USING AUDIENCE-CENTRIC DESIGN AND COMMUNITY FEEDBACK TO MANAGE COMPLEX PRIVACY SETTINGS

by

Jason Watson

A dissertation submitted to the faculty of
The University of North Carolina at Charlotte
in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in
Computing & Information Systems

Charlotte

2014

Approved by:

____

Dr. Heather Lipford

____

Dr. Rick Wash

____

Dr. Celine Latulipe

____

Dr. Mohamed Shehab

____

Dr. Richard Lambert

ABSTRACT

JASON WATSON. Using audience-centric design and community feedback to manage complex privacy settings. (Under the direction of DR. HEATHER LIPFORD)

Today, technology is enabling people to share information on an unprecedented scale. Although much of this information is intended to be shared with a large group of people or even the public, some disclosure is intended for smaller audiences—a subset of a larger group. People may want to limit information visibility because the information is private or sensitive, or they may feel others would not be interested in the content. When people want to selectively share to different audiences, many technologies fail to provide usable mechanisms to manage these more complex sharing situations. In many cases, people lack understanding about which audiences are able to see what items of information. Additionally, the effort to manage audiences and control access to information adds some extra physical and cognitive burden. This research suggests two methods to help people better understand and control sharing. The first examines audience-centric design: using mechanisms that integrate with the primary task and allow sharing to multiple audiences to improve understanding of how information flows to multiple groups of people. The second method examines using community feedback to enhance privacy/sharing default settings thereby lessening the user's configuration burden. This knowledge contributes to existing research by understanding the extent of how users share information to multiple audiences and react to community feedback mechanisms designed to ease configuration burden.

ACKNOWLEDGMENTS

I may be non-traditional in having the opportunity to thank my very supporting wife Jaylyn and my five wonderful children: Addi, Jeffrey, Will, Mira and Roy. They have (literally) cheered me through struggles and the stresses of learning to research. My advisor, Heather is the perfect advisor and I have never witnessed someone so understanding of such a wide range of problems that afflict graduate students. Andrew has worked through every research problem and idea at my side. I have a large and supportive group of family and friends who know how much they mean to me and have been there when needed. Thank you all.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

According to a recent Pew Research Center report, 73% of Internet users over 18 use social media sites [1]. Smart mobile devices have interfaces to upload photographs and status updates from almost anywhere in the world. People desire to share information and have found social media sites enable them to keep in contact with distant friends and family and reconnect with past acquaintances. Accordingly, people post a lot of personal information to these sites—some that is not intended to be seen by everyone. As with real-world social interactions, people want to control how, when and to whom they disclose personal information. However, with online social media sites, disclosure is often to larger audiences and persists for longer durations than disclosure in the physical world. Thus, managing privacy with online social sites can be difficult and complex. Many people desire to share to different social groups, yet struggle to manage privacy and disclosure to these groups because of complex settings with cumbersome control mechanisms [15, 88]. This dissertation seeks to understand how people manage privacy in online social media interaction and if more usable mechanisms can help ease configuration burden.

Privacy management can be characterized as a form of boundary control between restricting interaction and seeking interaction [6]. It is an internal optimizing process

[1] *Social Media Update 2013 (December 30, 2013)* (accessed January 21, 2014); available from http://pewinternet.org/Reports/2013/Social-Media-Update.aspx.

and the theoretical foundations of privacy management are applicable to both real-world and online interactions. People seek to achieve a desired privacy state in both settings. We seek to socialize with others and also desire to adequately control who we share information with. In the physical world, we manage this boundary by thoughtfully considering disclosure based on who is present within the social context. However, with online social interactions, it can be more difficult to determine who and when someone can access disclosed personal information.

Online social media sites enable us to share to various different social groups where time and space are different than disclosure in the physical world. Palen and Dourish suggest managing disclosure with information technology is more difficult because people lack a conceptual framework of how interrelated privacy issues work when technology is present [68]. In real-world social interactions, we can see the social context and control disclosure appropriately. People also understand that information shared in real-world social settings is largely ephemeral. In contrast, online disclosure can persist indefinitely and the temporal constraints are different. These challenges in understanding online social interactions motivate research that seeks to improve appropriate information disclosure in online social media sites.

