction of evidence. In this behavior participants described an extreme version of ensuring that evidence of some past act (act here could be as simple as disclosing a name and address) would not be shared with anyone in the future: purposefully destroying evidence of the act. Participants described destroying photos, destroying devices that recorded their actions, shredding old credit cards, shredding physical mail, and deleting internet browsing history. In all of these cases information about a participant had already been recorded and the participant described behaviors designed to destroy this record.

Checking

Checking behavior involves taking effort to inspect information about a participant that is kept by others. This may include inspecting records to ensure that (usually financial) information is not being used without permission and inspecting other documents (such as friend's facebook pages) to identify what information, related to the participant, is being shared with others. Participants described checking credit card bills and online interim statements to make sure there were no erroneous charges: "I kept checking my credit card to see if anyone made like ridiculous charges" (YA Female); "you have to make sure you check them all the time" (OA Female) and checking to see if photos of them had been posted online. Notably, participants felt that it was their responsibility to engage in checking behavior to avoid unintended consequences: "If you're not checking, then it's kinda your fault, too" (YA Female).

Summary of Qualitative Analysis of Privacy Behaviors

Three high-level privacy behavior categories emerged from the interview data collected for this study. The three behavioral categories were avoidance, modification, and alleviatory behavior. Within each high-level category, I identified lower level behaviors that were composed of more specific subcategories of behavior. Many of the reported behaviors were related to sharing specific information with some people while keeping it from others. In the previous section I provided a description of each behavior and behavioral category. In the following section I present an analysis of how the frequency of reported behaviors differed with respect to age and type of technology (scenario).

Quantitative Analysis of Privacy Behaviors

After behaviors were coded into categories, the number of behaviors in each high-level category (i.e., avoidance, modification, and alleviatory) were subjected to chi-square analyses to determine whether there were quantitative differences in behavior across type of technology and with respect to age. An alpha level of .05 was used for all statistical tests.

Behavior Distribution

A chi-square goodness of fit test was performed to determine whether the three behaviors were reported equally. Overall, participants reported more avoidance behaviors than modification or alleviatory behaviors χ^2 (2, N = 507) = 78.96, p = .001.

	N
Avoidance	261
Modification	141
Alleviatory	105

Reported Behaviors by Age Group

A chi-square test of independence was performed to examine the relationship between age group and reported behavior. Type of reported behavior differed across age group χ^2(2, N = 507) = 22.73, p = .001.

To determine which cell or cells produced the statistically significant results, residuals (the difference between the observed frequency and the expected frequency) were converted to z-scores and compared to a critical value corresponding to an alpha of 0.05 (i.e., +/- 1.96). Avoidance behaviors were overrepresented for older adults, whereas alleviatory behaviors were overrepresented for younger adults (α's < .05; see Table 10). The number of modification behaviors reported was similar for older and younger adults.

Table 10. Percentage of Reported Behaviors by Age

	Younger Adults	***Older Adults***
Avoidance*	45%	62%
Modification	28%	27%
Alleviatory*	27%	11%

Note: Percentages were rounded.
* p<.05

Behavior across Scenario

For the purpose of analysis of behavior across scenario, data from older and younger adults were combined (separately some cells contained less than 5, the minimum for chi-square analysis). Despite being reported with the greatest frequency overall, avoidance behavior was not the most commonly reported behavior across all scenarios. For example, in photo sharing alleviatory behaviors were most common and in health disclosure modification behaviors were most common. To assess these differences across scenarios, adjusted residuals were examined (as described above).

Photo Sharing

With respect to photo sharing, participants most often described alleviatory rather than avoidance or modification behaviors (Table 11). For example, participants mentioned limiting distribution of photos by not uploading them to a photo sharing or social networking site (e.g., facebook) more often than avoiding taking the photo in the first place.

Table 11. Photo Sharing

	Photo Sharing
Avoidance*	35%
Modification*	11%
Alleviatory*	55%

Note: Percentages were rounded.
*p<0.05 (i.e., category is significantly over or underrepresented)

Identity Theft

For the identity theft scenario, avoidance was the most commonly reported behavior (Table 12). For example, participants reported that they would refuse to give a credit card number over the phone (FG2), "try to find somewhere else to go where you can go hide in the corner" (FG2), use a wired internet connection instead of wireless (FG3), refuse to use a wireless network that was not secured, use an alternative payment system (cash instead of a credit card), purchase an item at a brick and mortar store rather than an online store, and use a service like pay-pal instead of pay with a credit card. They also would not type personal information while in a crowded room where what they were typing might be visible (FG2).

Table 12. Identity Theft

	Identity Theft
Avoidance*	61%
Modification*	15%
Alleviatory	25%

Note: Percentages were rounded.
*p<0.05 (i.e., category is significantly over or underrepresented)

Health Disclosure

For the health disclosure scenario, modification was the most frequently reported behavior (Table 13). Participants reported that they would not share certain pieces of information while in a waiting room in front of other patients, would be vague when describing their medical conditions, and would whisper or speak quietly so others would not hear what they were saying to a health care provider.

Table 13. Health Disclosure

	Health Disclosure
Avoidance	44%
Modification*	49%
Alleviatory*	8%

Note: Percentages were rounded.
*p<0.05 (i.e., category is significantly over or underrepresented)

Location Tracking

For the location tracking scenario, avoidance was the most commonly reported behavior (Table 14). Participants reported that they had refused to use devices because they contained location tracking functionality, would turn off a system if it had location tracking functionality, would turn off the function itself, would restrict the level of detail about the content of their location and would restrict who might have access to this information.

Table 14. Location Tracking

	Location Tracking
Avoidance*	70%
Modification	24%
Alleviatory*	6%

Note: Percentages were rounded.
*p<0.05 (i.e., category is significantly over or underrepresented)

Surveillance

For the surveillance scenario, avoidance was the most commonly reported behavior, though all behavioral categories were reported with expected frequency (Table 15). Participants reported that they would censor their own behavior and not engage in risky behaviors (e.g., not run red lights) while being surveilled.

Table 15. Surveillance

	Surveillance
Avoidance	67%
Modification	22%
Alleviatory	11%

Note: Percentages were rounded.
*p<0.05 (i.e., category is significantly over or underrepresented)

Self-Disclosure

For the self-disclosure scenario, avoidance was the most commonly reported behavior (Table 16), though they were reported with the expected frequency. Modification behaviors, on the other hand, were reported more frequently than expected. Modification behaviors included being careful with what was said, not saying certain things in front of other people, and being vague.

Table 16. Self-Disclosure

	Self-Disclosure
Avoidance	57%
Modification*	40%
Alleviatory*	3%

Note: Percentages were rounded.
*p<0.05 (i.e., category is significantly over or underrepresented)

Summary of Quantitative Analysis of Privacy Behaviors

During the qualitative analysis, three high level privacy behavior categories emerged: avoidance, modification, and alleviatory behavior. In the quantitative analysis, I examined how the frequency of reported behaviors differed with respect to age group and technology type. Overall, participants were most likely to report avoidance-related behaviors. However, in further analyses, older adults reported more avoidance behaviors than expected, whereas younger adults reported more alleviatory behaviors than expected. In addition, reported behaviors differed across different technology types. In the following section I will discuss the implications of these results on existing theories of privacy and present implications for design.

CHAPTER 4

DISCUSSION OF FOCUS GROUP RESULTS

In this study I examined users' everyday privacy behaviors. Based on this examination I determined that there were a variety of privacy behaviors, but that there were also commonalities in reported behaviors. Behaviors grouped into one of three categories: avoidance, modification, and alleviation. Within each of these high level groups, sub-behaviors were also identified and described. Behaviors were reported with differing frequency across technology context (scenario) and reported with different frequency by each of the two age groups.

The behaviors and sub-behaviors identified have a number of implications both in terms of theory and in terms of design. The remainder of the discussion is organized as follows: First, I discuss how the identification of groupings of everyday privacy behaviors across technologies suggests an alternative to the claim that privacy is too contextual a topic to understand at a psychological level. Instead, I propose that the commonalities identified in this study suggest a way to organize many of the previous findings in privacy and HCI. Then, I contrast the groups of privacy behaviors identified in this study to Altman's proposed privacy regulation mechanisms and show how the alternative grouping may be useful to designers. Next, I discuss the findings in relation to Altman's model of privacy regulation and suggest that Altman's model does not reflect users' privacy behaviors. Then, based on the empirical investigation, I propose an alternative model of privacy regulation. Finally, I discuss how these theoretical contributions relate to design.

Theoretical Implications

The results of this study suggest that common privacy behaviors (e.g., avoidance, modification and alleviation) exist across technologies and contexts. This result is to some extent inconsistent with a general claim in the privacy literature: that it is impossible to draw generalities about privacy in HCI. Multiple previous reports state that the experience and definition of privacy is different for everyone. For example, Ackerman and Maiwaring (2005, pg. 6) claimed that privacy is “extremely contextual, based in the specifics of by who, for what, where, why, and when a system is being used” and Karat, Karat and Brodie (2008) claimed that, “privacy can and does mean different things to different people.” The sentiment underlying both of these statements and the many others making similar claims (see Caine, 2008 for additional discussion) is that because privacy is different in different contexts and across people, researchers cannot gain a basic understanding of privacy and that privacy must be studied, not at a general level, but only at the level of an individual technology.

This study suggests an alternative to this view. I propose that the results of this study suggest that there are commonalities in the way people discuss and behave with respect to privacy. In addition, the commonalities identified in this study suggest a way to organize many of the previous findings in the field of privacy and HCI. For example, the finding that girls reported taking a phone to a private area of the house to have voice conversations (March & Flueriot, 2006) could be classified under “hiding” (an avoidance behavior), and the access control technology that utilizes testing for shared knowledge developed by Toomin, Zhang, Fogarty & Landay (2008) could be considered a solution to the issue of selective sharing. As described in the following section, the categories identified in this study are different from previous categorizations of privacy behaviors.

Everyday Behaviors vs. Behavioral Mechanisms

Altman (1975) proposes that people use behavioral mechanisms to achieve privacy goals. In his conceptualization, if a person recognizes that they have less privacy than they want, they may engage in behaviors designed to lessen their interaction; alternatively, if a person recognizes they have more privacy than they want, they may engage in behaviors to increase their interaction.

To describe this notion, Altman introduces the ideas “interpersonal control” and “interpersonal boundary regulation,” both of which refer to the notion of a person “maintaining an appropriate and desired level of interaction between themselves and the external physical and social environment.” To maintain the appropriate level of interaction, people regulate privacy to a desired level by using behavioral mechanisms (Table 17). Behavioral mechanisms used to achieve privacy goals include verbal behavior, paraverbal behavior, nonverbal behavior, personal space, territoriality and culture (Altman, & Chemers, 1980; Altman 1975).

Table 17. Behavioral mechanisms used to regulate privacy.

Behavioral Mechanism	Definition	Examples
Verbal	the contents of what a person says	Saying: • "Let's talk" • "Can I raise an issue with you" • "Sorry, I'm too busy now" • "No, I can't make it this evening"
Para Verbal	way of speaking, how someone says something	Speaking in a cool or warm tone
Non Verbal	communication without words including posture, gaze, facial expressions and gestures	• body orientation • turning away • smiling • grimacing • frowning • looking away • fidgeting with own clothing • rubbing own hands together • looking at our watches • assuming rigid, symmetrical body positions
Personal Space	"the space within an invisible boundary around people that is with them everywhere they go." (Altman & Chemers, 1980, p. 102)	• increase or decrease physical distance between self and another person o by backing away o by moving closer
Territory	control and ownership of a place by a person or group	• invite someone into a territory they occupy • closing a door • use signs saying keep out or welcome • offering a chair • providing refreshments • not inviting in
Culture	customs, rules and norms which communicate availability to other members in the same culture	• not dropping by a friend's house at dinner time • too early in the morning or too late at night avoiding • coming to parties too early and leaving at a reasonable hour • not opening shut doors (at least without knocking) etc.)

(Altman & Chemers, 1980; Altman, 1975)

However, because of the general nature of Altman's grouping of behavioral mechanisms, designers find it difficult to guide design: "It is by no means an easy task to apply Altman's theory of privacy to the problem of designing." (Boyle, 2005). Because Altman's analysis was top down, the mechanisms identified may not represent users' ideas about privacy, especially as it relates to technology. The grouping of behaviors in this study was not imposed top down as Altman's was. Instead I used a bottom up category generation coding strategy; groups of behaviors emerged from the data. Thus, unlike Altman's top down, conceptual analysis of privacy and categorization of privacy behaviors, the categories of everyday behaviors identified here are centered on users' privacy vocabulary and experience. I propose that the alternative grouping of privacy behaviors described in this paper may prove to be more useful to designers and researchers. For example, as described above, these categories of everyday behavior suggest a way to organize previous findings from the privacy literature. I reserve a discussion of design implications for a separate section but will note here that the alternative categorization suggests multiple design options.

Besides questioning Altman's behavioral mechanisms of privacy, I also question Altman's model of privacy regulation. In the following section, I present a critique of Altman's model of privacy regulation and suggest an alternative model.

Proposing an Alternative Model of Privacy Regulation

The model of privacy regulation that Altman proposes is that of the "shifting permeability of a cell membrane" (Altman, 1975). The membrane can be more open or less open depending on the desired level of privacy (see Figure 6).

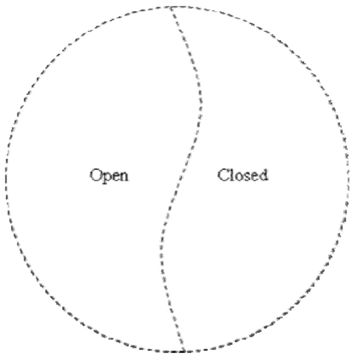


Figure 6. Adaptation of Altman's Model of Privacy Regulation

In this hypothetical personal boundary the cell membrane may be more open—where it is more receptive to interaction with others—or more closed where the “self” is less open to interaction. Altman argues that this regulation is dynamic, meaning individuals, influenced by changing conditions, open or close themselves to others resulting in a desired level of interaction. Privacy is considered an optimizing process where people seek to interact not too much or too little, but at an optimal level. This openness/closedness cycle vacillates as if on a wavelength, suggesting that people will be more open, on the whole, then less open, on the whole.

However, this analysis of privacy behaviors indicates that participants wanted to *withhold information from some people while sharing with specific others*. The idea of sharing specific information with specific others is contrary to Altman’s conceptualization of information sharing as like a “cell membrane”. In his conceptualization, information sits behind a permeable wall. Information to be disclosed can pass through the permeable wall therefore being exposed to others. However, participants in the current study suggested a different model of boundary regulation where each piece of information was distinct AND each recipient was distinct. Thus, information could pass to one person without being exposed to all others.

For example, in selective sharing, participants not only wanted to selectively share content, they also wanted to selectively share with different people. This finding provides empirical support for Westin's theoretical conceptualization of privacy as "the claim of individuals… to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin, 1967; p. 7) while running contrary to the conceptualization to Altman's model of privacy regulation. Unlike a cell membrane, participants in this study described behaviors that allowed for them to be simultaneously open to some people while closed to others. Thus, I propose an alternative model of privacy regulation that reflects participants' descriptions of privacy (Figure 7).

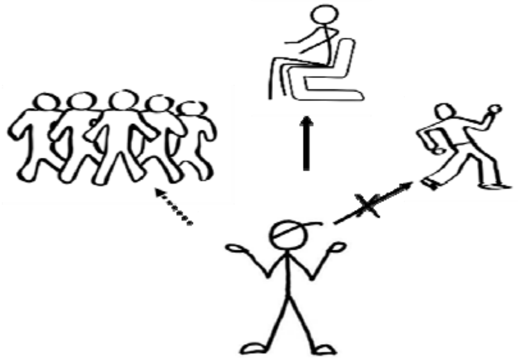


Figure 7. Alternative Model of Privacy Regulation

In this alternative model of privacy regulation, a person may share some information with some people, all information with another person and no information with another person simultaneously. This implies that protecting privacy involves allowing people to share *what* they want to share with *whom* they want to share with while keeping the same information from others. This is consistent with multiple previous examinations of privacy in HCI that have suggested that one piece of information may be considered more or less private depending on whom that piece of information was going to be shared with (e.g., Adams, 1999; Consolvo et al., 2005;

Hawkey & Inkpen, 2005; Khalil & Connelly, 2006; Lederer, Mankoff, & Dey, 2003; Muller, Smith, Shoher, & Goldberg, 1991; Olson, Grudin, & Horvitz, 2005; Patil & Lai, 2005).

One prediction of the alternative model of privacy is that there will be an *information type* by *information receiver* interaction (see Figure 8). That is, neither the type of information, nor the information receiver alone predicts the level of perceived privacy of an event. Rather, it is both of these variables in combination that predict the perceived privacy of an event. For example, a high privacy information type (e.g. location information) may not be considered highly private when the information receiver is a spouse or significant other. However, if the information receiver is a stranger then location information will be considered highly private (e.g., Khalil & Connelly, 2006).

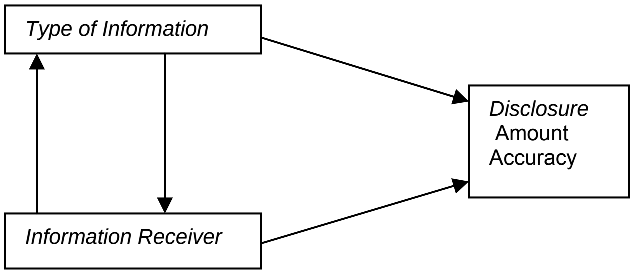


Figure 8. Information Type by Information Receiver Interaction

When we examine previous studies where both variables have been observed in combination, the relationship of perceived privacy (often operationalized as privacy comfort level or sharing preference) indeed differed based on both information type and information receiver. For instance, in a study of web browser use, privacy comfort level was influenced by a combination of viewer (information receiver) and sensitivity of content (information type; Hawkey & Inkpen, 2006). Similarly, for a project management groupware system, users who engaged in participatory design wanted to restrict sharing different aspects of projects with a variety of potential information receivers (Mueller, Smith, Shoher & Goldberg, 1991).

If these variables truly interact then it may not be appropriate to examine either in isolation as the results may appear contradictory, leading to the conclusion that "privacy means different things to different people". For example, to find out which types of information people consider the most private we need to specify an intended recipient or else risk that each participant imagines a different potential receiver of such information. It is likely that participants would perceive an invasion of privacy if we ask about giving out social security number, credit card information and birth date to "the public". However, if we specify "your credit card company" as the receiver of such information, participants are less likely to claim an invasion of privacy.

However, the alternative model of privacy presented here may not fully address the additional considerations that technology brings to privacy. A possible reason for the increase in concern over privacy is that technology changes the storage, search ability, reproducibility and availability of data and therefore may fundamentally change the conception of privacy (Sparck-Jones, 2003). For example, if users realize that their data is stored for a longer period of time, more easily searched and reproduced more readily, their concerns about privacy may multiply. In the next section I propose an additional consideration for privacy in HCI.

Proposing Multi-Stage Disclosure

In general, the three categories of behavior that emerged can be thought of in a temporal order. Avoidance behaviors occur prior to some act, modification behaviors occur during an act, and alleviating behaviors occur after an act. However, because privacy may become a concern (or be realized as a concern) at more than one point in the life of a piece of information, this relationship is not perfect. In a non-recorded environment (no technology), an act is ephemeral; once it has been performed it is gone. It may exist in the memory of the actor or an audience member if there is one present. However, besides by being described and/or demonstrated by the actor or audience member, the act cannot be transmitted directly (reproduced) to any other entity. In an environment where technology (e.g., recording equipment) is present, the case is different. In a recorded environment an act, once captured, may be transmitted to any number of recipients. Therefore, disclosure in a technologically mediated environment is a multi-stage process.

That is, opportunities for disclosure decisions occur in at least two separate moments. The first moment is prior to the first disclosure or act. At this moment, an individual considers whether he or she wants to act in front of or disclose to another person or group of people. At the second moment, an individual, realizing that information about them has been captured using some technology, then considers whether they want to disclose the information artifact to another person or group. Technology transforms the once single stage process of disclosure to a multi-stage process. As a result, designers should consider not only preserving privacy by designing for initial disclosure, but also at moments of secondary disclosure. In the next section I focus exclusively on suggestions for design.

Opportunities for Design

People have been managing privacy in non-mediated settings since pre-civilization (Westin, 1967). Humans have developed many strategies for managing privacy that are intuitive, easy to use, and successful (i.e., useful for privacy management). Despite the facility with which people are able to manage privacy in non-mediated settings, designing technologies that are privacy-sensitive has proven to be very difficult (e.g., within the ubiquitous computing domain; Lederer, Hong, Dey, & Lanaday, 2004). In the following section, I provide a number of suggestions to designers of privacy-sensitive systems to consider for helping people manage their privacy in a more intuitive way and propose opportunities for design.

Support Users' Existing Behaviors

For most scenarios (with the exception of the surveillance scenario) there was a category of behavior that represented a majority of the reported behaviors. By examining the most frequently reported behavior from each scenario we may be able to determine how to support the behaviors users are already accustomed to using in a particular context.

For example, the majority of behaviors reported for the photo sharing scenario were alleviatory behaviors. This suggests that people are currently waiting until after a photo has been taken and perhaps shared to begin managing privacy associated with the photo. Although one explanation for the difference in behavior could be due to a lack of awareness about what was captured in the photo, participants' comments reveal an alternative explanation, one that mirrors the high-level finding of sharing with specific people: participants wanted to have photos and share those photos with certain people, but there were specific others they did not want to share with. For example, one participant described how she did not want to share already-taken photos on facebook because someone else would be jealous:

> "Yeah, I've had to deal with that 'cause one of my like best guy friends; I liked him prior to like me dating my boyfriend now… my boyfriend doesn't care… but, his girlfriend apparently is like really jealous. And so, like we like go to football games, or we like we'll meet for coffee, and like he's asking like specifically … don't like load up… my facebook with pictures of us. Like I don't care, but I don't wanna hear about it from her. And she knows who I am, and it's not even that like I'm a threat, but she's still like. It would cause unnecessary issues between them, so I just don't do it because of that kind of thing."
> -YA Female

This implies that designers should consider ways to enable users to easily share already-collected information with certain others and also engage in alleviatory behaviors, such as checking, destroying evidence, and asking others to remove or not share information about them.

As another example, in general, older adults reported more avoidance behaviors than expected, whereas younger adults reported more alleviatory behaviors than expected. This could be due to younger adults' previous experience with technology, especially technology that captures, stores, reproduces, and/or transmits captured information to others. Based on this finding, one suggestion could be to highlight avoidance behavior options in interfaces for older adults and highlight alleviatory behaviors in interfaces for younger adults. Designs that focused on making these types of behaviors easier for users would likely seem intuitive for users since this is how they report managing privacy. However, supporting users' existing behaviors is not the only design strategy that makes sense. Another strategy that may be used is to create supports where few strategies exist.

Create Supports Where Few Strategies Exist

The idea of creating supports where few strategies currently exist is the counterpoint to the previous suggestion to support users in existing behaviors. As opposed to supporting the types of behaviors users are already engaging in to manage their privacy, this is an opportunity for designers to create support where it is currently difficult or unlikely for users to engage in privacy regulation behaviors.

The location tracking scenario is an example where participants reported a high number of avoidance behaviors. Thus, there is an opportunity to design alternatives that are inspired by modification or alleviation (which were both significantly underrepresented).

As another example, participants reported very few avoidance or modification behaviors during the discussion surrounding the photo-sharing scenario. Thus, there is an opportunity to design technologies aimed at supporting avoidance or modification privacy behaviors. One suggestion for an avoidance-enhancing technology for photo sharing could be a camera that requests an approval from the person in the photo before a photo is shared with others. This suggests an alternative model of ownership, where the subject of a photo becomes part owner of the content, rather than the photographer taking full ownership and control over the destiny of the photo.

One notable point here is that avoidance behaviors were the most commonly reported behaviors across all scenarios. A substantial portion of these avoidance behaviors involved avoiding a specific technology in favor of another technology or method. This finding is consistent with other reports that privacy concerns lead to lack of adoption among technologies (e.g., Herbsleb, Atkins, Boyer, Handel & Finholt, 2002; Want, Hooper, Falc & Gibbons, 1992). Thus, if designers want users to adopt their technologies it is critical to create mechanisms that enable users to easily manage privacy using modification and/or alleviatory strategies, or else risk that users will engage in avoidance behaviors and thus may reject their technologies.

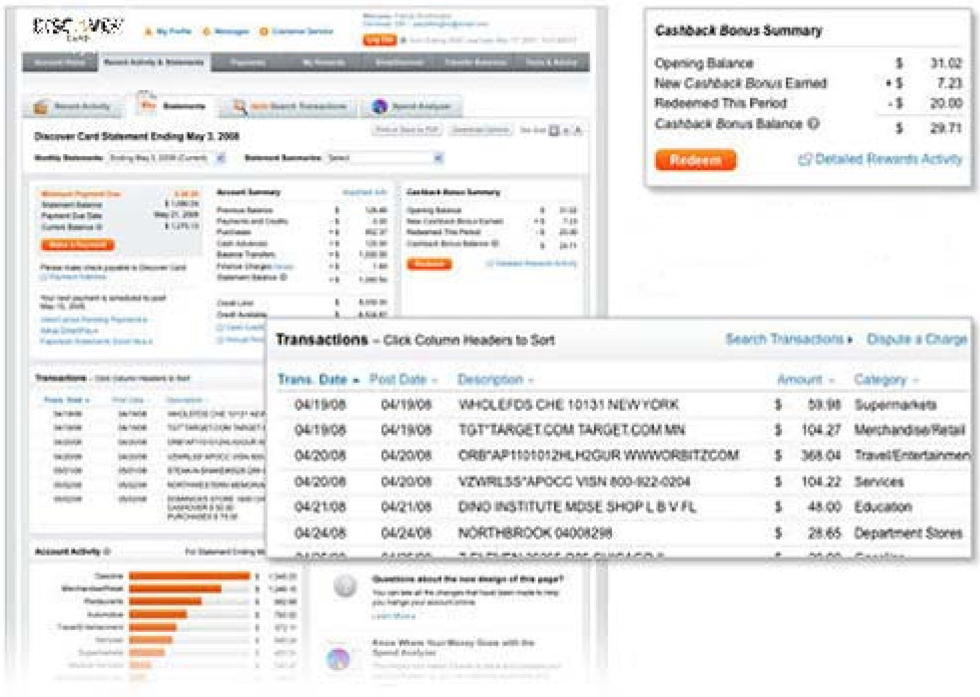
Translate Behaviors into Design

Perhaps the greatest opportunity for design lies in translating existing behaviors into digital instantiations. Participants in our study reported many different behaviors they are familiar with using and talking about. Thus, it seems likely that these ways people are already managing their privacy may inspire designs that are analogous to existing behavior.

Facilitate Checking

One behavior participants reported was to “checking” to make sure that something has or has not happened. Participants reported that they checked to see if charges were made, checked online postings to ensure they were accurate, and double checked to make sure information they planned to disclose was correct. Thus, a design implication is to facilitate checking. This could be done in a number of ways including making detailed account information available quickly as well as by providing previews and/or enhanced views highlighting information that may be particularly likely to be checked (e.g., information that had changed recently).

For example, participants often reported that they would check their monthly bills to ensure that there were no erroneous charges. One way to facilitate this behavior might be to provide up-to-the minute access to the charges on an account (see Figure 9) in an online format. An alternative way to facilitate checking would be to provide proactive cues to participants about account activity. As one example, each charge on a particular account could result in a one time audio-only notification sent directly to a cellular phone. The notification could be a pleasant chime or ding that would signal that a charge had been made, but would not represent an interruption as it would require no action from the user. Users would likely become familiar with the notification in conjunction with account activity. However, if they received a notification when they had not made a charge, they would know to investigate the charge to determine whether or not it was appropriate (thus facilitating checking in situations where it is warranted).



Cashback Bonus Summary

Opening Balance	$	31.02
New Cashback Bonus Earned	+ $	7.23
Redeemed This Period	- $	20.00
Cashback Bonus Balance	$	29.71

Transactions – Click Column Headers to Sort

Trans. Date	Post Date	Description	Amount		Category
04/19/08	04/19/08	WHOLEFDS CHE 10131 NEWYORK	$	59.98	Supermarkets
04/19/08	04/19/08	TGT*TARGET.COM TARGET.COM MN	$	104.27	Merchandise/Retail
04/20/08	04/20/08	ORB*AP1101012HLH2GUR WWWORBITZCOM	$	368.04	Travel/Entertainmen
04/20/08	04/20/08	VZWRLSS*APOCC VISN 800-922-0204	$	104.22	Services
04/21/08	04/21/08	DINO INSTITUTE MDSE SHOP L B V FL	$	48.00	Education
04/24/08	04/24/08	NORTHBROOK 04008298	$	28.65	Department Stores

Figure 9. Example of Checking Facilitation

Another example of an everyday privacy behavior that can be easily translated in to a digital instantiation is the modification behavior “being vague”. Many participants described how in everyday interactions they modified what they disclosed by “being vague”. Participants described behaviors such as leaving out details, being purposefully unclear, or making the meaning of what they were disclosing ambiguous. Thus, one suggestion for design is to provide ways for people to share with others in a way that allows for ambiguity or not giving full detail. This everyday privacy behavior can be used to inspire an alternative “vague” input design.

For example, consider a traditional online form that requires a user to input age information (Figure 10). This type of age input may be observed in countless computer based (and pen and paper) questionnaires. This type of input field requires very specific information and does not allow a user to engage in modification behaviors such as “being vague". Rather, if a user wanted to manage privacy by being vague when encountering this form they would be left three options. First, they could attempt to leave the input field blank. Second, they could fill the input field in with incorrect information, or third they could fill the input field in with the correct information. Only the third option provides any useful information at all; the first two provide either no information or contribute bad data. Clearly, none of these options is ideal.

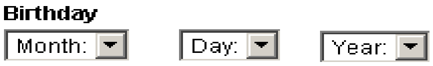
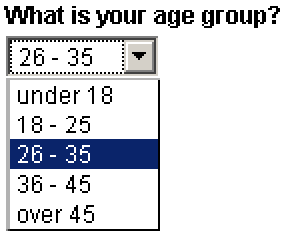


Figure 10. Traditional Age Input

Being able to be vague may be especially important if the type of information is embarrassing or potentially embarrassing. However, if information is not embarrassing, and a person is not generally anxious about privacy, why would a person *not* want to provide the exact date of their birth (or why would a designer not want to be responsible for protecting it)? Because it has been demonstrated that extremely detailed information such as birth date, especially when combined with other similarly specific data, can be used to individually identify a person. Acquisti & Gross (2009) demonstrated that information about an individual's date of birth, combined with birth location information was enough to predict the individual's Social Security Number (which can then be used for identity theft). Similar previous research demonstrated that analogous attacks including re-identification by linking could be used with large databases of ostensibly anonymized data to identify individuals (Sweeny, 2002).

Vague Input

As an alternative to asking people to provide their exact date of birth, I propose "vague input" (Figure 11). In this alternative input design, users are asked to provide their age group, rather than their exact date of birth. This is preferable from a privacy perspective because information at the group level is less susceptible to an attack as described by Acquisti & Gross (2009) and Sweeny (2002) without requiring anonymization (at least with respect to age data).



What is your age group?

26 - 35

Figure 11. Alternative "Vague" Age Input

As an additional justification, information such as age is often binned for analysis anyway. In most circumstances it is unnecessary to know the exact date of an individual's birth; rather, what is desired is a general idea of the person's age group. For example, take the example of health screenings. In this case, the information a health care practitioner requires for determining the appropriate health screenings is age group and gender, not date of birth. Cholesterol screenings are recommended for men over 30, not for people born on April 15th. Vague inputs, inspired by an everyday privacy behavior as described by participants, limits the privacy consequences of disclosing personal information, while preserving useful information.

Clearly there will be some instances where an actual birth date is required. For example, a birthday reminder will not be functional without knowing an exact birth date. However, in this case, an input for birth year is unnecessary. This suggests a higher level design implication: designers should ask only for the amount of information that is necessary. The criteria for determining what level of information that is necessary should include a careful consideration of 1) what the data will be used for and 2) what the potential harm of having more detailed information might be. In the case of exact age information, the harm could be great (e.g., Acquisti & Gross, 2009).

Summary and Interim Conclusion

In this study I examined everyday privacy behaviors as described by participants. The purpose of the focus group study was to gain a better understanding of existing privacy behaviors. In particular, a goal of this study was to categorize reported privacy behaviors across multiple circumstances and technologies to identify common themes. The results of this study suggest that common privacy behaviors exist across technologies and that these behaviors may be supported by alternative designs. Behaviors grouped into one of three categories: avoidance, modification, and alleviation. Within each of these high level groups, sub-behaviors were also identified and described. The groups of everyday privacy behaviors identified in this study suggest an alternative to the claim that privacy is too contextual a topic to understand at a psychological level. Instead, I demonstrated that there are commonalities in reported privacy behaviors across contexts.

I then suggested that these commonalities and the resulting classification provide a way to organize many of the previous findings in privacy and HCI. I also contrasted the everyday privacy behaviors identified in this study to Altman’s privacy regulation mechanisms and showed how the alternative grouping proposed here may be useful to designers. Then I discussed the findings of this study in relation to Altman’s model of privacy regulation and argued that Altman’s model does not reflect users’ discussion of their privacy behaviors. Next, based on this study, I proposed an alternative model of privacy regulation. Finally, I demonstrated how the descriptions of everyday privacy behavior may be used to inspire privacy preserving designs. One overall implication of the findings is that for technologies to effectively support privacy, they need to support the kind of nuanced disclosure that people want. One part of supporting nuanced disclosure is to ensure that the disclosure is error-free. In the following chapters I address disclosure errors.

CHAPTER 5

METHOD FOR STUDY 2 – CRITICAL MISCLOSURE INCIDENTS

A misclosure is the unintentional revealing of personal information to others while using a technology. A critical incident technique was used to examine the type, nature, and conditions surrounding previous instances of misclosure.

Critical Incident Technique

The critical incident technique (CIT) is “a set of procedures for collecting direct observations of human behavior in such a way as to facilitate their potential usefulness in solving practical problems and developing broad psychological principles” (Flanagan, 1954, p. 327). Originally, the critical incident method was developed to identify critical requirements for job fit. Using this method, Flanagan (1954) identified the characteristics of a person that made them particularly appropriate for performing a specific job (e.g., the critical requirements for an airline pilot). Since its inception, the method has also been used to identify the problems of a system, areas for improvement of a system, and has more recently been expanded to include the identification of vulnerable areas of a system that may cause problems in the future (Schulter, Seaton & Chaboyer, 2007, p. 107). In this dissertation, I used the critical incident method to explore privacy-related problems across multiple systems and identify vulnerable areas of systems that may cause system usage errors in the future.

The unique methodological contribution of the critical incident technique is that not all incidents related to a topic of interest are collected. Rather, only those incidents that are deemed to have special significance are gathered and analyzed, resulting in more efficient and effective research. The rationale for collecting only those incidents deemed to have special significance is twofold. First, atypical events are more easily recalled; multiple studies demonstrate that there is a bias to report dramatic or special types of events over mundane, frequently occurring events. While often considered a flaw in traditional methods of retrospective report, this feature of memory is exploited in the critical incident method. Therefore, many of the criticisms of traditional retrospective reports (e.g., that participants will not correctly remember or may only report highly salient events) are allayed. Second, these atypical events are by nature infrequent and occur unpredictably. Thus, despite the importance of these events, they are often difficult to observe as they occurring. However, by applying the critical incident technique these barriers can be overcome.

Steps in a Critical Incident Study

There are five high-level steps in a critical incident study: identify aims, identify type of events to collect, collect data, analyze data, and disseminate results. Because many of these steps are analogous to steps in other methods, only those points where differences exist between this and other, more familiar, methods will be discussed.

The first step, identify aims, includes determining what is necessary if the results of an action are judged to be successful or effective. In some cases (e.g., a job-related task) a supervisor determines how to judge success and therefore the aim. However, in the case of this study, users determined the aim of their actions, thus had to supply the criteria for success or failure. In this study, the critical aims were gleaned from a review of the literature as well as preliminary archival analysis of the focus group discussion. A primary aim that was repeatedly mentioned in both the literature as well as the focus group data was misclosure prevention; that is, retaining privacy involves disclosing information to some, while keeping it from others.

The second step in a critical incident study is to identify the types of events to collect. According to Flanagan (1954, p. 338), critical incidents are, “extreme behavior, either outstandingly effective or ineffective with respect to attaining the general aims of the activity.” Because the focus was on misclosures rather than disclosures, for this study I gathered outstandingly ineffective behaviors, or those which eventually led to a misclosure instance. As a further specification, because I am interested in understanding privacy and technology, only misclosure incidents when a technology is involved were collected.

The third step in a critical incident study is to collect the data. Data for critical incident studies may be collected in many ways including questionnaires (anonymous, mail, or email), interview (individual, phone, online, or group), by directly observing critical incidents, or by examining written records. In this study, I collected data through the use of a structured interview. A structured interview is a survey technique used to reliably gather data on a specific topic in a manner that preserves question order across participants. It is similar to a questionnaire but is administered orally instead of in written form. One of the reasons to choose a structured interview over a questionnaire is because of increased data quality. A skilled interviewer is expected to elicit accurate behavioral descriptions from participants by encouraging participants to provide specific, veridical descriptions. In addition, an interviewer may be able to answer questions participants may have during the course of the study.

A reason to choose a structured interview over an unstructured interview is to ensure that all participants receive the same questions in the same order. This standardization serves two purposes. First, it ensures that data can be compared across groups (e.g., younger vs. older adults) because it minimizes order effects. For example, if in using an unstructured interview all older adults happened to discus the person or people they misclosed to first, yet younger adults spoke about the technology first, it would be difficult to compare the aggregated responses at the group level because of context effects. Second, data obtained from a structured interview are easier to analyze because the categories of responses are often known in advance (i.e., flexible closed ended) and because the answer to each specific question is identifiable. In an unstructured interview each participant will explain examples in a unique way. For example a participant may begin talking about misclosure example A. While talking about misclosure example A, they may be reminded of misclosure example B and begin talking about that example before fully explaining misclosure example A. Despite coding with the surrounding contextual transcript, it is often difficult to follow a participant's sequence of description through coding.