People's choice to disclose information to others in the physical world is governed by norms based on the social context of the setting. If information stays within the intended social context, contextual integrity is maintained [64]. However, if we choose to disclose personal information to a specific social context and that information permeates to other social groups, contextual integrity is violated. With online social media sites, the social context is not always visible and it is more difficult to understand if information is allowed to flow beyond the intended context. Therefore, it is important for research to examine how users of online social media sites understand if information they intend to be for a specific group is able to flow to other unintended groups of friends. In this work, I describe using audience-centric design and community feedback to help people better understand these information flows and configure complex privacy settings.

1.1 Audience-Centric Design

People naturally have different social groups—family, work friends, school associates, etc. For the purposes of this dissertation, I refer to such groups as audiences. Audiences form an essential part of how we choose to share information. For example, a person discloses information differently in a work setting than at home or with close friends. With online social media sites, people tend to have a large number of friends that often represent many different audiences. As the number of these audiences grows, the complexity of the privacy policy also increases.

Most of the larger online social media sites of today include mechanisms to control filtering of information by audiences. Because of the volume of shared information and large number of audiences, many current mechanisms are difficult to use [88]. As a result, users tend to adopt sharing strategies that might not reflect how they would share with audiences in the real-world. For example, some people decide to reduce sharing by only sharing information that a person considers to be appropriate for a public audience. Ideally, online social media interactions would be similar to sharing in the physical world where a person could mentally map the desired social context to an audience at the moment the person desires to disclose information. To achieve this level of social interaction, the user would need to both understand the information flow and have a usable mechanism to control disclosure.

Configuring sharing settings on online social media sites is considered a secondary task—a task that is auxiliary to the primary focus of the interaction, in this case, socializing [101]. Users sometimes feel overly distracted from the primary task when a secondary task requires too much time or effort. When the secondary task is difficult, users might ignore the task altogether and effectually ignore secondary privacy or security protections [98]. I postulate that integrating the configuration of complex privacy policies with the primary task can increase user understanding and reduce configuration burden. I consider this design technique as *audience-centric design*—using interface mechanisms to allow the user to view or control information disclosure to different audiences.

Audience-centric design integrates sharing configuration closer to the primary task. Many online social media sites allow the user to create audiences and configure privacy policies to control sharing. However, most of these mechanisms are not integrated with the primary task. Recently, Google introduced a new social media site named Google+. Google+ introduces the concept of circles as a way to group friends into different audiences. Circles are a highly visible and prominent feature in the interface and sharing interaction is integrated with these audiences. Thus, Google+ is a good attempt at providing an audience-centric design to control personal information disclosure and may be a good platform to explore how users react to an integrated audience-centric sharing mechanism. In this dissertation, I investigate the effectiveness of different audience-centric design techniques and provide better understanding of their impact on configuring complex privacy settings.

1.2 Community Feedback

Audience-centric design may improve understanding of online disclosure, however, it adds additional burden to create and manage audiences (see Section 3.3), reducing the net effectiveness. Privacy is still a secondary task and people may ignore usable configuration mechanisms if it takes too much time to configure a desired privacy policy. One potential area to reduce configuration time is to provide better default privacy settings. Privacy preferences are subjective and individuals vary widely in how willing they are to share personal information with others. Thus, incorporating usable mechanisms to configure complex privacy settings is a good step but achieving the desired privacy policy may be difficult if the default policy does not closely match the user's preference. The purpose of online social media sites is to share information and many have default privacy settings that are permissive [88]. Permissive privacy settings achieve the goal of increased social interaction, but can lead to privacy breaches. An obvious improvement for better default settings is to provide many different policies that would contain settings that more closely resemble the user's desired policy. Community feedback might be useful in suggesting better default settings and reduce the configuration burden. Community feedback is the process of collecting setting preferences from other members of a community—other online social media users—and using this data to inform another user's settings or decisions. This may provide the user with sharing settings that potentially start in a state closer to their desired sharing preferences.

Today we see many applications of using community feedback. Online shopping sites recommend additional purchases as we add items to our shopping cart. These recommendations are created as suggestions based on what other community members who buy similar items have also purchased. When we purchase books, we see other recommendations that are similarly based on community data. Thus, community feedback is a promising area to help users navigate online. Researchers are exploring if community feedback can be used to also help users with privacy and security decisions.