The fourth and fifth steps are analyze the data and disseminate findings. Because these steps are not unique to the critical incident method they will not be described in detail here. Flanagan maintains that the purpose of data analysis is to make the findings easier to report while pointing out that dissemination of findings includes interpreting the analyzed data and providing this information in the form of a report.

Overview of Study

Participants were asked to recall specific, relevant events and relate these to the interviewer. In addition to the event, participants were also asked to report the conditions surrounding each misclosure, including cognitive/psychological factors such as attention (e.g., attentional demands, whether attention was divided), noise conditions, working memory demands, and social demands. Each incidence of misclosure was coded along the dimensions of information type, system type, cognitive factors, and type of misclosure. The precise point of error during the disclosure process as well as relevant psychological characteristics were identified, thus providing a psychological basis for design suggestions for improving privacy in technology which is grounded in empirical findings.

Participants

Because participants must have had an opportunity to experience a misclosure (i.e., used technology where a misclosure could have occurred), only those participants who had experience with technology were recruited. Since younger adults were Georgia Tech undergraduates, it was assumed they had experience with technology and this was confirmed via a technology experience questionnaire. Older adults were screened for medium to high communication technology experience, defined as, at minimum, reported use of cell phone and email, prior to recruitment.

Participants were 30 older adults (14 female) between the ages of 66 and 79 (*M* = 72.43, *SD* = 3.70) and 27 younger adults (14 female) between the ages of 18 and 23 (*M* = 20.22, *SD* = 1.45). Older adult participants were recruited from a database of people that had previously expressed interest in participating in studies in the Human Factors and Aging Lab. Younger adult participants were recruited from the Psychology Subject Pool via experimetrix at Georgia Tech.

As shown in Table 18 participants were well educated and diverse in terms of ethnicity. Participants were fluent English speakers. Younger adults received class credit for participation whereas older adult participants were remunerated for their time at a rate of $25 for the 1 – 2 hour study. Approval for the study was given by the Georgia Institute of Technology Institutional Review Board.

Table 18. Misclosure Sample Description

	Younger Adults (N = 27)	***Older Adults (N = 30)***
Age: *M (SD*)	20.22 (1.45)	72.43 (3.70)
Gender: *% (N*)		
Male	48% (13)	53% (16)
Female	52% (14)	47% (14)
Education: *% (N*)		
≤ High school	19% (5)	13% (4)
Vocational training, some college, Associate’s degree	70% (19)	7% (2)
Bachelor’s, Master’s Doctoral Degree	11% (3)	80% (24)
Ethnicity: *% (N*)		
Hispanic	4% (1)	3% (1)
Non-Hispanic White	67% (18)	80% (24)
Non-Hispanic Black	0% (0)	17% (5)
Other	29% (8)	0% (0)

Note: Percentages were rounded.

As is typical in the aging literature, younger adults performed more quickly and more accurately on the reverse digit span and digit-symbol substitution tasks, whereas older adults outperformed younger adults on the Shipley vocabulary task (see Table 19).

Table 19. Abilities Test Results

	Younger Adults	***Older Adults***
Reverse Digit Span: *M (SD*)	10.08* (2.38) [1]	7.93 (2.26)
Digit-Symbol Substitution: *M (SD*)	74.41* (10.43)	53.93 (12.05)
Shipley Vocabulary: *M (SD*)	30.56* (4.14)	35.90 (2.89)

* indicates significant age-related difference, p=.001

[1] N=25; 2 YA participants data were not usable (because they began cheating by writing backwards)

Materials

Materials for the study included multiple questionnaires, a critical incident questionnaire, critical incident coding worksheet and exit interview. Demographic, health, and technology experience questionnaires are provided in Appendix C, while the Critical Incident Interview (for the purposes of data collection presented with the Critical Incident Coding Worksheet), and Exit Interview are provided in Appendix B.

Demographic and Health Questionnaire

The demographic questionnaire (see Czaja et al., 2006a) gathered broad characteristics of the sample including age, gender, ethnicity, and work status; the health questionnaire gathered self-reported health status, satisfaction with health, and number of medical problems.

Technology Experience Questionnaire

The technology experience questionnaire (see Czaja et al., 2006b) gathered information about technology experience, usage, and attitudes.

Critical Incident Interview

The critical incident interview gathered information about the number and type of misclosure incidents, as well as the conditions surrounding each misclosure.

Critical Incident Coding Worksheet

The critical incident coding worksheet was designed to assist the interviewer in collecting data during the interview. It contained misclosure questions as well as potential answers (collected from pilot testing).

Exit Interview

The exit interview was designed to give the participant an opportunity to express opinions or provide data they were not previously asked about.

Equipment

As a secondary method of data collection, all critical incident interviews were recorded using an Olympus DS-30 voice recorder. Following the interview, interviews were transferred to PC and converted to wav files using WinFF (open source freeware for file conversion) for storage and verification purposes. Audio clips were extracted using Audacity, an open source freeware application for sound editing.

Procedure

After giving informed consent, participants were asked to complete the demographics and health and technology experience questionnaires. Next, participants were introduced to the goals of the study and given instructions about how to complete the interview. This description introduced the concept of misclosure as well as explained the different types of misclosure (i.e., recipient, information, and combination). Next, the interviewer asked the participant to take up to 5 minutes to reflect on any critical incidents that may have occurred and note those on a piece of paper for their own memory. Participants were instructed that the notes they made were for their own use and would not be collected by the interviewer. These memory aids were discarded at the conclusion of the study.

Next, the interviewer began the critical incident questionnaire by asking the participant to describe the first [recipient OR information OR combination] misclosure incident they noted on their scratch paper. Order of type of misclosure incident asked about was counterbalanced using a partial latin square design. Then the interviewer followed the interview script, asking all follow up questions about the misclosure incident. This procedure was repeated until all misclosure incidents were reported.

If the participant reported that they had never experienced a misclosure incident, the interviewer provided additional examples to encourage recollection of misclosure incidents. If the participant still did not report having experienced a misclosure incident, the participant was asked follow up open-ended questions that addressed their opinions about why they thought they had never experienced a misclosure. Finally, participants were thanked for their time and the session was concluded.

After all critical incidents were gathered participants were debriefed, remunerated via check or experimetrix credit and thanked for their participation in the study. A conceptual overview of the study procedure is given in Figure 12.

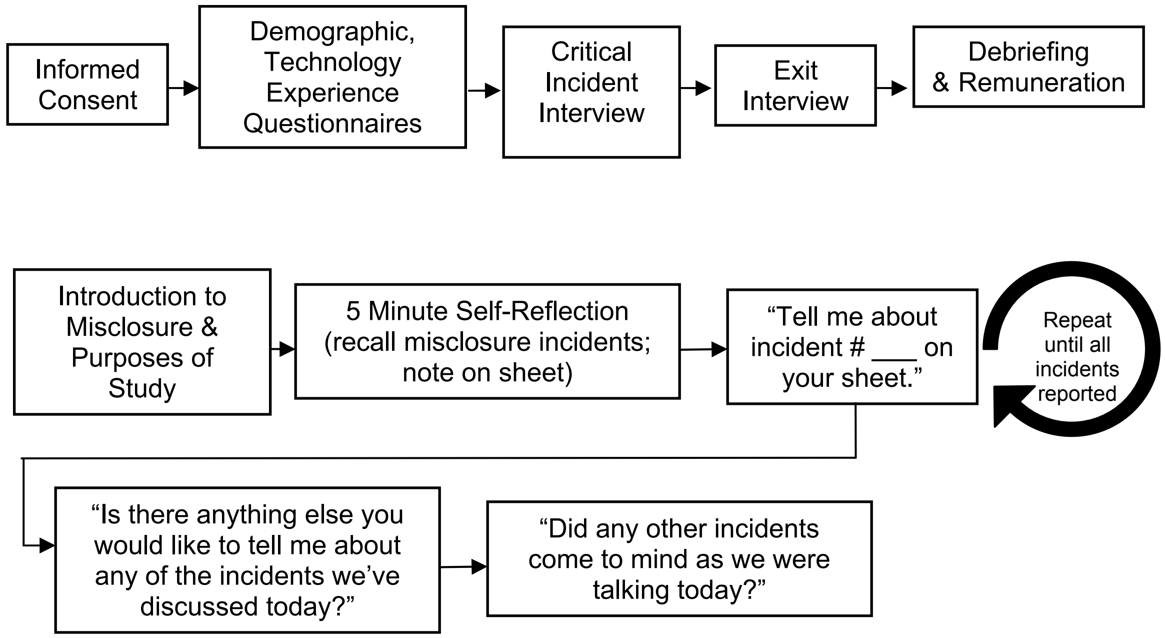

Informed Consent
Demographic, Technology Experience Questionnaires
Critical Incident Interview
Exit Interview
Debriefing & Remuneration
Introduction to Misclosure & Purposes of Study
5 Minute Self-Reflection (recall misclosure incidents; note on sheet)
"Tell me about incident # ___ on your sheet."
Repeat until all incidents reported
"Is there anything else you would like to tell me about any of the incidents we've discussed today?"
"Did any other incidents come to mind as we were talking today?"

Figure 12. Critical Incident Study Procedure

Data Analysis Strategy

Because the critical incident questionnaire was highly structured, and because the critical incident coding worksheet was used during the interview, a large amount of coding was completed in real time. That is, as the interview was being conducted the interviewer marked tallies into pre-defined categories on the worksheet, similar to the way data collection is completed in a questionnaire.

In addition to marking tallies into pre-defined categories, the interviewer also took notes about comments that were related to the aim of the study, but not captured on the worksheet, thus providing flexibility not offered by the use of a traditional questionnaire. These notes provided an additional reference if the codes on the code worksheet were ambiguous. Data from participants who were unable to produce any critical incidents were replaced up to the proposed N.

T-tests and Pearson Chi-square tests were used to determine the significance of relationships between variables of interest. In Chi-square tests residuals (the difference between the observed frequency and the expected frequency) were converted to z-scores and compared to a critical value corresponding to an alpha of 0.05 (i.e., +/- 1.96) to determine which cell or cells produced statistically significant results.

CHAPTER 6

RESULTS OF STUDY 2: CRITICAL MISCLOSURE INCIDENTS

Most participants (100% of younger; N = 27 and 83%; N = 30 of older) reported at least one misclosure incident (see Figure 13**Error! Reference source not found.**). Whereas all younger adult participants reported at least 1 misclosure incident, 5 older adult participants reported 0 misclosure incidents.

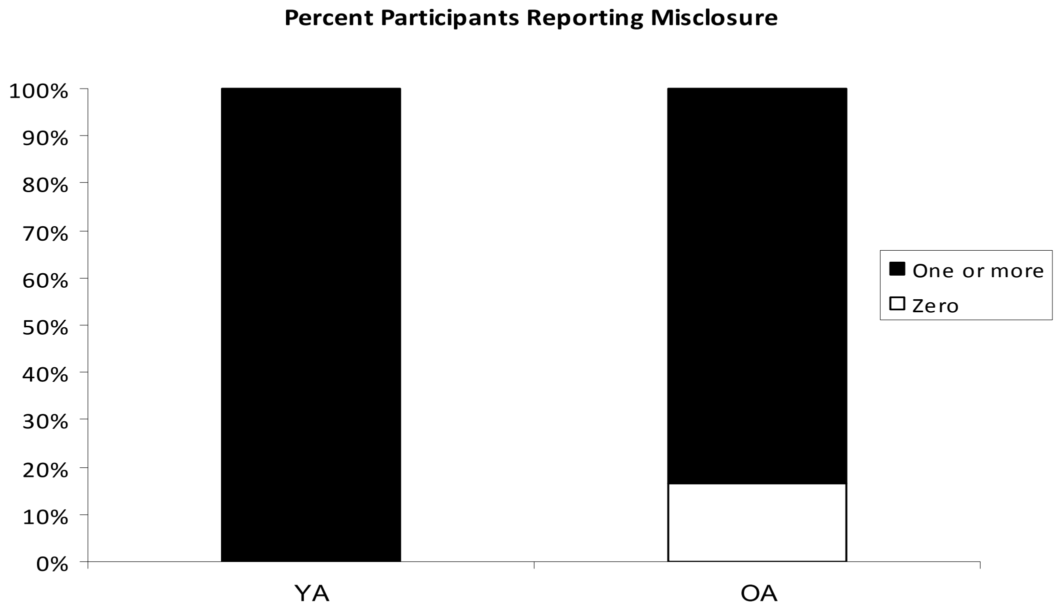


Figure 13. Percentage of Participants Reporting Misclosure

Number of Misclosures Reported

An independent samples t test was performed comparing the mean number of misclosure incidents reported by all (both those reporting 0 misclosures and those reporting more than 0) older adults (M = 2.50, SD = 1.89) with the mean number of misclosure incidents reported by younger adults (M = 3.70, SD = 1.41). Using this analysis strategy there was a significant difference in the number of misclosure incidents reported by older adults and the number of incidents reported by younger adults t(55) = 2.7, p = 0.01.

A second independent samples t-test was performed comparing the mean number of misclosure incidents reported by older adults who *reported at least one misclosure* (M = 3.00, SD = 1.66) with the mean number of misclosure incidents reported by younger adults (all of whom reported at least one misclosure, M = 3.70, SD = 1.41). Using this analysis strategy there was not a significant difference in the number of misclosure incidents reported by older adults and the number of incidents reported by younger adults t(50) = 1.65, p = .11. Older and younger adults reported just over 3 misclosure incidents per person.

For the remainder of the results sections participants reporting no misclosure incidents (N=5; all older adults) will be excluded from analysis (resulting in final N=52).

Type of Incidents Reported

In addition to specific misclosure incidents, participants also reported: non-specific incidents (i.e., incidents where participants could remember a misclosure happening multiple times but were unable to recall details about a specific incident), times when they were the recipient of a misclosure, and near misses. These incidents were collected but were not analyzed for the purposes of this study. All data presented from this point forward come from reports of specific misclosure incidents.

Misclosure Type

Participants reported information, recipient and combination misclosures. There was a significant relationship between age group and the type of misclosure most commonly reported $\chi^2(2, N = 159) = 15.76, p = .001$. Younger adults reported more information misclosures whereas older adults reported more recipient misclosures (α's < .05; see Table 20). The number of combination misclosures did not differ across age group.

Table 20. Type of Misclosure

	Younger Adults (n=91)	***Older Adults (n=68)***
Information*	61%	32%
Recipient*	33%	65%
Combination	6%	3%

*p< .05

Note: Percentages were rounded.

Length of Time since Incident

For both younger and older adults the majority (~60%) of misclosure incidents reported occurred within the six months prior to the interview (see Table 21). Younger adults reported very few incidents occurring more than five years prior to the interview while 15% of the incidents older adults reported were from more than five years prior to the interview.

Table 21. Length of Time Since Misclosure Incident

	Younger Adults	***Older Adults***
< 1 month	19%	27%
1 – 6 months	47%	31%
7 – 12 months	10%	15%
1-5 years	19%	13%
> 5 years	3%	15%
Do not recall	1%	0%

Note: Percentages were rounded.

Type of System

Misclosures occurred across a number of different technologies (see Table 22). For both younger and older adults, misclosure occurrences most often occurred while the participant was using an email system. Younger adults also reported misclosures while using instant messaging, text messaging and social networking. Older adults on the other hand reported misclosures while shopping online and while using a landline telephone.

Table 22. Type of System Used During Misclosure Incident

	Younger Adults	***Older Adults***
Email	39%	52%
cell phone	3%	15%
instant messaging	13%	0%
text messaging	13%	0%
online social network (e.g., facebook)	12%	2%
online shopping	3%	10%
Combination	1%	4%
Fax	1%	2%
landline phone	2%	6%
Blog	3%	2%
online project management	3%	0%
Other	6%	9%

Note: Percentages were rounded.

Experience with System

Participants were asked to estimate how long they had been using each system at the time each misclosure incident occurred. The majority of incidents were associated with systems that participants had been using for over six months (see Table 23).

Table 23. Length of Time Using System Prior to Incident

	Younger Adults	*Older Adults*
< 1 month	7%	-
1 – 6 months	12%	3%
7 – 12 months	14%	2%
1-5 years	56%	65%
> 5 years	9%	28%
Missing	2%	3%

Note: Percentages were rounded.

Familiarity

Participants were also asked to rate their level of familiarity with each system at the time of each misclosure incident. In line with the results from reports of length of time using the system, as well as independent reports (from the technology experience questionnaire) of technology experience, for the majority of misclosure incidents participants reported that they were familiar or very familiar with the system they were using when the misclosure occurred (see Figure 14).

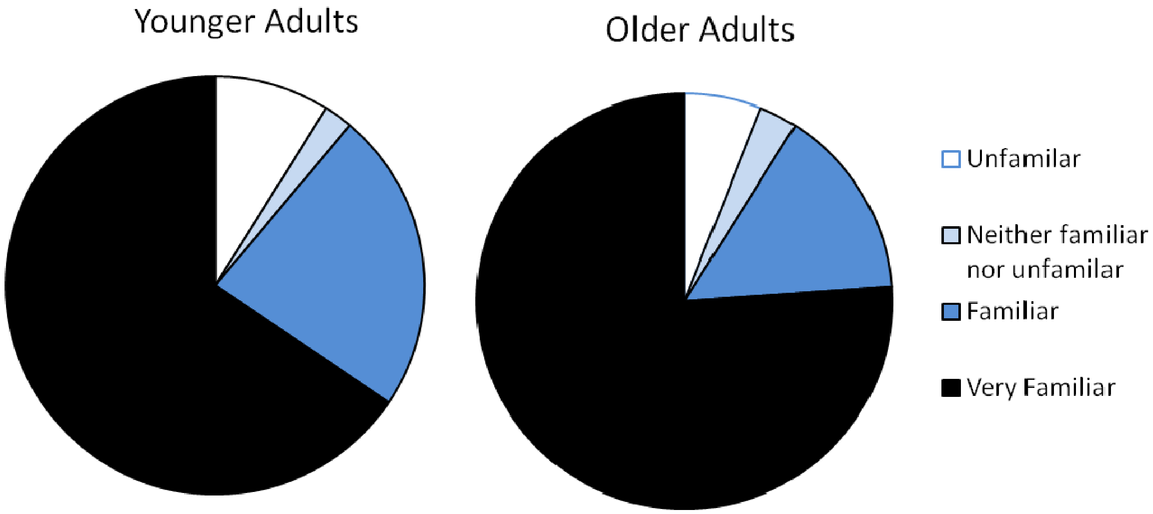


Figure 14. Familiarity with System

Attribution of Error

Overall, participants reported that most of the time misclosure errors were their fault rather than the fault of the technology. There was a significant relationship between age group and the attribution of error $\chi^2(3, N = 159) = 14.00$, $p = .001$. Misclosures by older adults who blamed themselves were overrepresented, whereas misclosures by younger adults who blamed both (the technology and themselves) were overrepresented (α's < .05; see Table 24). The number of misclosures blamed on the technology did not differ across age groups. Older adults blamed themselves more often than younger adults, whereas younger adults blamed both the technology and themselves more often than younger adults.

Table 24. Primary Attribution of Error

	Younger Adults	***Older Adults***
Technology	4%	9%
Self*	56%	77%
Both*	39%	12%

Note: Percentages were rounded.
* p<.05

System Factors

Regardless of the answer to the forced choice attribution of blame question, participants were asked whether there were any system factors that contributed to the misclosure. In line with the results of the question about error attribution, older adults reported that for the majority of misclosure instances (63%) there were no system factors that contributed to the misclosure. However, younger adults reported that there were no system factors that contributed to a misclosure instance in only 33% of the cases.