In real-world social interactions, disclosure is largely governed by social norms. As we mature, we observe how others disclose information in various social contexts. Technology can make it difficult for people to discern the intended social context. As people interact with online social sites, they often are unsure when and who can view their shared information. Community feedback may improve control over disclosure and provide a similar mechanism to real-world social norms. This dissertation contributes understanding of how people react to community feedback with privacy settings in online social sites. Thus, I present findings on how community feedback can be used to reduce users' configuration burden while trying to achieve their desired privacy policies.

1.3 Thesis Statement

> *Audience-centric designs improve user understanding of information flows by enabling the user to selectively share and digest information by using smaller and more manageable audiences. Real-world interactions occur*

more commonly amongst audiences, so audience-centric design improves the user's mental model of who receives shared information. However, managing sharing settings with audience-centric designs can increase the user's configuration burden. Default sharing settings can be enhanced by community feedback to mitigate this additional burden. Audience-centric designs combined with sharing default settings enhanced by community feedback make it easier for users to understand information flows and achieve desired sharing preferences.

1.4 Contributions

This dissertation documents four contributions derived from the thesis statement:

1. Exploration of theoretical privacy research to provide a foundation of how people interact with audiences and how these theories relate to online social interaction. A further exploration into collective behavior theory to connect how this behavior can relate to using community feedback to enhance default sharing settings.

2. Experimental results that demonstrate how audience-centric designs improve user understanding of sharing personal information.

3. Experimental results that provide better understanding of how people react to automated privacy setting changes based on community feedback.

4. Experimental results that demonstrate how community feedback information such as profile item characterizations enhance default privacy settings and help

reduce user burden to configure sharing preferences for online social interaction.

The first contribution represents my attempt to examine the foundations of social science research related to privacy and collective behavior and apply these theories to the information age world. Regarding privacy, other researchers have contributed to this task. For example, Palen and Dourish examined Irwan Altman's privacy theories and suggested new perspectives about privacy in a socio-technical environment [4, 68]. To my knowledge, no one has attempted to relate sociology collective behavior theory to the more modern area of research on social influence and community feedback. In this dissertation, I summarize theoretical principles from collective behavior research and propose using these principles to enhance technology-based social influence processes.

The second contribution presents research intended to explore and test hypotheses about the usefulness of audience-centric design interfaces. My formative research examines how the user reacts to audience oriented views and if the user is able to better understand who is able to see personal information [77]. Here, I present additional research that examines user reaction to several distinct graphical presentations of audience oriented views and discuss the results of this research. I also present research conducted to determine how early adopters of a production online social network system (Google+) formed, used and understood sharing with audience-centric mechanisms.

For the third contribution, I explore how users react to default setting changes. I present study results that provide better understanding of user reactions to privacy settings modified by community feedback. Findings suggest the conditions where users are able to tolerate automated changes to privacy settings. Results also indicate users are more concerned with changes in specific profile items and seem to not equally tolerate changes to different profile items.

The fourth contribution is a study that examines the overall effect of using community feedback to enhance default sharing settings. Users characterize individual profile items differently and this affects how they perceive automated changes. In this study, I gather sharing preferences and profile item characterizations for all items used by a popular online social network site, Facebook. Using this information from a sample representing the community feedback, I segment the sample based on privacy attitude and formulate several canonical privacy policies. I use these canonical policies to evaluate the effectiveness of these enhanced privacy defaults for another sample group. The studies in this dissertation provide a cumulative contribution to the general body of research in the Human-Computer Interaction and Usable Security and Privacy fields.

1.5 Organization

The chapters and sections of this dissertation are organized in a conventional manner. Chapter 2 provides background and related work. Chapters 3, 4 and 5 present the experimental methods, detailed analysis and discussion of the results of individual studies included in this dissertation. I compile and discuss the overall research contribution of the proposed work in Chapter 6.

In Chapter 2, I present the background by starting from early sociological research and relate some of these theories to the current online and digital environments that exist today. The remaining sections of Chapter 2 discuss the large body of past and current research that relates to audience-centric designs and community feedback.