If participants stated that there were system factors that contributed to the error, they were asked to describe each contributing factor (note that people were allowed to report more than one factor contributing to each misclosure). System factors that contributed to misclosure occurrences include lack familiarity, general interface issues making a technology difficult to use, auto fill and predictive text features, visual similarity of system features with different functions, interface button proximity for action and/or recipient selection, reply all features, recipient and file name truncation, automatic focus or cursor changes, lack of clarity with respect to request or recipient, difficult sharing/privacy settings and no warning or feedback provided by the system (see Table 25).

Table 25. System Factors Contributing to Misclosure

	Younger Adults	***Older Adults***
Lack of familiarity	7%	0%
Hard to use/general interface	15%	4%
Auto-fill/predictive text features	7%	11%
Visual similarity of system features with different functions	11%	7%
Interface/button proximity for action	9%	15%
Interface/button proximity for recipient selection	15%	11%
Reply all feature not obvious	3%	4%
name of recipient truncated by system	1%	0%
name of file/information truncated by system	7%	4%
Focus/cursor changes automatically	7%	7%
Request or recipient unclear	1%	26%
Sharing/privacy settings difficult	8%	4%
No warning and/or feedback	7%	4%
Self issues attributed to technology	3%	4%

Note: Percentages were rounded; percentage of misclosures where system factors were reported to have contributed to the misclosure.

Person Factors

Participants were also asked whether there were any things that they did (i.e., self factors) that contributed to the misclosure. Both younger and older adults reported that in a large majority of misclosures (95% and 94% respectively) they had done something that contributed to the misclosure event. When participants stated that there were self factors that contributed to the error, they were asked to describe each contributing factor. Self factors that contributed to misclosure occurrences include not paying attention, carelessness, not double checking, being in a hurry, and pressing the wrong button (See Table 26).

Table 26. Self Factors Contributing to Misclosure

	Younger Adults	***Older Adults***
Not paying attention	20%	19%
Carelessness	18%	11%
Did not double check	16%	8%
In a hurry	7%	12%
Hit wrong button	7%	11%
Multitasking/concurrent activities	2%	3%
Lack of familiarity	2%	0%
Distracted by surroundings	2%	2%
Distracted by state of mind	4%	2%
File names too similar	8%	3%
Old habit or rule applied	2%	7%
Should have known better	2%	6%
Misspelled, misread, etc.	4%	4%
Lack of awareness	4%	3%
Poor health/ability	1%	4%
Failed to logout	2%	0%
Don't remember	1%	1%
Tried to take a short cut	1%	1%

Note: Percentages were rounded.

Negative Consequences

Participants were asked whether there were any negative consequences associated with each misclosure. For the most part, participants reported that there were not negative consequences (see Table 27). However in 29% of the cases for younger adults and 43% of the cases for older adults, participants reported that there were negative consequences. Negative consequences included embarrassment, having to apologize, annoyance, feeling “stupid”, having to cancel a credit card, and having to expend effort to correct the error.

Table 27. Percentage of Misclosures With Negative Consequences

	Younger Adults	***Older Adults***
Yes	29%	43%
No	70%	57%
missing/other	1%	2%

Note: Percentages were rounded.

Repeat Occurrences

Participants were asked whether, following an initial misclosure, they experienced another similar misclosure. Participants reported that in about 40% of misclosures they had experienced another similar misclosure after the initial misclosure incident (see Table 28).

Table 28. Percentage of Misclosures With Repeat Occurrences

	Younger Adults	***Older Adults***
Yes	43%	41%
No	57%	54%
missing/other	-	4%

Note: Percentages were rounded.

Steps Taken to Prevent Future Occurrences

Participants were asked whether, after a misclosure occurrence, they had taken any steps to ensure that a similar event did not take place in the future. In about three quarters of the cases participants reported that they had taken steps to prevent future misclosure occurrences (see Table 29).

Table 29. Percentage of Misclosures When Additional Steps Were Taken to Prevent Future Occurrences

	Younger Adults	***Older Adults***
Yes	73%	77%
No	28%	24%

Note: Percentages were rounded.

When participants reported that they had taken steps to prevent future misclosure occurrences, they were asked to describe these steps in more detail. Participants reported that they tried to be more careful, double check, pay more attention, use a system less, avoid using a system when distracted, corrected information, tried to be more organized, set more restrictive sharing settings and practiced using a system to try to prevent future misclosure occurrences (see Table 30). In the following chapter I discuss the results presented here.

Table 30. Steps Taken to Prevent Future Misclosures

	Younger Adults	***Older Adults***
Tried to be more careful	29%	44%
Always double check	33%	16%
Pay more attention	15%	14%
Used system/committed action less	7%	8%
Less use when distracted	1%	11%
Corrected or erased particular case	8%	2%
Better organizing or planning actions	1%	5%
More restrictive privacy settings	4%	0%
Got more familiar with system/practiced	1%	2%

CHAPTER 7

DISCUSSION OF CRITICAL MISCLOSURE INCIDENT RESULTS

This study was designed to collect information about critical misclosure incidents. In this study I recorded and counted the number of misclosure occurrences each participant reported, categorized each misclosure incident in terms of type of misclosure (i.e., recipient misclosure, information misclosure, or combination misclosure), and gathered information on the conditions surrounding each misclosure occurrence.

Misclosures were reported by most participants, had occurred recently, and occurred even with systems participants were familiar with and often had been using for a year or more. The types of incidents gathered covered multiple technologies including email, social networking, cell phones (including texting), and many others. There were no age differences in the number of misclosures reported by younger and older adults, however, there were age differences in how older and younger attributed the blame for misclosure errors.

The remainder of the discussion is organized as follows: First I discuss the general results of the study. Then I discuss how these results suggest a) design considerations b) a focus on social wysiwyg and c) implications for theory.

On average, participants (both younger and older) reported 3 misclosure occurrences each. This suggests that misclosure incidents are memorable events, perhaps because of their significance. Usually these misclosures had occurred within the last year. One way to restate this is that people may experience about 3 misclosures annually. In addition, it appears that most people have experienced a misclosure at least once; only 5 participants in the entire study did not report any misclosures. In combination, these numbers suggest that misclosures are a potential threat to the privacy of many users.

In terms of type of misclosure, younger adults reported more information misclosures, whereas older adults reported more recipient misclosures. Judging by the types of systems used where older adults experienced the most misclosures, it may be that those technologies (e.g., email and cell phone) are more prone to recipient misclosures, whereas technologies that were reported by younger adults almost exclusively (e.g., instant messaging, text messaging, and social networking) are more prone to information misclosures. As expected, combination misclosures (which combine a recipient and information misclosure) were reported with the least frequency across age groups.

Misclosures occurred while participants were using a variety of systems, including: email, cell phone, instant messaging, text messaging, online social networking (e.g., facebook), online shopping, fax, landline phone, blog, and online project management software. That misclosures occurred across such a wide variety of systems indicates that misclosures are a widespread issue that should be addressed for multiple technologies.

The majority of misclosure incidents reported resulted from interactions with technologies the participants were experienced with using at the time of the incident (e.g., cell phone, email) rather than when a participant was using a new system that he or she was not familiar with. More than half the time, participants had at least one year of experience using the system when the misclosure occurred. This suggests that the likelihood of misclosure may not be mitigated by time using a system. It is also worth noting that because certain technologies are used more often they provide more opportunities for misclosure.

Besides having experience with a system, participants also reported that they were familiar with the system they were using when they experienced a misclosure. Well over half of the time, participants reported being very familiar with a system when a misclosure occurred. This indicates that misclosures occur even on systems with which participants are highly familiar and buttresses the previous suggestion that the likelihood of a misclosure may not be mitigated by familiarity with a system.

That misclosures occur on systems that users have been using for a relatively long time and rate themselves as very familiar may seem surprising. However, Reason's (1984) theory of errors suggests that when encountering a familiar system, people may be prone to motor-sensory errors, especially given environmental demands (e.g., a distracting crowd or busy schedule). Thus, it is possible that some of the errors that led to misclosure experiences may have been motor-sensory. If this is the case, one way to decrease the likelihood of misclosure occurrences in the future is to focus on preventing motor-sensory errors.

Both younger and older adults blamed themselves more often than the technology for the misclosures they experienced. However, older adults blamed themselves more often than younger adults, whereas younger adults often blamed errors on a combination of themselves and the technology. In general, the finding that both younger and older adults blamed themselves is surprising given that we would expect self-protective attributions (blame the machine) rather than self-blame. It may be that because the errors were social in nature participants found it harder to blame a machine for the errors.

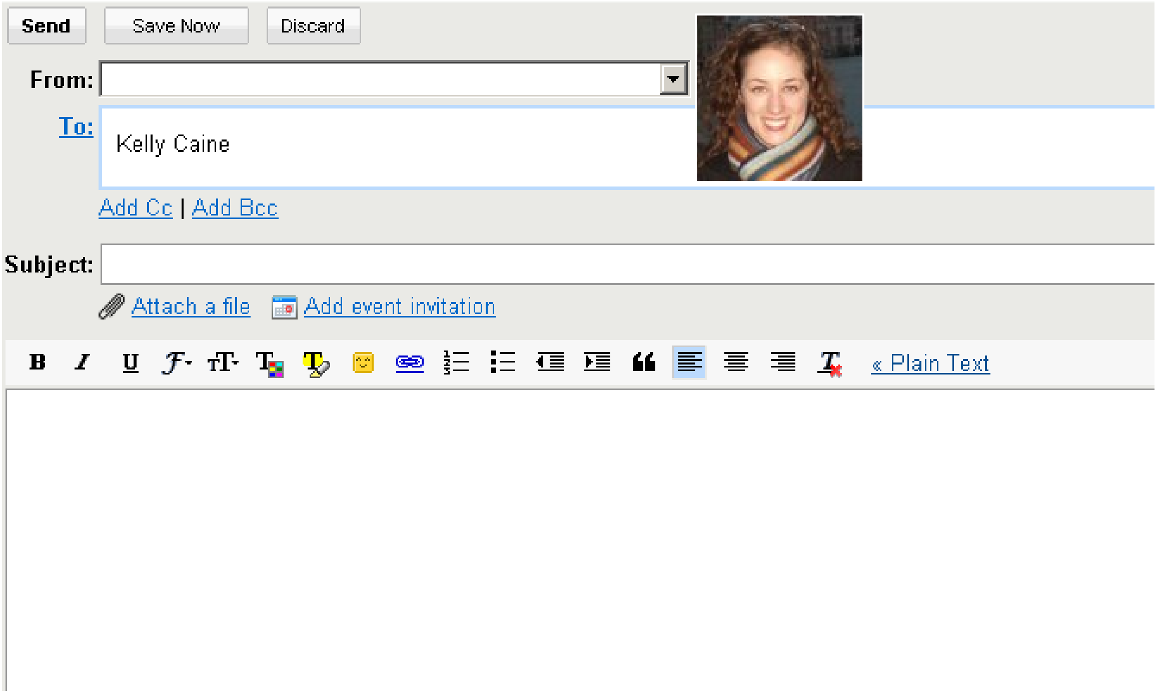
When participants did express that the technology had at least some part in contributing to the misclosure, system factors that were mentioned included general interface issues making a technology difficult to use, auto fill and predictive text features, visual similarity of system features with different functions, interface button proximity for action and/or recipient selection, reply all features, recipient and file name truncation, automatic focus or cursor changes, lack of clarity with respect to request or recipient, difficult sharing/privacy settings and no warning or feedback provided by the system. Participants also reported "lack of familiarity" as a system factor that contributed to their misclosure experience. This is notable because participants are blaming the system for their own lack of familiarity, indicating that participants may feel it is the system's responsibility to be easy to use and thus seem familiar.

Participants also reported that they contributed to misclosure occurrences. For example, participants reported that they contributed to misclosure occurrences by not paying attention, being careless, not double checking, being in a hurry, and pressing the wrong button. From a human factors perspective, many of these "contributions to an error" may be due to poor design, rather than to "not paying attention" or "being careless". Systems should be designed so that users do not have to take additional steps to prevent misclosure, rather this should be the default state.

When misclosures did occur, they sometimes resulted in negative consequences. For example, participants reported that they were embarrassed, had to apologize and "felt stupid" after misclosure occurrences. This suggests that misclosures may negatively affect a person's well being. Perhaps because of these negative consequences, a majority of participants (about ¾) reported that they had taken steps including trying to be more careful, double checking, paying more attention, using a system less, and changed their usage habits to try to prevent future misclosure occurrences. Despite these attempts, in about 40% of the misclosures reported, participants reported that a similar misclosure had occurred after the first incident. This indicates that despite additional effort, participants may not have been able to prevent future misclosures and suggests that design alternatives may be in need.

Design Implications

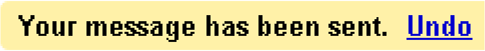
Some implications for design may be drawn directly from the system factors that participants reported contributed to the misclosures. For example, participants mentioned that the reply/all feature on some systems is not obvious. There are at least two ways to deal with this issue from a design standpoint. One way to address this is to make the fact that a user is replying to multiple people visually salient. A design that already accomplishes this, but is not in widespread use is called facemail (Lieberman & Miller, 2007; see Figure 15). In this email client, pictures of selected recipients are automatically displayed in a peripheral display while a user is composing an email message. Findings from studies of facemail indicated that the peripheral display of faces improves users ability to detect a potential misclosure (in this case, misdirected email).



To: Kelly Caine

Figure 15. Example similar to Facemail

A second way to address the issue of sending a message to unintended recipients is to implement an undo function. In the context of email, this could be in the form of a "recall" function. Despite technical challenges inherent in providing email recall, some email providers are already offering such an option, albeit a limited one. Google offers gmail users 5 seconds to "undo" sending an email once the user has clicked "send" (see Figure 16). If a user realizes that they have accidentally sent an email to the wrong person or to too many people within this time period, they are able to click undo and recall the email before it arrives in another person's email box. One consideration related to this is that in some email clients a recall option is available, however the recipient continues to have access to the email but is suggested not to read the email. It is possible that if shown a notice that an email sender wants to recall the contents of an unintentionally sent email, the receivers may be *more* rather than *less* likely to actually read the email.



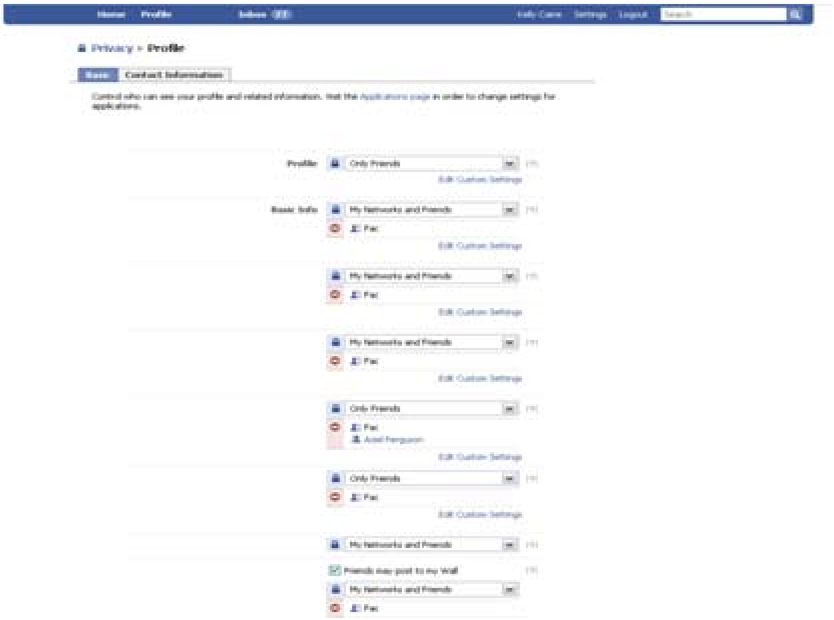
Your message has been sent. Undo

Figure 16. Gmail undo feature

Another system factor that participants reported contributed to misclosures was auto-fill/predictive text. Participants' reported that systems would often guess a name they were trying to type too soon and automatically fill in an incorrect name in a recipient field. While predictive text may be considered useful and a time-saver in many contexts, in situations where privacy is critically important, auto-fill features should be considered carefully. For example, in the design of an electronic medical record, a function designed to provide deliberate control as to the recipient may be more appropriate than an auto-fill system that provides quick access to multiple health care providers or other potential recipients. In this case, the risk of automation encouraging a misclosure may be greater than the benefit of a specific type of convenience (i.e., auto-fill).

Participants also reported that misclosures occurred as a result of file and/or recipient information being truncated. The design implication here is obvious: increase the size of space available for file/recipient information viewing. A related problem participants mentioned was that often files shared the same "space". That is, image files may share a folder with document files due to lack of organization or some other factor. In this case it became easy for participants to "grab" the wrong file (e.g., a photo instead of a document). This suggests that alternative file organization strategies may prevent some types of misclosure. Another straightforward issue is feedback. Participants reported that lack of a warning or feedback contributed to their misclosures. Therefore providing additional feedback may decrease misclosure occurrence.

Finally, participants reported that often misclosures occurred because privacy/sharing settings were difficult to understand. As an example of privacy settings that are confusing, examine facebook's privacy setting page (see Figure 17). In this example it is difficult to tell what information is shared with whom. It is not clear what information is contained in "profile" and what information is contained in "basic info". Also, it is not possible to see the people in each of the groups listed. Instead, a user must rely on memory to recall the members of each group.



Control who can see your profile and related information. Visit the Applications page in order to change settings for applications.

Profile: Only Friends

Basic Info: My Networks and Friends; Fac

My Networks and Friends; Fac

My Networks and Friends; Fac

Only Friends; Fac; Adell Ferguson

Only Friends; Fac

My Networks and Friends

☑ Friends may post to my Wall

My Networks and Friends; Fac

Figure 17. Sample facebook privacy settings

Social Wysiwyg

In combination, many of these suggestions for design constitute a need for social wysiwyg. Wysiwyg is an acronym for What You See Is What You Get and refers to a system where the output or final product appears visually similar to content that is being edited. I propose social wysiwyg as an analogy to wysiwyg in that social wysiwyg may make sharing/privacy easier in the way wysiwyg makes document editing easier. In social wysiwyg the idea is that users should be given a visual representation of where (to whom) their information (what information) is going. Given a clear presentation about where and to whom information is going, users may be less likely to misclose.

As an example of a social wysiwyg interface, I have created an interface called “selectiveShare”. In selectiveShare content and recipient are both displayed simultaneously (see Figure 18). If I wanted to share my dissertation with colleagues at Indiana University, I could either a) first select the content, then choose the recipients or b) first choose the recipients then choose the content. Either way, both recipient and content would be displayed at the same time and I would see a preview of what information was going to whom before information was transferred.