Chapter 3 explores how audience-oriented views help users better understand with whom they share information in the online social network domain. Previous research shows that users do benefit and prefer audience-oriented views [77]. Analysis from the resulting two studies in this chapter indicate users equally prefer both compact and expanded forms of audience-oriented views and some of the additional cognitive and configuration burdens introduced by providing the user with audience-centric mechanisms. In this way, these studies provide pointed motivation for using community feedback as a potential method to mitigate some of these additional burdens.

Chapter 4 presents an exploratory qualitative study designed to evaluate user reactions to automated default settings. These results suggest users can tolerate automated privacy changes under certain conditions. Users also characterize their social network profile items differently when reacting to automated changes. This research is used to inform the final study of this dissertation.

Chapter 5 presents an experimental study that builds on knowledge from Chapter 4. Permissive default privacy settings for social network profile items may not adequately reflect individual privacy attitudes. In this study, I gather user privacy setting preferences along with characterizations that indicate privacy attributes related to profile data items commonly used in online social networks. This information is used to build canonical privacy policies representing distinct privacy attitudes and test how these can be applied as default policies to reduce user burden to configure complex privacy settings.

The concluding Chapter 6 restates the research and details the contributions. Here, I examine the contributions and how they contribute to different research areas within the Human-Computer Interaction field. Additionally, I summarize the entire body of work along with limitations in this dissertation and discuss potential future research questions.

CHAPTER 2: BACKGROUND

This dissertation presents two methods to help users manage complex privacy settings: audience-centric design and community feedback. Here, I present a comprehensive background of research for both methods. The motivation section builds upon motivating factors presented in the introduction chapter. Then, I discuss other related research to my dissertation.

2.1 Motivation

The purpose of privacy settings is to help users control disclosure of personal information. Privacy research and privacy theory help understand how and why people share information. As with much life found in nature, humans are social creatures and people desire to appropriately share information with peers and social groups. In this section, I explain two modern western privacy models and discuss how these relate to privacy settings and sharing preferences. Then, I discuss how these more traditional models are still relevant but controlling online information disclosure is more difficult and harder to understand. I also discuss previous research that explores issues and challenges with online disclosure of personal information. Lastly, I address community feedback and collective behavior theory as motivation for using community data to more individualized privacy settings.

2.1.1 Privacy

> The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire [100] (p. 7).

In classic Latin, privatus was used to describe a person who was not in public office—an ordinary private citizen. Modern conceptions of privacy describe privacy as a process that includes many factors. The most relevant privacy-related research to this dissertation begins at the dawn of the information age. Before 1960, researchers speculated on how the development of the computer might impact privacy [49, 100]. Until this point in history, privacy issues were largely debated in legal and political arenas. In 1967, Westin provided a summation of these political issues and discussed novel impacts on privacy introduced by electronic storage. More importantly, Westin discussed privacy theory in terms of different sized social units and different levels or degrees of privacy related to these units [100].

Westin analyzed individual privacy in terms of four types or states: solitude, intimacy, anonymity and reserve [100]. Each of these states represent an individual's voluntary withdrawal from general society. When a person desires privacy, they ultimately end up in one of the aforementioned states. Solitude represents the most extreme condition where a person is alone and completely free from observation. The state of intimacy occurs when a person is within the setting of a small familiar group and desires that group to be unmolested by outside intruders. Anonymity happens when a person achieves privacy as a result of being part of a very large crowd, making it hard to be recognized. Reserve is more of a psychological state; it is when someone achieves privacy by psychologically removing themselves from others around them.

Westin combines these states of privacy with four functions of privacy: personal autonomy, emotional release, self-evaluation and protected communication [100]. Personal autonomy is a more traditional function of privacy and represents a theory proposed by sociologists such as Goffman who described privacy as protecting an individual's secrets from outside discovery [40]. Emotional release permits people to retract themselves from social settings and norms and relax from those expectations. The self-evaluation function represents the temporary removal from public to plan and meditate about one's role and future plans. Protected or limited communication serves as the function where people can join in small groups and share confidences with trusted friends. The combination of both state and function by Westin redefines privacy as a process that involves both individuals and groups [100].