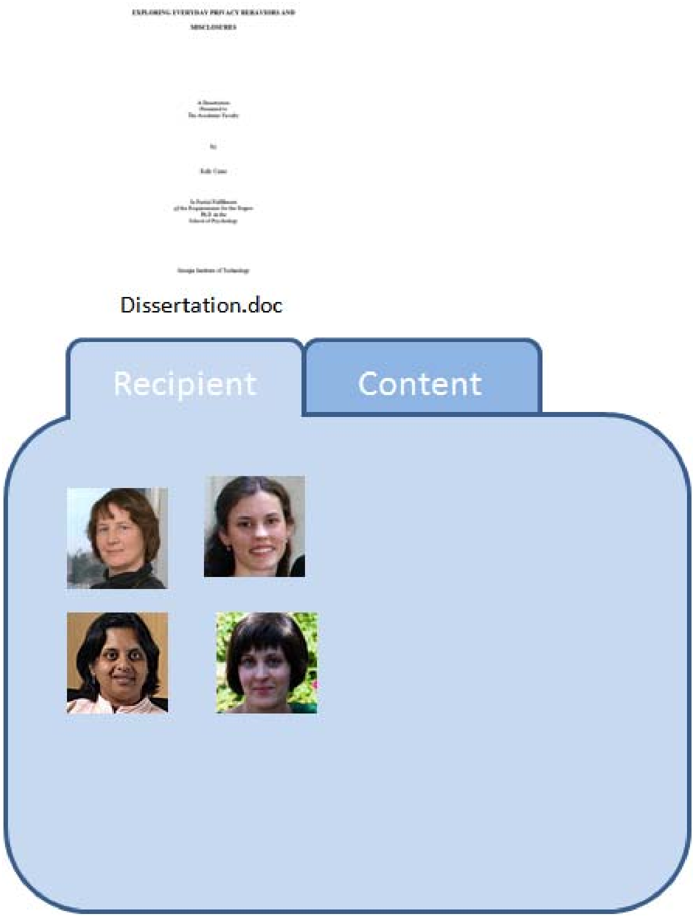

EXPLORING EVERYDAY PRIVACY BEHAVIORS AND MISCLOSURES
Georgia Institute of Technology
Dissertation.doc
Recipient
Content

Figure 18. SelectiveShare Interface Sketch

As with other examples, it is not suggested that selectiveShare is necessarily a better option than existing privacy/sharing settings. SelectiveShare is just a sketch and has not been tested with users. Alternative designs would need to be developed and usability tested before selectiveShare was implemented anywhere. Second, selectiveShare may not be appropriate for settings where privacy issues are not critical, as it is possible that it would increase the time it takes users to complete common sharing tasks. For example, Kieras & Bovair (1986) demonstrated that an overly simplified model may lead users to become frustrated with an interface or device if they are asked to interact with an incomplete or superficial device model rather than the actual model. However, in settings where privacy is very important, for example when older adults need to be able to control the flow of monitoring information with a caregiver, selectiveShare or something like it has the potential to be useful as a more usable sharing/privacy interface, especially with respect to preventing misclosure.

Theoretical Implications

Although it is difficult to draw predictions from Altman's model of privacy regulation (Caine, 2008), there is one area where it is possible to pit Altman's model against the alternative model proposed in this dissertation. Altman's model of privacy regulation suggests that people manage privacy through a personal boundary regulation process where they may be more open (more receptive to disclosing) or more closed (less likely to disclose). Given this model of privacy we would have expected to observe more combination misclosures where unintended information went to an unintended person because the model suggests that information is either kept inside the boundary or let outside the boundary rather than aimed at a specific entity. In the alternative model of privacy proposed in this dissertation, on the other hand, privacy is maintained when the intended recipient receives intended information. Therefore, based on this model, we would expect more information and recipient misclosures than combination misclosures. Indeed, participants did report more information and recipient misclosures than combination misclosures.

CHAPTER 8

CONCLUSION

The goal of this dissertation was to gain a better understanding of the psychological aspects of privacy in HCI. To accomplish this goal I used two complementary methods. First, I conducted a broad investigation of younger and older adults reported privacy behaviors. The results of this study include the identification and categorization of privacy behaviors across multiple technologies. Three broad categories of behavior emerged from the data: avoidance, modification, and alleviation. These categories of behaviors and the sub-categories of behaviors call in to question existing theories of privacy and suggest designs that may improve user privacy.

In the second study I proposed misclosure as a framework for understanding some of the human factors issue associated with privacy in HCI. As part of this study, I examined misclosure occurrences to gain an understanding of the system and psychological conditions under which misclosures are likely to occur. This examination resulted in a number of recommendations about how to support privacy by preventing misclosure.

In the following section I provide a discussion of some of the limitations of the studies presented in this dissertation. Next, I discuss some of the future work that is suggested by the results of the dissertation. Following this discussion, I conclude by providing a summary of the dissertation findings and implications.

Limitations

This study has a number of limitations. First, the sample may be better educated and more experienced with technology than the average population. Second, the exploratory nature of the studies calls for caution in drawing conclusions. In particular, it is critical to remember that all data reported here was self-report in nature. Each of these concerns is discussed in more detail below.

The sample in this study may not be representative of younger or older adults living in the US. With respect to younger adults, participants in our study are better educated and have more technology experience than average younger adults. With respect to older adults, as with other samples reported in the aging literature, the sample in this study was healthier and better educated than the average older adult. Thus, the results of these studies may not generalize to the population as a whole.

However, because of the direction of the differences, we may be able to generalize with caution. The older adult participants in this sample had *more* experience with technology and were *better* educated than an average older adult, and the younger adult participants had more technology experience than the average younger adult. Thus, participants in our sample should arguably be less likely to experience misclosure incidents, if we expect that either intelligence or technology experience decrease the likelihood of misclosure. On the other hand, if misclosures are simply a function of how often a person uses technology, then the sample in this study may have reported more misclosures than we would likely see in the population as a whole. Either way it is unlikely that the reasons for misclosure occurrences are unrepresentative.

Second, the studies presented in this dissertation were exploratory in nature. Thus, none of the design suggestions (e.g., vague design) presented in this dissertation have been tested with users. Although there is perhaps good reason to hypothesize that many of the design suggestions will improve the overall privacy usability of some systems, further testing is needed to evaluate these hypotheses.

Additionally, although participants in the focus groups were introduced to a wide variety of systems, not all potential privacy invasive situations were discussed. In the scenarios, the choice was made to focus on areas that had been highlighted from previous research on privacy in HCI. Therefore, technologies that have not received much attention in the past, were not represented here.

Finally, this study is subject to the many drawbacks of self-report data. One of the drawbacks is reliance on memory. It may be the case that participants recalled more avoidance behaviors than modification or alleviatory behaviors and therefore reported them more often. Although I analyzed the results of the focus groups quantitatively, it is important to remember the nature of these data. The data from the focus group came from open-ended discussions. Behaviors that were coded were discussed freely by participants. A more appropriate way to determine quantitative differences in the number of actual privacy behaviors people engage in would be to ask participants direct questions querying the frequency of such behaviors in the past, or observe participants' actual behavior. In the future, studies using alternative methods that are less susceptible to issues of self-report (e.g., direct observation, diary study, experimentation) should be conducted to test the conclusions presented here.

One clear example of a limitation of self-report in this study is in the lack of reports of lying behavior. Although I did not return to the data to do an explicit search for lying behaviors, it was not a category of behaviors that emerged during coding. Participants may have considered lying behaviors socially inappropriate and therefore not reported them during the focus group sessions. Deceptive behaviors have been observed in other related research (e.g., Hancock, Birnholtz, Bazarova, Guillory, Perlin & Amos, 2009; Hancock, Toma, & Ellison, 2007). A future study could examine this in more detail.

Another interesting question, if not limitation, is related to which of these types of behaviors is the most successful at preserving privacy. Based on the results from these studies it is not possible to tease apart which behaviors are most beneficial to users in terms of privacy management. If we knew this we would be able to focus our design efforts on technologies that were not only most often mentioned by people but were also most effective at achieving this goal.

Future Work

Clearly the two studies presented here represent the beginning of much future work, rather than a definitive study concluding that an area is now well understood. One area for future research is in testing the designs suggested from the focus group work. For example, based on the evidence suggesting that participants rarely reported avoidance behaviors with respect to photo sharing, I suggested that one design alternative would be to consider designs that supported avoidance behaviors. Specifically, I suggested that an avoidance-enhancing camera could be designed that requests approval from the person in the photo before a photo is shared with others and further suggested that this alternative model of ownership may enhance a person's sense of privacy. To test whether this design enhanced a person's sense of privacy, a study could be designed such that participants are shown a demonstration of a camera that utilizes avoidance-enhancing technology as well as a standard digital camera and then asked to rate which technology is more privacy-preserving.

Another example for future research is to further investigate vague design. It will be informative to consider how this design idea can be extended to other types of information. Additional questions include: Will people report that vague designs are more privacy protective? Will designers be able to adapt their input designs to vague designs? Can tools be designed to assist designers in adjusting input designs? Compared to other anonymization strategies, how effective is vague design?

In terms of misclosure, there are multiple avenues for future research. A first step will be to conduct a study of misclosures as they happen, rather than rely on self-report behavior. For example, a diary study could be used to gather data about misclosures as they occur. Another type of study that could be conducted is experimental. Now that we have some idea about the types of interface characteristics that are associated with misclosure, these could be manipulated experimentally and the resulting misclosures could be recorded. This type of study would provide solid evidence about which design features are associated with misclosure.

Final Summary

The purpose of this research was to investigate privacy issues associated with the use of technology. Two studies were designed to explore different aspects of the privacy issues of technology. The goal of the first study was to broadly examine privacy behaviors as they relate to current technologies. This investigation resulted in a categorization of privacy behaviors associated with technology and furthered our understanding about the psychological underpinnings of privacy concerns. The goal of the second study was to analyze a specific human factors issue thought to threaten privacy: disclosure error. This investigation resulted in a systematic exploration of unintentional disclosure errors made while using technology.

In this dissertation I identified privacy behaviors across a broad swath of technologies. By analyzing reported privacy behaviors and errors, this research constitutes an attempt to systematically examine privacy in the context of technological mediated environments. The empirical investigation revealed that there are commonalities among privacy behaviors and suggests that these commonalities may be exploited by designers to increase the privacy features in their designs. Because this study was focused on gaining a better understand of the way users view privacy, it is not specific to one set of technologies.

While some of the design suggestions may seem “obvious” or “simple”, I argue that they are only deceptively so. It is worth pointing out that designers struggle daily with developing privacy-sensitive technologies and how to prevent “data leakage”. Many complex security measures have been developed explicitly to deal with just one of the problems that a design solution was proposed for in this paper (i.e., k-anonymity vs. “vague input”).

Some design alternatives inspired by findings from these studies have been suggested. However, an additional contribution of this paper is in describing users’ privacy behaviors so that other designers may be able to better understand privacy from a user perspective. It is my hope designers will be able to take what I have described here and generate many design alternatives.

The results from these studies study advance our understanding of users' everyday privacy behaviors and the errors that occur when users are managing their privacy. Previous work on privacy in HCI had not focused on existing privacy behaviors as a source of design inspiration. By examining these behaviors I was able to suggest a number of things for designers of privacy protective systems to consider.

In addition, the results from this study advance our theoretical knowledge about privacy in HCI. The groupings of everyday privacy behaviors across technologies suggest an alternative to the claim that privacy is too contextual a topic to understand at the psychological level. The findings in this study indicate commonalities do exist and that these commonalities may be useful in helping to organize previous findings from the privacy in HCI literature. In addition, the findings in this study suggest that Altman's model of privacy does not reflect users' privacy behaviors. Instead, an alternative model of privacy regulation is proposed that accounts for participants' conceptualization of privacy and also predicts misclosures when errors in this conceptualization occur.

APPENDIX A
MATERIALS FOR STUDY 1

Privacy Focus Group Script

{INFORMED CONSENT}

I have given you two copies of the consent form, one copy is for us and the other is for your own records. Note that before you sign the consent forms, please make sure that you feel comfortable with participating today. If you decide for any reason that you are not able to participate today, let me know at any time. If you do not have any questions and you still wish to continue, you may sign the consent forms.

{INTRODUCTION}

Welcome, and thank you for your participation today. I would like to make a few introductions before we get started with the discussion. My name is Michelle and I will be leading the discussion today. Helping me today is Kelly – she will be writing things on the whiteboard and joining in the discussion as well.

Today we will discuss your ideas and concerns about privacy. We will be recording the session today. Because we care very much about what each of you has to say, please speak up. We don't want to miss anything that you have to say.

{DISCUSSION}

Now, we will move on to the focus group discussion. How many of you have participated in one of these before? We will be treating it just like a discussion. Before we begin, you should understand that there are no right or wrong answers, only different experiences and opinions. Feel free to express your opinions, perhaps in disagreement with another group member, as these types of discussions enable us to learn a lot about the different kinds of opinions that people have. In doing so, however, please remain respectful of the other members of the group.

A very important component to this type of study is confidentiality. There are two parts to this confidentiality that I wish to point out. First, as you read in the consent form, your name and your voice will not be tied to any of the data collected in this study. We will keep any information that ties you to the data on a password-protected computer in our lab. Secondly, we ask that anything we say in this room remain confidential amongst you guys. We hope that if you choose to talk about this study that you will not use each others names, and protect the identity of those in this room.

The session will last about two and a half hours. We would ask that you please turn off or silence your cell phones for this session. If there is something that Kelly or I can do to make you more comfortable, like get you a different chair or get you something to drink, please let us know. Also, before we begin, if you need to use the restroom, please do so now.

Ok, I'm going to turn on the tape recorder and begin recording now.

Discussion Questions

1) Please introduce yourself to the group by stating your first name and where you grew up/hometown.

2) We are here today to talk about privacy, so the first thing I would like to do is to have everyone take that blank piece of paper you see in front of you and write down your individual definition of privacy, or what it means to you. Feel free to brainstorm, but please work individually. When you are finished please fold the paper and put it in the envelope in front of you, and place the envelope under your chair or behind you. Thank you!

3) Ok, so what were some of the ways people defined privacy. Kelly will keep track of all the different things we have to say by writing them on the easel.
    a. Would anyone like to share their definition with the group?
    b. What are some key words you associate with privacy? What immediately pops into your head?

4) Now I'd like you all to think of the last time you thought about privacy before today.
    a. When was the last time that privacy came to your consciousness?
    b. What were you thinking or talking about it?
    c. Would anyone like to share their story with the group?

5) Group discussion (using examples that the group thought of)
    i. So what is privacy in these situations that we have just discussed?
    ii. What is private about [insert example]?

Scenarios

In the last section of this focus group, we are going to discuss privacy in a few different situations or contexts. We know that people think about privacy in many different ways: some people may have concerns in certain situations, and some people may not. So for each one of the scenarios we discuss, please express your concerns if you have some, and tell us a little bit about why that is a concern for you. If you feel that you do not have any concerns about the scenario, please tell us why not. If you feel that you have concerns other than privacy, please mention them briefly.

Since we are really interested in what concerns you may have and what types of things you may do in these situations, please try to put yourself in the role of the scenario as best as you can.

[For example, if the scenario is "You are walking in the supermarket," and you do not have any privacy concerns, it is quite alright to say "I am not concerned about privacy in the supermarket," instead of "Someone might be concerned with having the checkout person see what you are buying."]

Does anyone have any questions before we begin?

1) **You have a lifetime of photos you are thinking of storing on a website.**
   c. Standard Probes
      i. Do you have any privacy issues or concerns with this situation?
      ii. What about this situation makes it concerning?
      iii. Why

   d. Additions to this scenario
      i. What if you used a scrapbook?
      ii. What about an online photo album (like Flickr, Picasa, Snapfish, etc - Only say these if participants ask for examples.)?
      iii. What about if they were just photos from a recent trip?
      iv. What if there were sensitive photos included in your set?
      v. What if you could pick exactly who saw the photos?

2) **You are using your credit card to buy dinner in your favorite restaurant. When the waiter picks up the bill with your card in it, he takes the card in the other room for 5 minutes.**

   e. Standard Probes
      - i. Do you have any privacy issues or concerns with this situation?
      - ii. What about this situation makes it concerning?
      - iii. Why

   f. Additions to this scenario
      - i. What if the restaurant is one that you've never been to before?
      - ii. What about using your credit card to order takeout online?
         1. At home
         2. In a crowded place (library, work)
         3. On a network that is not yours
      - iii. Sometimes when you fly you have to swipe your credit card at the airport kiosk to pull up the flight information.
      - iv. Are there any other times when using your credit card that you think about privacy?
      - v. Participants may say "This is something that I've done before and I feel confident that nothing will happen" or something to that effect. If so – say "Do you remember the first time that you did ___? Did you have a different experience then?"

3) **Health Information: You have the symptoms of an illness that have lasted for over a week. You call your doctor's office and describe your symptoms to a nurse.**

   g. Standard Probes
      - i. Do you have any privacy issues or concerns with this situation?
      - ii. What about this situation makes it concerning?
      - iii. Why

   h. Additions to this scenario
      - i. What about if you are in a crowded room?
      - ii. What if your symptoms were more serious? Embarrassing? (AIDS, Mental Health, STDs)
      - iii. What about finding information about a health issue that you have online?
         1. "Is there anything that you wouldn't look for online?"

4) **Location: You are using a cell phone with a locating device (such as GPS). You find out that there is a way for <u>anyone in the world</u> to find out your exact location.**

   i. Standard Probes

      i. Do you have any privacy issues or concerns with this situation?
      ii. What about this situation makes it concerning?
      iii. Why

   j. Additions to this scenario

      i. What if your location was approximate?
      ii. Would it matter if only certain people could determine your location? [for example, only those in your family's cell phone plan]
      iii. Grocery Store
      iv. Out to dinner
      v. Home

5) **Traffic Light: Atlanta is trying to crack down on traffic violations by installing traffic cameras on every stop light. These cameras monitor traffic and then take a snapshot of anything out of the ordinary, such as someone running a red light. (Red-light camera)**

   k. Standard Probes

      i. Do you have any privacy issues or concerns with this situation?
      ii. What about this situation makes it concerning?
      iii. Why

   l. Additions to this scenario

      i. What if there were video cameras recording at all times?
      ii. What if this info was available to anyone on a certain TV channel?
      iii. What if Atlanta was going to crack down on traffic violations by placing more cops at intersections around town?
      iv. If participants say that there is no benefit from this – ask "What if cops needed to see if it was you driving your car, or if you were using your cell phone?"

6) **Conversation: You are having a conversation with friends at home.**

   m. Standard Probes

      i. Do you have any privacy issues or concerns with this situation?
      ii. What about this situation makes it concerning?
      iii. Why

   n. Additions to this scenario

      i. What about in another location, such as a crowded park? Small coffee shop? Taxi/subway?
      ii. What about on the phone?
      iii. What about if you are discussing politics or religion?
      iv. What about if this conversation is taking place over instant messenger? Over a video conference? Or an internet forum? ("What if I asked you to give me your im conversations that are logged?")

Extras

7) Having guests over? (kind of like conversation one)
8) Overhearing someone's cell phone conversation (kind of like having conversation one)
9) Being emotional/sick in front of strangers
10) Imagine you are creating a website about you
11)

Standard follow-ups for all questions:

If off track – say, "That's good, but the focus of this question is [repeat part of question]."

If need additional probe – say, "Any [others, more, one else, thing else]?"

If need explanation – say, "What do you mean?"

If use the term 'privacy' or 'private' – say, "Can you use another word instead of 'private' or 'privacy' in that statement?

Repeat Privacy Definitions

We have talked a lot about different privacy concerns today, so now we would like to revisit an exercise we did at the beginning of the focus group. I'd like you to each take the additional piece of paper in front of you and write out your definition of privacy. Once you are done, please fold the piece of paper and place it in the same envelope as before.