Irwin Altman extends and elaborates on privacy as a process [4, 5, 6]. Specifically, Altman defines privacy as "an interpersonal boundary-control process." The process is dialectic—a state of tension or opposition between two interacting forces—which involves a force resisting interaction in opposition to a force seeking interaction. This dichotic tension creates an optimizing process where an individual seeks to regulate the gap between desired privacy and the actual achieved privacy. Altman describes this balance as:

> Desired privacy is a subjective statement of an ideal level of interaction with others . . . Achieved privacy is the actual degree of contact that results from interaction with others. If the desired privacy is equal to the

> achieved privacy, an optimum state of privacy exists. If achieved privacy is lower or higher than desired privacy—too much or too little contact—a state of imbalance exists [4] (pp. 10-11).

Altman proposes that this boundary regulation in order to achieve privacy goals is controlled by behavioral mechanisms. These behavior mechanisms are: verbal and nonverbal behavior, personal space, territory and cultural mechanisms. Verbal and nonverbal behavior obviously represent our communications we use to achieve desired privacy. Personal space is how we use the immediate space around us for both individual and group privacy. People use territory or possession of objects and area as another behavior mechanism. Lastly, cultural mechanisms represent customs or social norms within a culture to regulate contact and sharing with others [4]. Nonverbal behavior, personal space and territory are all behavior mechanisms that are inseparably connected to the physical environment. Thus, Altman's theory is useful in describing the privacy process in a physical space, but lacks somewhat to provide a theoretical framework for privacy in online social communities.

2.1.2 Online Disclosure

Although Humprey [49] and Westin [100] discuss privacy in regards to computer information, online social interactions did not exist until decades later. Altman's [5] work stems from social science and also predates online social communities. Affordable consumer video cameras introduced video conferencing and vaulted socializing and collaboration into a technology domain. In this domain, research highlights some differences between socializing with and without technology [37]. Gaver contrasts the affordances—properties of the environment that offer actions—that exist in media spaces with those that exist situated in the physical environment. Socializing and collaborating with technology does not always imply fewer affordances. For example, the lack of physical presence may provoke people to share more when using technology. Parks and Floyd found that people report disclosing more personal information when using the Internet compared to their disclosure in the physical world [69]. Therefore, regardless of how technology changes social interactions, new and different affordances should be considered [37].

Technology introduces new features that make managing privacy different than the way we do in the physical world. In response to this, people begin to establish new management practices and social protocols [36, 67]. For example, Palen found that users of a groupware calendaring system would create new social mechanisms to manage privacy. Because the company norm was to maintain an open calendar, users would add personal appointments with cryptic names. Some would just simply omit personal appointments from their calendars [67]. These examples indicate that people struggle to properly manage disclosure when technology is used as the sharing platform. Grudin suggests such behavior reflects an awareness at a level more fundamental than privacy and describes this as, "the steady erosion of clearly situated action [45]." The erosion of situated action suggests that people are losing control and knowledge of the consequences of sharing with technology because of how anything recorded digitally can be seen at the present as well as in the future [45].

Palen and Dourish describe some differences between how we manage privacy with technology and the physical world [68]. They build upon Altman's privacy theory [4, 5, 6] and elaborate on issues surrounding three differences between the physical world and the online world:

> 1. Audiences are no longer circumscribed by physical space; they can be large, unknown and distant.
> 2. ...the recordability and subsequent persistence of information, especially that which was once ephemeral, means that audiences can exists not only in the present, but in the future as well.
> 3. ...our existence is understood through representations of the information we contribute explicitly and implicitly, within and without our direct control [68] (p. 131).

The difference between sharing in the online world and the physical world disrupts and destabilizes our ability to regulate privacy as a boundary management process. Palen and Dourish identify three boundaries where technology frustrates our privacy management process: the disclosure boundary, the identity boundary and temporal boundaries [68].

The disclosure boundary is the dialectic tension between privacy and publicity [68]. In an online environment, our choice to share is not always a deliberate act at a specific period in time. For example, an online search can reveal personal information posted years ago and represents an intention to share at that time, but possibly not at the time when the search was initiated. As online social media sites mature, this problem may become more problematic. This example illustrates a lack of control within the disclosure boundary. People may choose to share at the moment information is posted, however, people may not understand consenting to share at any time in an unknown future. Nissenbaum suggests the disclosure boundary is governed by contextual norms and disclosure is regulated based on the appropriateness of the audience [64]. She further suggests people's attitudes of privacy violations "concur more systematically with breaches of contextual integrity than with breaches of only intimate or sensitive realms [64]."