Final questions

So, let's just think back over this hour and a half that we've been together, and try to summarize it a bit.

1) Please sum up your thoughts about privacy into a few sentences. What is your personal take-away from this session?
2) Next, please think about what everyone in the session discussed. If you were going to tell someone who was not here today what the important parts of the discussion were, what would you say?
3) Have your views about privacy changed over the years? Are there circumstances that have changed your views?

OK, we are finished with the discussion. Does anyone have any questions? I am turning the tape recorder off now.

Please complete this technology experience questionnaire. After you complete this questionnaire you are free to go. Thank you for your participation in this focus group.

Credit Consent Form

Georgia Institute of Technology

Project Title: Privacy and Technology: Folk Definitions and Behaviors
Investigators: *Dr. Wendy A. Rogers, Dr. Arthur D. Fisk, Michelle Kwasny & Kelly Caine*

Research Consent Form

You are being asked to be a volunteer in a research study.

Purpose:

The purpose of this form is to inform you about your rights as a research volunteer. Feel free to ask any questions that you may have about the study, what you will be asked to do, and so on.

Thank you for your interest in participating in the study. Our work could not be completed without the help of volunteers. The purpose of this experiment is to understand privacy issues in general and as they relate to technology. We are doing this by asking about 15 older adults and about 15 younger adults to participate in focus group discussions about their perceptions of privacy. With this information, we hope to help inform privacy theory as well as inform designers about the privacy concerns that people may have.

Procedures:

If you decide to participate in this study, your part will involve taking part in a focus group with the experimenter, an assistant, and 5-7 other participants.

It will probably take about 2-2.5 hours to complete this study. You are welcome to take a break at any time during the study. This focus group discussion will be audio-taped and your responses will be transcribed for later analysis. However, your answers to the focus group questions will not be personally identifiable. There is no deception in this study and you can ask any question at any time.

Risks/Discomforts

The following risks/discomforts may occur as a result of your participation in this study:

- Participation in this study involves minimal risk or discomfort to you. The risks involved are no greater than those involved in daily activities such as having a long conversation or doing normal paperwork.

Benefits

The following benefits to you are possible as a result of being in this study:

- You are not likely to benefit substantially from participating in this study. However, your participation will help us obtain information about how adults view privacy. In addition, we hope that others will benefit from what we find in this study.
- If you would like to receive the results of this study, please make sure that we have your contact information.

Compensation to You

You will receive 1 hour of extra credit for each hour you spend in the study. The time to complete the study is approximately 2-2.5 hours, so you will receive 2-2.5 hours of extra credit. If you do not complete the study, you will receive credit based on the time that you were involved in the study.

Confidentiality

The following procedures will be followed to keep your personal information confidential in this study: The data that are collected about you will be kept private to the extent allowed by law. To protect your privacy, your records will be kept under a code number rather than by name. Your records will be kept in locked files and only study staff will be allowed to look at them. Your name and any other fact that might point to you will not appear when results of this study are presented or published. The audio recordings of the focus group will be transcribed and your name will not be included in the transcription. Audio files will be permanently deleted within approximately 2 weeks of transcription.

Confidentiality cannot be guaranteed; your personal information may be disclosed if required by law. This means that there may be rare situations that require us to release personal information about you, for example, in case a judge requires such release in a lawsuit.

To make sure that this research is being carried out in the proper way, the Georgia Institute of Technology IRB will review study records. The Office of Human Research Protections may also look at study records.

Because each individual's data are completely confidential, we cannot mail your individual results. We will mail the group results and a summary of the conclusions once the project is completed.

In Case of Injury/Harm:

Reports of injury or reaction should be made to:
Dr. Wendy Rogers at (404) 894-6775 or
Dr. Arthur Fisk at (404) 894-6066

Neither the Georgia Institute of Technology nor the principal investigator has made provision for payment of costs associated with any injury resulting from participation in this study.

Research Participant Rights

- Your participation in this study is voluntary. You do not have to be in this study if you do not want to be.

- You have the right to change your mind and leave the study at any time without giving any reason, and without penalty.
- Any new information that may make you change your mind about being in this study will be given to you.
- You will be given a copy of this consent form to keep.
- You do not waive any of your legal rights by signing this consent form.

Questions about the Study or Your Rights as a Research Participant

- If you have any questions about the study, you may contact the investigator at 404-385-0798 or 404-894-8344.
- If you have any questions about your rights as a research participant, you may contact Ms. Melanie Clark, Georgia Institute of Technology at (404) 894-6942.

If you sign below, it means that you have read (or have had read to you) the information given in this consent form, and you would like to be a volunteer in this study.

____

Participant Name

____

Participant Signature
Date

____

Signature of Person Obtaining Consent
Date

If you must cancel a scheduled time to come to the lab, please call: (404) 894-8344.

Pay Consent Form

Georgia Institute of Technology

Project Title: Privacy and Technology: Folk Definitions and Behaviors

Investigators: *Dr. Wendy A. Rogers, Dr. Arthur D. Fisk, Michelle Kwasny & Kelly Caine*

Research Consent Form

You are being asked to be a volunteer in a research study.

Purpose:

The purpose of this form is to inform you about your rights as a research volunteer. Feel free to ask any questions that you may have about the study, what you will be asked to do, and so on.

Thank you for your interest in participating in the study. Our work could not be completed without the help of volunteers. The purpose of this experiment is to understand privacy issues in general and as they relate to technology. We are doing this by asking about 15 older adults and about 15 younger adults to participate in focus group discussions about their perceptions of privacy. With this information, we hope to help inform privacy theory as well as inform designers about the privacy concerns that people may have.

Procedures:

If you decide to participate in this study, your part will involve taking part in a focus group with the experimenter, an assistant, and 5-7 other participants.

It will probably take about 2-2.5 hours to complete this study. You are welcome to take a break at any time during the study. This focus group discussion will be audio-taped and your responses will be transcribed for later analysis. However, your answers to the focus group questions will not be personally identifiable. There is no deception in this study and you can ask any question at any time.

Risks/Discomforts

The following risks/discomforts may occur as a result of your participation in this study:

- Participation in this study involves minimal risk or discomfort to you. The risks involved are no greater than those involved in daily activities such as having a long conversation or doing normal paperwork.

Benefits

The following benefits to you are possible as a result of being in this study:

- You are not likely to benefit substantially from participating in this study. However, your participation will help us obtain information about how adults view privacy. In addition, we hope that others will benefit from what we find in this study.
- If you would like to receive the results of this study, please make sure that we have your contact information.

Compensation to You

You will receive $10 per hour for each hour you spend in the study. The time to complete the study is approximately 2-2.5 hours, so you will receive about $25.

Confidentiality

The following procedures will be followed to keep your personal information confidential in this study: The data that are collected about you will be kept private to the extent allowed by law. To protect your privacy, your records will be kept under a code number rather than by name. Your records will be kept in locked files and only study staff will be allowed to look at them. Your name and any other fact that might point to you will not appear when results of this study are presented or published. The audio recordings of the focus group will be transcribed and your name will not be included in the transcription. Audio files will be permanently deleted within approximately 2 weeks of transcription.

Confidentiality cannot be guaranteed; your personal information may be disclosed if required by law. This means that there may be rare situations that require us to release personal information about you, for example, in case a judge requires such release in a lawsuit.

To make sure that this research is being carried out in the proper way, the Georgia Institute of Technology IRB will review study records. The Office of Human Research Protections may also look at study records.

Because each individual's data are completely confidential, we cannot mail your individual results. We will mail the group results and a summary of the conclusions once the project is completed.

In Case of Injury/Harm:

Reports of injury or reaction should be made to:
Dr. Wendy Rogers at (404) 894-6775 or
Dr. Arthur Fisk at (404) 894-6066

Neither the Georgia Institute of Technology nor the principal investigator has made provision for payment of costs associated with any injury resulting from participation in this study.

Research Participant Rights

- Your participation in this study is voluntary. You do not have to be in this study if you do not want to be.
- You have the right to change your mind and leave the study at any time without giving any reason, and without penalty.

- Any new information that may make you change your mind about being in this study will be given to you.
- You will be given a copy of this consent form to keep.
- You do not waive any of your legal rights by signing this consent form.

Questions about the Study or Your Rights as a Research Participant

- If you have any questions about the study, you may contact the investigator at 404-385-0798 or 404-894-8344.
- If you have any questions about your rights as a research participant, you may contact Ms. Melanie Clark, Georgia Institute of Technology at (404) 894-6942.

If you sign below, it means that you have read (or have had read to you) the information given in this consent form, and you would like to be a volunteer in this study.

____

Participant Name

____

Participant Signature
Date

____

Signature of Person Obtaining Consent
Date

If you must cancel a scheduled time to come to the lab, please call: (404) 894-8344.

APPENDIX B

MATERIALS FOR STUDY 2

Protocol

I. Informed consent
   a. Bring participant in and seat him/her, provide informed consent forms and pens
   b. Explain informed consent
   c. Give informed consent forms (one for participants receiving credit, one for participants receiving payment)
   d. Wait for participants to read consent
   e. Answer questions
   f. After participants have signed consent forms, sign as experimenter
   g. Give participants their copy of their informed consent for their records

II. Instructions
   a. Provide participants with introduction to interview, topics to be covered
   b. Answer any questions

III. During Testing/Interview
   a. Provide demographics questionnaire, technology experience questionnaire, and privacy attitudes questionnaire
   b. Be available to answer questions
   c. Go through structured interview

IV. Exit Survey
   a. Thank participant for completing task
   b. Read survey questions from script
   c. Record answers to survey questions

V. Debriefing
   a. As they complete the study, provide participants with the debriefing form in the next room
   b. Provide debriefing form to participant
   c. Answer questions participant might have

VI. Compensation
   a. Provide participant with check
      or
   b. Assign credit

Critical Incident Interview

In this interview we are interested in learning about experiences you may have had with misclosures. A *disclosure* is when you intentionally reveal personal information to others. A *misclosure,* on the other hand, is when you unintentionally reveal information or make a disclosure error.

In particular, in this interview, we are interested in misclosures that may have occurred while you were using technology.

Examples of the type of technology we are interested in include cell phones, email, online banking, online healthcare, shopping online like Amazon, and social networking like Facebook and similar technologies.

There are different types of misclosures. First, you may give unintended information to the person you intended to give it to. Second, you may give information you intended to give, but to a person you did not intend to give it to. Thirdly, you may give unintended information, and give it to a person you did not intend to give it to.

For example, I could have speed dialed my mother on my phone and left a message, but accidentally speed dialed someone else. This constitutes the first kind of misclosure.

As another example, I could have sent an email to my boss, but attached a family photo. I meant to attach a photo from a presentation I gave, but I attached the family reunion photo instead. This constitutes the second kind of misclosure, even though I sent it to the right person. However, it wouldn't be a misclosure if you wrote an email and then forgot to attach an attachment because you did not disclose information that you did not intend to.

We would also like for you to include any instances where these kinds of misclosures almost happened, but you caught yourself before the event actually occurred.

We will begin by asking you to write down specific incidents in the past, and then ask questions about each incident specifically.

We will not ask you to reveal any specific personal information, just what kind of information it was that you misclosed. What we want to know about is the circumstances surrounding the kinds of events that we will ask you about.

Please remember that you are free to refuse to answer any of these questions without any penalty, and that you may stop participating in this interview at any time.

Think about the (first, second, next…) example that you have written down.

When did this happen?

Did you disclose the information that you intended to?

- o ___Yes
- o ___No

IF NO: What was wrong with the information you sent?

- o ___Completely wrong
- o ___Inaccurate
- o ___Not current
- o ___Other:

Did you disclose the information to the intended person?

- o ___Yes
- o ___No

IF NO: Who did you mean to send it to?

- o ___Family member
- o ___Significant other
- o ___Friend
- o ___Colleague
- o ___Boss/superior
- o ___Professional
- o ___Merchant
- o ___Don't Remember
- o ___Other:

And who did you actually send it to?

- o ___Family member
- o ___Significant other
- o ___Friend
- o ___Colleague
- o ___Boss/superior
- o ___Professional
- o ___Merchant
- o ___Don't Remember
- o ___Other:

What kind of information were you trying to disclose? (Something general like health or location is as far as you have to go to answer this question.)

- o ___Health

- o ___Location/activity
- o ___Work related
- o ___Family related
- o ___Financial
- o ___Personal
- o ___Conversation
- o ___Request for information
- o ___Sex
- o ___First Name
- o ___Education Level
- o ___Age
- o ___Marital status
- o ___Interests/Hobbies
- o ___Product preferences
- o ___Race/Ethnicity
- o ___Occupation
- o ___Email address
- o ___Number of people in household
- o ___Political party affiliation
- o ___Recent online purchases
- o ___Last name
- o ___Religion
- o ___Postal address
- o ___Income
- o ___Telephone number
- o ___Draft of work project
- o ___Child's name
- o ___Credit care number
- o ___Banking information
- o ___Social security number
- o ___Location
- o ___Don't remember
- o ___Other:

How private did you consider this information?

- o ___(5) Very private
- o ___(4) Private
- o ___(3) Neutral
- o ___(2) Not very private
- o ___(1) Not at all private

How sensitive did you consider this information?

- o ___(5) Very sensitive
- o ___(4) Sensitive
- o ___(3) Neutral

- ___(2) Not very sensitive
- ___(1) Not at all sensitive

What kind of system were you using?

- ___Cell phone
- ___Email
- ___Instant messaging
- ___Text messaging
- ___Online banking
- ___Online health care
- ___Online shopping
- ___Online social network (facebook, etc.)
- ___Online work/project management
- ___Online school/project management

How familiar were you with the system?

- ___Very familiar
- ___Familiar
- ___Neither familiar nor unfamiliar
- ___Not very familiar
- ___Never used before (completely unfamiliar)

How long had you been using this system?

Would you place the blame on this mistake more on the technology, yourself, or both?

- ___Tech
- ___Self
- ___Both

Were there any factors of this system that contributed to this mistake?

- ___Single aspect of the system
- ___Lack of familiarity
- ___Hard to use
- ___Auto-fill/predictive text features
- ___Similar to other system, but different function

Were there any things you did that contributed to this mistake?

- ___Carelessness
- ___Did not double check
- ___Multitasking/concurrent activities
- ___Lack of familiarity
- ___Distracted by surroundings
- ___Distracted (inside? By self/thoughts)
- ___In a hurry

Where were you?

o ___At home
o ___At work
o ___In the car
o ___In public
o ___On my way from [_________] to [_________]
o ___Do not recall
o ___Other:

Were you doing anything else when this happened? If so, what were you doing?

o ___Driving
o ___Shopping
o ___Social
o ___Church
o ___Class/work
o ___Not specific
o ___Do not recall
o ___Multitasking general
o ___Other:

How much was the setting or environment around you distracting you when this misclosure happened?

o ___Very distracting
o ___Somewhat distracting
o ___Neutral
o ___Not very distracting
o ___Not distracting at all
o ___Don't remember

How urgent did you think that it was to perform the action you intended to perform?

o ___Very Urgent
o ___Urgent
o ___Somewhat Urgent
o ___Not very Urgent
o ___Not Urgent
o ___Don't remember

How quickly did you have to try and [*insert task being discussed*] at that time?

o ___Very quickly
o ___Somewhat quickly
o ___Neutral
o ___Not very quickly
o ___Not at all

Were there any negative consequences?

- o ___Yes
- o ___No

What were they?

Has this happened any other times?

- o ___Yes
- o ___No

How often has this happened?

Have you taken any steps to make sure this doesn’t happen again?

- o ___No
- o ___Tried to be more careful
- o ___Always double check
- o ___Other:

Has anything like this ever happened to you?

Other Misclosures (order counterbalanced)

Recipient Misclosure
I noticed you mainly told me about times when you disclosed the wrong information to the person that you intended to. Another kind of incident that we want to know about is when you give information you intended to give, but to a person you did not intend to give it to.

Has anything like this ever happened to you? (repeat questions)

Combination Misclosure
Another kind of incident that we are looking for is when you give information that you didn’t intend to give, and you gave it to an unintended person.

Has anything like this ever happened to you? (repeat questions)

Near misses

Can you think of any times when these kinds of mistakes *almost* happened but did not?

(Repeat questions)

Specific Questions (still drafting these – will be updated as we run pilots and get more examples)

- Have you attached the wrong attachment (such as the wrong photo) to an email?

- Yes
- No

How often has this happened to you, etc.

- Have you attached the wrong attachment (such as the wrong photo) to an email?

- Yes
- No

Have you ever sent an email to the wrong person?

- Have you attached the wrong attachment (such as the wrong photo) to an email?

- Yes
- No

Have you ever replied to all when you meant to only reply to one person?

- Have you attached the wrong attachment (such as the wrong photo) to an email?

- Yes
- No

Have you ever posted information on a social networking site that you meant for only some people to see, but others that you didn't want to see were able to see?

- Have you attached the wrong attachment (such as the wrong photo) to an email?

- Yes
- No

Have you ever sent a text message to the wrong person?

- Have you attached the wrong attachment (such as the wrong photo) to an email?

Reminder Sheet for Participant

To begin, please take 5 minutes to think about times when you've made disclosure errors in the past.

Please list those below (for your own use)

Remember: it is a misclosure if you disclose information and either:

- You disclosed information you did not intend to disclose
- You disclosed information you did intend to disclose, but to a person you did not intend the information for
- You disclosed information you did not intend to disclose to a person you did not intend the information for.
- Have to have disclosed information, not forgotten to disclose it

Remember:

Intended information	→	Intended person	=	Successful Disclosure
	→	Unintended person	=	Misclosure
Unintended information	→	Intended person	=	Misclosure
	→	Unintended person	=	Misclosure

Consent Form

Georgia Institute of Technology

Protocol and Consent Title: Disclosure Errors (version 1, 2009)

Investigators: Dr. Arthur D. Fisk, Dr. Wendy A. Rogers (Principal Investigators), Kelly Caine and Alan Poole (Student Investigators)

Purpose:

You are being asked to be a volunteer in a research study. The purpose of this form is to tell you about the tasks you will be asked to complete today and to inform you about your rights as a research volunteer. Feel free to ask any questions that you may have about the study, what you will be asked to do, and so on.

Thank you for your interest in participating in the study. The purpose of this research to determine the conditions surrounding mistakes people make in the disclosure of private information when using technology systems. With this information, we hope to be able to inform designers about common errors with privacy and technology.

Exclusion/Inclusion Criteria:

Participants in this study must be between the ages of 18 and 28 or 65 and 80 and have used technology such as cell phones, email, or social networking in the past.

Procedures:

If you decide to participate in this study, your part will involve answering questions on questionnaires and responding to interview questions about any errors that may have occurred when you were using technology to disclose information. At the end of the session we will also ask you a few questions about your experience during the interview (an exit survey). We plan to record only the interview portion of this study using audio and/or videotape.

It will probably take about an hour and a half to complete the entire study. You are welcome to take a break at any time during the study.

There is no deception in this study and you can ask any question at any time.

Risks/Discomforts:

The following risks/discomforts may occur as a result of your participation in this study. Participation in this study involves minimal risk or discomfort to you. Risks are minimal and do not exceed those of normal office work. Please tell us if you are having trouble with any task.

Benefits:

You are not likely to benefit in any way from joining this study. However, we hope that others will benefit from what we find in doing this study.

Compensation to You:

You will receive either $25 or 1.5 Experimetrix credits if you complete this study. If you do not complete the study and are receiving money you will receive $25. Instead of monetary compensation, Georgia Tech students will receive 1.0 Experimetrix credits for each hour of participation. If you withdraw from the study early for any reason, you will receive 1 credit per hour for your time.

Confidentiality:

The following procedures will be followed to keep your personal information confidential in this study: All data that are collected about you will be kept private to the extent allowed by law. To protect your privacy, your records will be kept under a code number rather than by name. Your records will be kept in locked files and only study staff will be allowed to look at them.

The interview portion of this study will be audio and/or video recorded. We may use these recordings in presentations and/or publications resulting from this study, however, your name will not be associated with the recording.

Please, select ONE of the following options for use of audio/video recordings by initialing your preference below.

> If you are willing to allow us to use a recording of any portion of your interview, please initial here _______. If you have initialed here, we may use a portion of your interview in a presentation, for example, but you will never be identified by name.
>
> If you would prefer that we use information from your audio/video recording only in transcribed form (rather than as an audio or video clip), please initial here________.

Confidentiality cannot be guaranteed; your personal information may be disclosed if required by law. This means that there may be rare situations that require us to release personal information about you, for example, in case a judge requires such release in a lawsuit or if you tell us of your intent to harm yourself or others (including reporting behaviors consistent with child abuse). In addition, if you allow us to use a recording of your interview in a presentation it is possible that someone who sees the presentation may recognize you. If you prefer, we will only use information from your audio/video recording in transcribed form (rather than as an audio or video clip).

To make sure that this research is being carried out in the proper way, the Georgia Institute of Technology IRB may review study records. The Office of Human Research Protections may also look over study records during required reviews.

Because each individual’s data and test scores are completely confidential, we cannot mail your individual results.

Costs to You:

There are no costs to you, other than your time, associated with participating in this study.

In Case of Injury/Harm:

If you are injured as a result of being in this study, please contact Dr. Arthur D. Fisk at 404-894-6066 or Dr. Wendy A. Rogers at 404-894-6775. Neither the Georgia Institute of Technology nor the principle investigators have made provision for payment of costs associated with any injury resulting from participation in this study.

Participant Rights:

- Your participation in this study is voluntary. You do not have to be in this study if you don't want to be.
- You have the right to change your mind and leave the study at any time without giving any reason and without penalty.
- Any new information that may make you change your mind about being in this study will be given to you.
- You will be given a copy of this consent form to keep.
- You do not waive any of your legal rights by signing this consent form.

Questions about the Study or Your Rights as a Research Participant:

- If you have any questions about the study, you may contact the investigator obtaining consent (listed below) at 404-385-0798.
- If you have any questions about your rights as a research participant, you may contact Ms. Kelly Winn, Georgia Institute of Technology, Office of Research Compliance, at (404) 385- 2175.

If you sign below, it means that you have read (or have had read to you) the information given in this consent form, and you would like to be a volunteer in this study.

____

Participant Name (please print)

____

Participant Signature Date

Name of Investigator Obtaining Consent (please print)

____

Signature of Investigator Obtaining Consent Date

APPENDIX C

MATERIALS USED FOR BOTH STUDIES

Overview of Materials For Both Studies

1. Privacy Attitudes Questionnaire
2. Contact Form
3. Demographics and Health Questionnaire
4. Technology Experience Questionnaire

Privacy Attitudes Questionnaire

The purpose of this set of questions is to understand your privacy attitudes. Please answer the following eight questions by placing a check mark at the chosen response.

1. Consumers have lost all control over how personal information is collected and used by companies.

□	□	□	□	□
Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree

2. Most businesses handle the personal information they collect about consumers in a proper and confidential way.

□	□	□	□	□
Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree

3. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

□	□	□	□	□
Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree

4. I am concerned about online identity theft.

□	□	□	□	□
Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree

5. I am concerned about my privacy online.

□	□	□	□	□
Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree

6. I am concerned about my privacy in everyday life.

□	□	□	□	□
Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree

7. I am likely to read the privacy policy of an ecommerce site before buying anything.

□	□	□	□	□
Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree

8. Privacy policies accurately reflect what companies do.

□	□	□	□	□
Strongly Disagree	Disagree	Neither agree nor disagree	Agree	Strongly Agree

Education completed (check highest level)

□1 Less than high school graduate
(highest grade completed? ________)

□2 High school graduate/G.E.D.

□3 Some college, or trade, technical, or business school
(how many years? _________)

□4 Bachelor's degree

□5 Some graduate work (how many years? _____)

□6 Master's degree

□7 M.D., J.D., Ph.D., other advanced degree

1. Current marital status (check one)

□1 Single

□2 Married

□3 Separated

□4 Divorced

□5 Widowed

□6 Other (please specify _________________)

2. Race/ethnicity

□1 Black/African American

□2 Asian American/Pacific Islander

□3 White/Caucasian

□4 Hispanic/Latino

□5 American Indian/Alaskan Native

□6 Multiracial (please specify ____________)

□7 Other (please specify ________________)

3. In which type of housing do you live?

□1 Residence hall/College dormitory

□2 House/Apartment/Condominium

□3 Senior housing (independent)

□4 Assisted living

□5 Nursing home

□6 Relative's home

□7 Other (please specify ________________)

4. **Do you live alone a majority of the year?**

□1 Yes
□2 No

5. **What is your primary language?**

□1 English
□2 Spanish
□3 French
□4 Creole
□5 Portuguese
□6 Other __________

6. **Occupational status (check <u>all</u> that apply)**

□1 Working full-time

□2 Working part-time

□3 Student

□4 Homemaker

□5 Retired

□6 Volunteer worker

□7 Seeking employment, laid off, etc.

□8 Leave of absence
□9 Other (please specify):

7. **What is your current occupation? ______________________________**

<u>If retired:</u>

8. **What was your primary occupation? __________________________**

10. **What year did you retire?** __________________

Demographics and Health Questionnaire

Please answer the following questions. All of your answers will be treated confidentially. Any published document regarding these answers will not identify individuals with their answers. **If there is a question you do not wish to answer, please just leave it blank and go on to the next question.** Thank you in advance for your help.

Demographics Questionnaire

Gender: Male □1   Female □2   Date of Birth: __ __ / __ __ / __ __   Age: _______

9. What is your highest level of education?

□1 No formal education
□2 Less than high school graduate
□3 High school graduate/GED
□4 Vocational training
□5 Some college/Associate's degree
□6 Bachelor's degree (BA, BS)
□7 Master's degree (or other post-graduate training)
□8 Doctoral degree (PhD, MD, EdD, DDS, JD, etc.)

10.Current marital status (check one)

□1 Single
□2 Married
□3 Separated
□4 Divorced
□5 Widowed
□6 Other (please specify) ___________________

11.Do you consider yourself Hispanic or Latino?

□1 Yes
□2 No

3 a. If “Yes”, would you describe yourself:

□1 Cuban
□2 Mexican
□3 Puerto Rican
□4 Other (please specify) ________________

12.How would you describe your primary racial group?

□1 No Primary Group
□2 White Caucasian
□3 Black/African American
□4 Asian
□5 American Indian/Alaska Native
□6 Native Hawaiian/Pacific Islander
□7 Multi-racial
□8 Other (please specify) ______________________

13.In which type of housing do you live?

□1 Residence hall/College dormitory
□2 House/Apartment/Condominium
□3 Senior housing (independent)
□4 Assisted living
□5 Nursing home
□6 Relative's home
□7 Other (please specify) ________________

14.Which category best describes your yearly household income. Do not give the exact amount, just a range or approximate family income:

____

15.Is English your primary language?

□1 Yes
□2 No

7 a. If "No", What is your primary language? ________________________

8. What is your primary mode of transportation? (Check one)

□1 Drive my own vehicle
□2 A friend or family member takes me to places I need to go
□3 Transportation service provided by where I live
□4 Use public transportation (e.g., bus, taxi, subway, van services)

Occupational Status

9. What is your primary occupational status? (Check one)

□1 Work full-time
□2 Work part-time
□3 Student
□4 Homemaker
□5 Retired
□6 Volunteer worker
□7 Seeking employment, laid off, etc.
□8 Other (please specify) ____

10. Do you currently work for pay?

□1 Yes, Full-time
□2 Yes, Part-time
□3 No

10 a. If “Yes”, what is your primary occupation?

____

<u>If retired:</u>

11. What was your primary occupation? ___________________________

12. What year did you retire? ______________________

Health Information

1. In general, would you say your health is:

□$_1$ Poor □$_2$ Fair □$_3$ Good □$_4$ Very good □$_5$ Excellent

2. Compared to other people your own age, would you say your health is:

□$_1$ Poor □$_2$ Fair □$_3$ Good □$_4$ Very good □$_5$ Excellent

3. How satisfied are you with your present health?

□$_1$ Not at all satisfied □$_2$ Not very satisfied □$_3$ Neither satisfied nor dissatisfied □$_4$ Somewhat satisfied □$_5$ Extremely satisfied

4. How often do health problems stand in the way of your doing the things you want to do?

□$_1$ Never □$_2$ Seldom □$_3$ Sometimes □$_4$ Often □$_5$ Always

6. The following items are about activities you might do during a typical day. Does your health now limit you in these activities? Check one box for each type of activity.

	Yes$_1$, **Limited a lot**	Yes$_2$, **Limited a little**	No$_3$, **Not limited at all**
a. Bathing or dressing yourself			
b. Bending, kneeling, or stooping			
c. Climbing **one** flight of stairs			
d. Climbing **several** flights of stairs			
e. Lifting or carrying groceries			

f. Moderate activities, such as moving a table, pushing a vacuum cleaner, bowling, or playing golf			
g. Vigorous activities, such as running, lifting heavy objects, or participating in strenuous sports (e.g., swimming laps)			
h. Walking **more than a mile**			
i. Walking **one block**			
j. Walking **several blocks**			

6. **Are you on post-menopausal estrogen replacement therapy?**

□$_1$ Yes □$_2$ No □$_3$ Not applicable

7. **For each of the following conditions please indicate if you have ever had that condition in your life, have the condition now at this time or never had the condition.**
Check <u>one</u> box for each condition.

I...1.1.1 Condition	**In your lifetime$_1$**	**Now$_2$**	**Never$_3$**
a. Arthritis			
b. Asthma or Bronchitis			
c. Cancer (other than skin cancer)			
d. Diabetes			
e. Epilepsy			
f. Heart Disease			
g. Hearing Impairment			
h. Hypertension			
i. Stroke			
j. Vision Impairment			
k. Other significant illnesses (please list)			

Medication Usage Details

Please list all medical products that you are currently taking. Include medicinal herbs, vitamins, aspirin, antacid, nasal spray, laxatives, etc., as well as prescription medications (copy names from label if possible). This information will be completely confidential.

EXAMPLE

Name of Medication: Zarontin

Reason for taking: epilepsy Dosage (ea. time taken): 500 mg

How often do you take the medication? (circle one)

daily [✓ every other day] weekly as needed

On days that you take the medication, how many times per day do you take it?

What time of day do you take the medication? morning, afternoon, evening

How long you have been taking the medication? 5 years

Does this medication cause any problems? makes me sleepy

1. Name of Medication: ______________________________

Reason for taking: ______________________ Dosage (ea. time taken): ________

How often do you take the medication? (circle one)

daily every other day weekly as needed

On days that you take the medication, how many times per day do you take it?

What time of day do you take the medication?

How long you have been taking medication? ____________________________

Does this medication cause any problems? ____________

____

TECHNOLOGY AND COMPUTER EXPERIENCE QUESTIONNAIRE

The purpose of this set of questions is to assess your familiarity and experience with technology. Please answer all questions by placing a check mark at the appropriate response.

1. How often do you communicate with other people (e.g., family members, friends, doctors, customer service representatives)?

□$_1$ Daily
□$_2$ Weekly
□$_3$ Monthly
□$_4$ Yearly
□$_5$ Never

2. Within the last year, which of the following methods have you **used** for communication?

	Not sure what it is$_1$	Never$_2$	Once in a while$_3$	Some of the time$_4$	Most of the time$_5$	Always$_6$
1. Answering machine						
2. Cell phone						
3. Fax machine						
4. Internet (e.g., e-mail, chat room, videoconferencing)						
5. Telephone						
6. Videophone						

3. How often do you go shopping?

□1 Daily
□2 Weekly
□3 Monthly
□4 Yearly
□5 Never

4. Within the last year, which of the following have you **used** for shopping?

	Not sure what it is1	Never2	Once in a while3	Some of the time4	Most of the time5	Always6
1. Credit card						
2. Debit card						
3. In-store automated kiosk (e.g., self-checkout, price scanner, item locator)						
4. Internet (e.g., on-line purchasing, on-line product evaluation)						
5. Telephone						
6. Television shopping						

5. How often do you use customer service functions (e.g., technical support, product assistance, reservations)?

□1 Daily
□2 Weekly
□3 Monthly
□4 Yearly
□5 Never

6. Within the last year, which of the following have you **used** for customer service (e.g., technical support, product assistance, reservations)?

	Not sure what it is$_1$	Never$_2$	Once in a while$_3$	Some of the time$_4$	Most of the time$_5$	Always$_6$
1. Automated telephone menu system						
2. CD/DVD						
3. E-mail						
4. Fax machine						
5. Internet (e.g., on-line manuals, on-line interactive support, web site)						
6. Person on the telephone						

7. How often do you make financial transactions (e.g., bill paying, banking, investing/ financial planning, tax preparation)?

□$_1$ Daily
□$_2$ Weekly
□$_3$ Monthly
□$_4$ Yearly
□$_5$ Never

8. Within the last year, which of the following have you **used** for financial transactions (e.g., bill paying, banking, investing/financial planning, tax preparation)?

	Not sure what it is$_1$	Never$_2$	Once in a while$_3$	Some of the time$_4$	Most of the time$_5$	Always$_6$
1. Automated telephone menu system (e.g., banking, credit card information)						
2. Automatic teller machine (ATM)						
3. Drive-through banking						
4. Internet (e.g., on-line banking, on-line bill paying, on-line investing)						
5. Person on the telephone						
6. Software (e.g., Quicken, spreadsheet, MS Money, TurboTax)						

9. How often do you engage in healthcare related activities for yourself or others (e.g., going to see a doctor, checking blood pressure, finding information about a disease or medication)?

□$_1$ Daily
□$_2$ Weekly
□$_3$ Monthly
□$_4$ Yearly
□$_5$ Never

10. Within the last year, which of the following have you **used** for healthcare related activities for yourself or others?

	Not sure what it is$_1$	Never$_2$	Once in a while$_3$	Some of the time$_4$	Most of the time$_5$	Always$_6$
1. Automated telephone menu system						
2. Health information searching on the Internet						
3. Internet communication (e.g., e-mail, computer support groups)						
4. Medical-related Internet purchasing (e.g., medication or medical supplies)						
5. Person on the telephone						
6. Telemedicine (e.g., videoconferencing with doctors or nurses)						

11. How often do you use healthcare devices at home for yourself or others (e.g., glucose monitor, blood pressure monitor)?

□$_1$ Daily
□$_2$ Weekly
□$_3$ Monthly
□$_4$ Yearly
□$_5$ Never

12. Within the last year, which of the following healthcare devices have you **used** in your home?

	Not sure what it is$_1$	Never$_2$	Once in a while$_3$	Some of the time$_4$	Most of the time$_5$	Always$_6$
1. Blood pressure measurement device						
2. Digital thermometer						
3. Electronic dental hygiene system (e.g., electric toothbrush, Waterpik)						
4. Emergency call system (e.g., Lifeline)						
5. Heating pads						
6. Infusion pump						
7. Monitoring device (e.g., glucose, apnea, cardiac)						
8. Nebulizers						
9. Oxygen equipment						

13. How often do you use public transportation (e.g., train, bus, subway)?

□$_1$ Daily
□$_2$ Weekly
□$_3$ Monthly
□$_4$ Yearly
□$_5$ Never

14. How often do you drive?

□$_1$ Daily
□$_2$ Weekly
□$_3$ Monthly
□$_4$ Yearly
□$_5$ Never

15. How often do you travel by airplane?

□1 Weekly
□2 Monthly
□3 Quarterly
□4 Yearly
□5 Never

16. Within the last year, which of the following transportation-related systems have you **used**?

	Not sure what it is1	Never2	Once in a while3	Some of the time4	Most of the time5	Always6
1. Automated telephone menu system						
2. Automatic check-in station						
3. Automatic parking payment station						
4. Automatic ticket purchase station						
4. Cruise control in your car						
5. In-car navigation system (e.g., GPS, OnStar, Neverlost)						
6. On-line travel schedule						
7. Personal digital assistant (PDA)						
8. Person on the phone						
9. Remote control to start the car						
10. Travel direction/ map software (e.g., MapQuest, Streets & Trips, Keyhole)						

17. How often do you engage in leisure/hobby/entertainment-related activities?

□1 Daily
□2 Weekly
□3 Monthly
□4 Yearly
□5 Never

18. Within the last year, which of the following leisure/hobby/entertainment-related systems have you **used**?

	Not sure what it is$_1$	Never$_2$	Once in a while$_3$	Some of the time$_4$	Most of the time$_5$	Always$_6$
1. Books on tape (audio book)						
2. Computer/Video game (e.g., Gameboy, PlayStation, Nintendo, GameCube, X-Box)						
3. Digital photography (e.g., camera, camcorder)						
4. Fitness device (e.g., pedometer, pulse meter, golf swing enhancer, treadmill)						
5. Hobby-specific computer usage (e.g., Internet, Photoshop, genealogy software, patterns)						
6. MP3/IPOD						
7. Personal digital assistant (PDA)						
8. Recording and playback device (e.g., CD, DVD, VCR)						
9. TV set-top box (e.g., program TV, pay-per view movies, music stations, TiVo)						

19. How often do you engage in learning/educational/self-help activities?

□1 Daily
□2 Weekly
□3 Monthly
□4 Yearly
□5 Never

20. Within the last year, which of the following learning/educational/self-help-related systems have you **used**?

	Not sure what it is1	Never2	Once in a while3	Some of the time4	Most of the time5	Always6
1. Computer-based instruction (e.g., CD, DVD, VCR)						
2. Computer support group (e.g., chat room, discussion forum)						
3. Digital or tape recorder						
4. Internet searching (e.g., Google, directories, URLs, newspapers)						
5. Language learning and translation systems						
6. Online library database/catalog						

21. On average, how many hours per day do you spend at home?

□1 Less than 8 hours
□2 8-11 hours
□3 12-15 hours
□4 16-19 hours
□5 20-24 hours

22. Within the last year, which of the following home-based systems have you **used**?

	Not sure what it is1	Never2	Once in a while3	Some of the time4	Most of the time5	Always6
1. Garage door opener						
2. Microwave oven						
3. Home security system (e.g., visitor entry directory system, home alarm, gate access)						
4. Personal computer						
5. Programmable device (e.g., lights, thermostat, sprinkler, programmable food processor, programmable coffee maker)						
6. Robot (e.g., vacuum cleaner, lawn mower)						

23. On average, how many hours **per week** do you work (including volunteer work) in or out of the home? (For the purpose of this question you should not consider activities such as homemaking or family caregiving)

□1 0
□2 1 – 10 hours
□3 11 – 20 hours
□4 21 – 30 hours
□5 31 – 40 hours
□6 More than 40 hours

24. Within the last year, which of the following technologies have you **used** in the context of your work?

	Not sure what it is1	Never2	Once in a while3	Some of the time4	Most of the time5	Always6
1. Bar code scanner						
2. Cell phone						
3. Computer						
4. Copier/scanner						
5. Recording or playback device (e.g., CD, DVD, VCR)						
6. Electronic cash register (point of sale terminal)						
7. E-mail						
8. Fax machine						
9. Internet						
10. LCD projector						
11. Multifunction telephone system (e.g., with conferencing, speaker, transfer capabilities)						
12. Pager/Beeper						
13. Personal digital assistant (PDA)						
14. Voice recorder (e.g., dictaphone, digital recording						

	Not sure what it is$_1$	Never$_2$	Once in a while$_3$	Some of the time$_4$	Most of the time$_5$	Always$_6$
system, handheld tape recorder)						

25. For each of activities listed in the table, please indicate how important technology is to the performance of the activity.