Identity boundary is the tension between self and other [68]. People choose disclosure and behavior based on their social setting and according to what audience is present. Therefore, it is imperative that the audiences—whether large or small—are known to the person to be able to choose how and what information to share. Technology can make this unclear. The decision to share is made while peering into a computer screen and interacting with the interface of some website and it becomes difficult to mentally model all of the different types of audiences that will potentially view the disclosed information. In other words, as the choice to disclose information is related to the social context, if the social context is difficult to determine, privacy decisions will be more difficult to make as well. Thus, breaches of contextual integrity are more likely to occur when technology obfuscates the social context and people struggle to understand the intended audience [64].

Specific decisions to share online should not be considered isolated from other decisions to share. The inability to see the entire sequence of sharing events represent temporal boundaries [68]. Decisions to share and what to share are likely formed from the dynamic process of regulating other boundaries in the past. Palen and Dourish do not consider the technology effects on these temporal boundaries as limiting, but rather an essential role in the ongoing management of online privacy. However, not being able to always determine the complete sequence of sharing decisions can be destabilizing to online privacy management [68].

Although managing online privacy can be difficult, users still desire to appropriately share information. boyd [*sic*] and Ellison find that social network site users are concerned about whether shared content is suitable for all audiences that are able to view the information [15]. Additionally, they find users are concerned with contacts from different contexts being able to reach out and interact with one another as a result of the shared social connection [15]. Users of online social media sites want to adequately manage privacy boundaries and they show some understanding of sharing consequences of unintended disclosure.

Privacy theory as describe by Westin and Altman are equally relevant to both physical and online disclosure. Privacy boundaries remain intact when sharing information online. Technology simply introduces new and different challenges to managing disclosure boundaries. The solution to overcome these new challenges is non-trivial and needs more research to completely understand ways to improve online privacy management. Many online media sites provide privacy mechanisms to manage disclosure and some provide adequate and granular privacy control. However, people are sharing a lot of personal information with many different social groups and increasing the complexity of privacy management. Most current mechanisms are difficult to use and people struggle to manage such complex privacy settings. Because online information is often collected without the user's knowledge or consent [51] with no way to determine if the information was intended to be made public, it is important to research unintended disclosure of personal information. In the next section, I discuss some additional research problems related to complex privacy settings.

2.1.3 Complex Settings

Users of online social media sites develop various distinct social groups and desire to share appropriately to each of these groups [15]. Managing these groups requires user effort to form and manage access control. Research shows that managing these groups can be a significant burden on the user, especially as the number of contacts and relationship types grow to include multiple social circles [29, 46, 56].

Research suggests that privacy mechanisms used by online social sites are difficult to use and understand [89, 88]. Some sites provide separate configuration mechanisms, however making a privacy or security task explicit can be problematic and the design goal is to reduce privacy violations without significant user effort [2]. Many current privacy mechanisms fail to achieve this goal and users under-utilize configuration features and risk privacy violations [3, 88]. Thus, users exhibit a strong desire for privacy management, but seem to struggle to achieve desired privacy when settings mechanisms are complex and difficult to use.

As online media systems mature, larger percentages of users are reporting modifying default privacy settings. The shift in reported behavior appears in research published in the last five years. Strater and Lipford observe users report only initially modifying privacy settings and then only changing settings when privacy violations occur [89, 88]. More recent research shows users are more concerned and a larger percentage report actively managing privacy settings in online social media sites [16].

All of the previously mentioned research focuses on users' reported behavior and may not reflect actual disclosure. A study of more than 4,000 university student profiles shows a high rate of *actual* disclosure of personal information in Facebook [44]. Research also shows that users have a tendency to report being privacy conscious and acting accordingly only when privacy configuration does not interfere with the primary task [87]. It appears that users want to share appropriately online and will manage privacy settings, however the mechanisms need to be sufficiently usable to avoid excessive configuration burden.

2.1.4 Community Feedback and Collective Behavior

Community feedback provides community information to other people or processes. In the physical world, people often use community feedback to make decisions. For example, if a person sees two restaurants together and one has a crowded parking lot and the other an empty lot, she might consider that information as community feedback about the quality of the food. Online shopping sites use community feedback to provide purchasing recommendations by displaying what items others have looked at or previously purchased. In this section, I provide community feedback and collective behavior theory as motivation for generating better default privacy settings using community data.