	Not at all important$_1$	Somewhat important$_2$	Neutral$_3$	Important$_4$	Very important$_5$
1. Communication activities					
2. Customer service activities					
3. Financial transaction activities					
4. Healthcare related activities for yourself or others					
5. Home activities					
6. Learning/education/ self-help activities					
7. Leisure/hobby/ entertainment activities					
8. Shopping activities					
9. Transportation activities					
10. Use of healthcare devices in your home					
11. Work activities					

26. How much more training would you like to have in the use of technology?

□$_1$ None

□$_2$ A little

□$_3$ Moderate training

□$_4$ A lot

27. Have you had experience with computers?

□1 Yes

□2 No (Skip the rest of the questionnaire)

28. For each input device listed below, please indicate how much experience you have had with the device in the past year.

	Not sure what it is1	Never used2	Used once3	Used occasionally4	Used frequently5
1. Joystick					
2. Keyboard					
3. Light-pen					
4. Mouse					
5. Rotary input knob					
6. Speech Recognition System					
7. Touch screen with finger					
8. Touch screen with stylus					
9. Trackball					

29. For each basic computer operation listed below, please indicate how much experience you have had with the operation in the past year.

	Not sure what it is1	Never used2	Used once3	Used occasionally4	Used frequently5
1. Delete a file					
2. Insert a disk/CD/DVD					
3. Install software					
4. Open a file					
5. Save a file					
6. Set printer options					
7. Set monitor options					
8. Transfer files					
9. Use a printer					
10. Use cut-and-paste					

30. For each item listed below, please indicate how much experience you have had with the item in the past year.

	Not sure what it is$_1$	Never used$_2$	Used once$_3$	Used occasionally $_4$	Used frequently $_5$
1. Apple (Macintosh) operating system					
2. CD/DVD creation software					
3. Computer graphics (e.g., Photoshop, Harvard Graphics, AutoCAD)					
4. Conferencing software					
5. Database management (e.g., Access, Filemaker, Lotus 123)					
6. E-mail					
7. Home computer network (e.g., wire or wireless)					
8. Instant messaging					
9. Internet phone					
10. Presentation software (e.g., PowerPoint, Freelance)					
11. Programming package (e.g., Basic, C++, Fortran, Java)					
12. Spreadsheet (e.g., Excel, Quattro Pro)					
13. Statistical package (e.g., SPSS, SAS)					
14. UNIX/LINUX operating system					
15. Web design software (e.g., Java, HTML)					
16. Windows operating system					
17. Word processing (e.g., Microsoft Word, WordPerfect)					

31. For each windows operation listed below, please indicate how much experience you have had with the operation in the past year.

	Not sure what it is$_1$	Never used$_2$	Used once$_3$	Used occasionally$_4$	Used frequently$_5$
1. Change audio settings					
2. Change screen settings					
3. Change network settings					
4. Click icon					
5. Close a window					
6. Empty trash					
7. Manage multiple windows					
8. Move between windows					
9. Open a window					
10. Perform operations using right click on mouse					
11. Resize a window					
12. Scroll horizontally					
13. Scroll vertically					
14. Search for files					
15. Update the clock					
16. Use drop-down menu					
17. Use windows help system					

Internet Questionnaire

The purpose of this set of questions is to assess your familiarity and experience with the Internet. Please answer all questions by placing a check mark on or filling in the appropriate response.

1. **About how many hours a week do you use the Internet?**

□1 Never (Skip the rest of the questionnaire)
□2 Less than one hour a week
□3 Between 1 hour and 5 hours a week
□4 Between 6 hours and 10 hours a week
□5 Between 11 hours and 15 hours a week
□6 More 15 hours a week

2. **How long have you been using the Internet?**

□1 Less than 6 months
□2 Between 6 months and 1 year
□3 More than 1 year, but less than 3 years
□4 More than 3 years, but less than 5 years
□5 More than 5 years

3. **Compared to a year ago, has your use of the Internet changed?**

□1 No change
□2 Increase in use
□3 Decrease in use

4. **If your use has changed, please explain why in a few words (e.g., training, equipment problems, frustration)**

____

5. **What was the** primary **method that you used to learn to use the Internet?**

□1 I taught myself by exploring it on my own
□2 I read books on how to use the Internet
□3 I attended a class
□4 I learned from a friend or family member
□5 I used an online tutorial
□6 I used a CD or videotape
□7 Other ways (please specify below): ________________________
□8 ------ *None of the Above* --------

6. **Please specify the frequency with which you have performed each of the following activities using the Internet in the past year.**

	Never used1	Used once2	Used occasionally3	Used frequently4
1. Banking/Money management (e.g., pay bills online, buy or sell stocks)				
2. Communication (e.g., e-mail, instant messaging)				
3. Community information (e.g., find information about community events or religious services)				
4. Education (e.g., participate in on-line degree or training program, search for information about educational courses or materials, use instructional/training software)				
5. Employment (e.g., post resume or search for information about employment)				
6. Entertainment (e.g., purchase tickets for cultural or entertainment events, find information about TV or radio shows, cultural or entertainment events, or information related to hobbies)				
7. Government and official issues (e.g., access a government website to download standard forms or find out information about benefits and programs)				
8. Health information (e.g., find information about an				

	Never used$_1$	Used once$_2$	Used occasionally$_3$	Used frequently$_4$
illness or order medication or health product)				
9. News information (e.g., find information about the weather, read the newspaper)				
10. Shopping (e.g., purchase clothes, search for information about a product)				
11. Travel (e.g., make airline, train, hotel, or rental car reservations, search for maps, travel information)				

APPENDIX D

FINAL CODING SCHEME FOR ARCHIVAL ANALYSIS OF FOCUS GROUP DATA

Category	Sub-Category	Description and/or Example
Avoidance		Behaviors designed to avoid a situation where privacy could become a concern
	Avoid listening	“Turn a deaf ear and forget about it.”
	Avoid using device/system	Avoid using a system because of privacy-invasive features
	Censor self	“you’re not going to scratch your butt in front of the camera.”
	Hiding	
	Selective Sharing	Content or recipient restriction
Modification		Behaviors designed to alter a situation because of privacy concerns
	Be careful	“the wisest thing is be careful”
	Alter for audience	“you can fix how they’re responding or reacting to whatever it is you’re saying”
	Be vague	“being vague” or “be general about it”
	Not in front of others	“I definitely like went like out in the hallway”
	Quietly	“whisper it in their ear”
	Use code or different language	“We’ll switch to Spanish.”
Alleviatory		Behaviors designed to reduce the consequences of information that has already been disclosed
	Ask to remove (external)	asking a person to remove information about the participant
	Ask not to share (external(	Asking a person not to share information about the participant
	Check	“you have to make sure you check them all the time”
	Destruction of evidence	“Burn them”
	Limit Distribution	After information has been collected, reducing further spread of information

REFERENCES

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). *Privacy in e-commerce: Examining user scenarios and privacy preferences*. Paper presented at the Proceedings of the 1st ACM conference on Electronic commerce.

Ackerman, M., & Mainwaring, S. (2005). Privacy issues and human-computer interaction. In S. Garfinkel & L. Cranor (Eds.), *Security and Usability: Designing Secure Systems That People Can Use* (pp. 381–400). Sebastopol, CA: O'Reilly.

Acquisti, A. & Gross, R. (2009). Predicting social security numbers from public data. *Proceedings of the National Academy of Science,* 10975-10980.

Acquisti, A., Friedman, A., & Telang., R. (2006). *Is there a cost to privacy beaches? An event study.* Paper presented at the Proceedings of the International Conference of Information Systems (ICIS).

Adams, A. (1999). *Users' perception of privacy in multimedia communication*. Paper presented at the CHI '99 extended abstracts on Human factors in computing systems.

Ahern, S., Eckles, D., Good, N. S., King, S., Naaman, M., & Nair, R. (2007). *Over-exposed?: Privacy patterns and considerations in online and mobile photo sharing*. Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems.

Altman, I. (1975). *The Environment and Social Behavior : Privacy, Personal Space, Territory, Crowding*. Monterey, Calif. :: Brooks/-Cole Pub. Co.,.

Altman, I., & Chemers, M. (1980). *Culture and Environment*. Monterey, CA: Brooks/Cole.

Altman, I., Vinsel, A., & Brown, B. B. (1981). Dialectic conceptions in social psychology: An application to social penetration and privacy regulation. *Advances in Experimental Social Pscyhology, 14*, 107-160.

Bakken, D., Parameswaran, R., Blough, D., Palmer, T., & Franz, A. (2004). Data Obfuscation: Providing Anonymity and Desensitization of Usable Data Sets. *IEEE Security and Privacy, 2*, 34-41.

Berscheid, E. (1977). Privacy: A hidden variable in experimental social psychology. *Journal of Social Issues, 33*(3), 85-101.

Boyle, M. (2005). Privacy in video media spaces.

Burgoon, J. (1982). Privacy and communication. *Communication Yearbook, 6*, 206–249.

Butz, A., Beshers, C., & Feiner, S. (1998). *Of vampire mirrors and privacy lamps: Privacy management in multi-user augmented environments*. Paper presented at the Proceedings of the 11th annual ACM symposium on User interface software and technology.

Caine, K. (2008). Linking Studies of HCI to Psychological Theories of Privacy. Georgia Institute of Technology.

Caine, K. E., Fisk, A. D., & Rogers, W. A. (2007). *Designing Privacy Conscious Aware Homes for Older Adults*

Paper presented at the Annual Conference of the Human Factors and Ergonomics Society.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: Legal and ethical issues. *Journal of Public Policy & Marketing, 19*(1), 7-19.

Consolvo, S., Smith, I. E., Matthews, T., LaMarca, A., Tabert, J., & Powledge, P. (2005). *Location disclosure to social relations: Why, when, & what people want to share*. Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems.

Czaja, S. J., Charness, N., Dijkstra, K., Fisk, A. D., Rogers, W. A., & Sharit, J. (2006a). Demographic and Background Questionnaire. . *CREATE Technical Rep. CREATE-2006-02*,

Czaja, S. J., Charness, N., Dijkstra, K., Fisk, A. D., Rogers, W. A., & Sharit, J. (2006b). Computer and Technology Experience Questionnaire. *CREATE Technical Rep. CREATE-2006-03*,

Czaja, S. J., & Hiltz, S. R. (2005). Digital aids for an aging society. *Commun. ACM, 48*(10), 43-44.

Flanagan, J. C. (1954). The critical incident technique. *Psychological Bulletin, 51*(4), 327-359.

Foddy, W. H. (1984). A critical evaluation of Altman's definition of privacy as a dialectical process. *Journal for the Theory of Social Behaviour, 14*(3), 297-307.

Goffman, E. (1959). *The presentation of self in everyday life.* Garden City, N.Y.,: Doubleday,.

Hawkey, K., & Inkpen, K. M. (2005). *Privacy gradients: Exploring ways to manage incidental information during co-located collaboration*. Paper presented at the CHI '05 extended abstracts on Human factors in computing systems.

Hawkey, K., & Inkpen, K. M. (2006). *Keeping up appearances: Understanding the dimensions of incidental information privacy*. Paper presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems.

Herbsleb, J. D., Atkins, D. L., Boyer, D. G., Handel, M., & Finholt, T. A. (2002). *Introducing instant messaging and chat in the workplace*. Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems: Changing our world, changing ourselves.

Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Commun. ACM, 42*(4), 80-85.

Iachello, G., & Abowd, G. D. (2005). *Privacy and proportionality: Adapting legal evaluation techniques to inform design in ubiquitous computing*. Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems.

Iachello, G., Truong, K. N., Abowd, G. D., Hayes, G. R., & Stevens, M. (2006). *Prototyping and sampling experience to evaluate ubiquitous computing privacy in the real world*. Paper presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems.

Jourard, S. M. (1971). *Self-Disclosure: An Experimental Analysis of the Transparent Self*. New York: John Wiley & Sons, Inc.

Kaasinen, E. (2005). User acceptance of location-aware mobile guides based on seven field studies. *Behaviour & Information Technology, 24*(1), 37-49.

Karat, C.-M., Karat, J., & Brodie, C. (2005). Editorial: Why HCI research in privacy and security is critical now. *International Journal of Human-Computer Studies, 63*(1), 1-4.

Karat, C.-M., Karat, J., Brodie, C., & Feng, J. (2006). *Evaluating interfaces for privacy policy rule authoring*. Paper presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems.

Khalil, A., & Connelly, K. (2006). *Context-aware telephony: Privacy preferences and sharing patterns*. Paper presented at the Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work.

Kieras, D. E., & Bovair, S., (1984). The role of a mental model in learning to operate a device. *Cognitive Science.* 8, 255-273.

Lederer, S., Mankoff, J., & Dey, A. K. (2003). *Who wants to know what when? Privacy preference determinants in ubiquitous computing*. Paper presented at the CHI '03 extended abstracts on Human factors in computing systems.

Leino-Kilpi, H., Valimaki, M., Dassen, T., Gasull, M., Lemonidou, C., Scott, A., et al. (2001). Privacy: A review of the literature. *International Journal of Nursing Studies, 38*(6), 663-671.

Lieberman, E., & Miller, R. C. (2007). Facemail: Showing faces of recipients to prevent misdirected email. Symposium On Usable Privacy and Security (SOUPS) 2007.

Ludford, P. J., Priedhorsky, R., Reily, K., & Terveen, L. (2007). Capturing, sharing, and using local place information. *Proceedings of the SIGCHI conference on Human factors in computing systems*

March, W., & Fleuriot, C. (2006). Girls, technology and privacy: "Is my mother listening?"*Paper presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems.*

Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. *Journal of Social Issues, 59*(2), 411-429.

Marshall, N. J. (1974). Dimensions of privacy preferences. *Multivariate Behavioral Research, 9*(3), 255-271.

Metzger, M. (2004). Privacy, trust, and disclosure: Exploring barriers to electronic commerce. *Journal of Computer-Mediated Communication, 9*(4).

Montgomery, B. M., & Baxter, L. A. (1998). *Dialectical Approaches to Studying Personal Relationships*. Mahwah, New Jersey: Lawrence Erlbaum Associates.

Muller, M. J., Smith, J. G., Shoher, J. Z., & Goldberg, H. (1991). *Privacy, anonymity and interpersonal competition issues identified during participatory design of project management groupware!*

O'Neil, D. (2001). Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review, 19*(1), 17-31.

Olson, J. S., Grudin, J., & Horvitz, E. (2005). A study of preferences for sharing and privacy. *CHI '05 extended abstracts on Human factors in computing systems*.

Paine, C., Joinson, A. N., Buchanan, T., & Reips, U.-D. (2006). *Privacy and self-disclosure online*. Paper presented at the CHI '06 extended abstracts on Human factors in computing systems.

Palen, L., & Dourish, P. (2003). *Unpacking "privacy" for a networked world*. Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems.

Parameswaran, R., & Blough, D. (2005). *A Robust Data Obfuscation Approach for Privacy Preservation of Clustered Data.* Paper presented at the Proceedings of the Workshop on Privacy and Security Aspects of Data Mining.

Patil, S., & Lai, J. (2005). *Who gets to know what when: Configuring privacy permissions in an awareness application*. Paper presented at the Proceedings of the SIGCHI conference on Human factors in computing systems.

Pedersen, D. M. (1979). Dimensions of privacy. *Perceptual and Motor Skills, 48*(3), 1291-1297.

Pedersen, D. M. (1982). Cross-validation of privacy factors. *Perceptual and Motor Skills, 55*(1), 57-58.

Pedersen, D. M. (1996). A factorial comparison of privacy questionnaires. *Social Behavior and Personality, 24*(3), 249-262.

Pedersen, D. M. (1997). Psychological functions of privacy. *Journal of Environmental Psychology, 17*(2), 147-156.

Pedersen, D. M. (1999). Model for types of privacy by privacy functions. *Journal of Environmental Psychology, 19*(4), 397-405.

Petronio, S., & Kovach, S. (1997). Managing privacy boundaries: Health providers' perceptions of resident care in Scottish nursing homes. *Journal of Applied Communication Research, 25*, 115-131.

Petronio, S., & Martin, J. N. (1986). Ramifications of revealing private information: A gender gap. *Journal of Clinical Psychology, 42*(3), 499-506.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*(1), 27-41.

Reason, J. (1990). *Human error*. Caimbridge: Caimbridge University Press.

Schluter, J., Seaton, P., & Chaboyer, W. (2007). Critical incident technique: a user's guide for nurse researchers. *Journal of Advanced Nursing, 61*(1), 107-117.

Sheehan, K. B., & Hoy, M. G. (1999). Flaming, complaining, abstaining: How online users respond to privacy concerns. *Journal of Advertising, 28*(3), 37.

Sims Bainbridge, W. (2003). Privacy and property on the net: Research questions. *Science, 302*(5651), 1686-1687.

Singer, E., von Thurn, D. R., & Miller, E. R. (1995). Confidentiality assurances and response: A quantitative review of the experimental literature. *Public Opinion Quarterly, 59*(1), 66-77.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3).

Sparck-Jones, K. (2003). Privacy: What's different now? *Interdisciplinary Scinece Reviews, 28*, 287-292.

Stewart, D. W., & Shamdasani, P. N. (1990). *Focus Groups: Theory and Practice*.

Sweeney. L. (2002) k-anonymity: A model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 557-570.

Toomin, M., Zhang, X., Fogarty, J. & Landay, J.A. (2009) Access control for shared knowledge. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* ACM Press.

Thede, L. (2008). Informatics: Electronic Personal Health Records: Nursing's Role. *The Online Journal of Issues in Nursing, 14*(1).

Tsai, J., Egelman, S., Cranor, L., & Acquisti, A. (2007). *The effect of online privacy information on purchasing behavior: An experimental study.* Paper presented at the Workshop on the Economics of Information Security (WEIS).

UCLA (2003). *The UCLA Internet Report: Surveying the Digital Future--Year Three*.

VandenBos, G. R. (Ed.). (2007). *APA Dictionary of Psychology*: American Psychological Association.

Want, R., Hopper, A., Falc, V., & Gibbons, J. (1992). The active badge location system. *ACM Trans. Inf. Syst., 10*(1), 91-102.

Warren, S. V., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193-220.

Webb, S. D. (1978). Privacy and psychosomatic stress: An empirical analysis. *Social Behavior and Personality, 6*(2), 227-234.

Westin, A. F. (1967). *Privacy and Freedom*. New York,: Atheneum,.

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 431-453.