Using community feedback is not without certain drawbacks. As it sometimes happens in the real world, the community consensus does not always represent a better decision. When people accept community decisions and ignore their own preference, this is know as an informational cascade [11]. Because the decision made is based on existing community information, no additional personal preferences are introduced into the community resulting in more homogeneity of decisions within the community. Herding is a specific type of informational cascade where community members make incorrect decisions that are used as feedback and cause others to make the same decision [38]. It should be noted that both of these drawbacks depend on people being presented with community feedback. If community data is used to only generate feedback for default settings, the overall impact of informational cascades may be reduced.

Gaming is another drawback of community feedback systems. This phenomenon occurs when someone injects enough preference information into the community data to manipulate community feedback recommendations. Gaming exploits are possible in any community feedback scenario and must be considered when providing community based suggestions. These drawbacks are important challenges to community feedback research. In the next section, I present a high-level conceptual view of a community feedback process model designed to enhance how community feedback is used for default privacy settings.

Social navigation is the process of using community information to help people make hard decisions by providing suggestions based on other people's decisions. Community feedback and social navigation research solutions focus on using a *snapshot* of the community data to provide a recommendation at the moment a user needs to make a decision. Yet, the known problems with community feedback such as informational cascades and gaming are related to the *behavior* of the community. I consider this as a dimensional disconnect that limits current solutions from being able to adequately mitigate community feedback problems. Solutions that are drawn from a single state of community data are one dimensional, however, problems such as herding and gaming include the current state of community data *and* a second temporal dimension. Collective behavior theory as I present here also exists with these two dimensions. Some collective behavior theoretical concepts are related to the current state of the collective and some are related to a second dimension that can only be calculated or detected by examining the change of the collective state over time. I believe the next evolution of community feedback research should focus on both the state of the community data and how the community data has changed over time. This concept may be somewhat novel to the field of community feedback, however data mining and economic models historically and extensively use similar techniques to examine trend information. Additionally, I believe early social navigation theorists intended the process to include information about collective behavior and not just data extracted from the current state of the community as Dieberger et al describe:

> Social navigation, in the sense of our individual actions being designed around *collective social behavior*, is not just something that is 'layered on top of' a space, but comes to transform both the space and the ways that people act within it [27] (p. 39 - emphasis added).

Collective behavior theory in social science refers to the behavior of a group of individuals. The theory seeks to understand the determinants of significant events that generate social collective action. These events, known as collective episodes, can be a spectrum of events such as rumors, crazes, panics or even revolutions. Early social research explains these episodes as spontaneous and fickle, however, Neil Smelser suggests collective behavior is surprising but occurs with regularity [85]. Thus, the aim of collective behavior theory is to understand and explain how and why collective episodes occur.

The components of social action are key to understanding the determinants of collective episodes. In sociology, these core theoretical concepts are used to analyze conventional human behavior. Conventional or individual social behavior is analyzed by these same theoretical constructs because both conventional and collective behavior is governed by social life. Smelser describes these components as: values, norms, mobilization into organized roles and situational facilities [85]. Values are the most general component of social action and do not specify any kind of norm or action. For example, belief in democracy represents a social value. There may be many methods and political systems that represent the value of democracy, but they are all democratic. Norms are rules that enable actions that reflect values. In our democracy example, norms are the rules for elections or what rights and privileges are afforded to citizens that reside under a certain democracy. Values and norms themselves do not determine the organized form of human action. Mobilization into organized action describes how society is grouped and organized. These groups can be social, political or economical and exist to execute societal actions. Situational facilities are means or obstacles that affect how organizations achieve their goals. With democracy, a constitution is a means to operating a democratic system whereas political corruption is an obstacle to democracy. The components of social action provide the foundation to understanding social structural strain and how collective episodes are formed.

Social research suggests ways to classify collective groups, or collectivities. Roger Brown suggests four dimensions used for classifying collectivities: size, frequency of congregation, frequency of polarization of group attention and degree of permanence of group members [18]. Size describes whether the group could fit in a room or even whether it is too large to congregate. The frequency of congregation denotes how often or if the group physically congregates. The frequency of polarization of group attention describes how often the group divides its focus on desired goals. The permanency of group members labels a member's status within the collectivity. Brown uses these classifications to identify and distinguish collective behavior from other forms of social behavior [18].

Within collective behavior, Herbert Blumer suggests two major foci of interest: the study of the forms of collective behavior and the study of how these forms develop into organized behavior. Blumer illustrates how normal collective behavior transitions into organized collective behavior and describes this as a social movement [12]. Smelser suggests using a set of determinants to describe whether a collective episode will occur. The first two determinants describe structural characteristics of a collectivity: (1) structural conduciveness and (2) structural strain. Conduciveness and strain together provide a state of how likely a collective episode is to occur within a collective body. The next determinant is (3) growth and spread of a general belief. Members of the collective generate beliefs or actions that serve as the source of structural strain. The spread of a general belief to cause structural strain is not likely to cause a collective episode without (4) precipitating factors. These are specific factors that set a collective episode in motion. However, precipitating factors alone do not determine the existence of a collective episode. Once an episode occurs, there is a (5) mobilization of action that marks the onset point of the collective episode. Finally, there is an (6) operation of social control which represents counter-determinants that prevent or interrupt the collective episode. The operation of social control has the effect of removing precipitating factors and reducing structural strain [85].

Collective behavior provides a theoretical framework that motivates using community feedback to provide privacy settings that are closer to user attitudes. The collective unit becomes available as a better resource to represent user preference. Online social network sites have access to how people interact with privacy settings. This behavior can represent the social movement described by Blumer and as this movement changes over time, collective episodes that represent privacy attitudes are formed and Smelser's determinants can be detected. As attitudes of similar groups within the community change, the collective behavior can be used to inform other privacy settings with an automated system. This theoretical framework provides many ideas for better understanding of how community information can be used to help reduce burden for configuring complex settings. For example, research needs to determine what community privacy behaviors represent a structural strain and what data might represent the precipitating factors that lead to a collective episode. When a privacy change is determined by a collective episode, how will the user react to the privacy change? My research is motivated specifically by two areas within this framework. First, Chapter 4 explores user reactions to privacy setting changes based on feedback from a collective episode, or an automated system that recommends the change. Second, Chapter 5 explores gathering more information about audience disclosure preferences that can be representative of Smelser's precipitating factors within a collectivity. I explore how this factor determines collective episodes (recommended privacy policy changes) and if they can be used to generate enhanced privacy settings—settings that are changed to better match the user's privacy attitude.

2.2 Related Work

Researchers of privacy in online communities are motivated to help online social site users lessen the gap between their desired privacy and achieved privacy. Making complex settings more usable provides a steady source of research questions and associated experiments. In its abstracted form, managing what information is shared with whom is an access control problem. In this section, I present related usability research done in the access control area, both with security and privacy problems. Next, I discuss similar privacy research done in the specific domain of online communities. I then discuss research related to enhancing management of complex settings with audience-centric designs. This dissertation includes using both audience-centric design and community feedback to help users understand and configure complex settings. Therefore, I finish with related research with community feedback and social navigation.

2.2.1 Usable Security and Access Control

Simplified, managing online information disclosure is a form of access control. Objects represent items of personal information and boundary management represents the individual decisions to grant or deny access to external parties. As previously discussed, managing access becomes more difficult as the number of objects and external parties increase. In usable security, access control research is related to easing the burden of managing complex privacy policies.

Access control has been a research problem from the beginnings of sharing computer systems and digital information [79]. Abadi et al. provide a formalized approach to managing access control [1] and Carminati et al. [21] formalize a comprehensive access control mechanism for web-based social networks. These formal approaches show that work is being done to develop actual control mechanisms, however, traditional access control models often neglect usability concerns. Access control models vary and are usually distinguished by who controls access. Previous models include Mandatory Access Control (MAC) and Discretionary Access Control (DAC) [80]. MAC is a more traditional approach where control is enforced by security labels that are attached to users and objects. DAC controls access on the basis of an object owner who establishes the permissions or denials for an object [80]. Thus, privacy decisions in the domain of online social networking can be thought of as a form of DAC—determining who can have access to particular information and under what circumstances access is to be denied.

Role-based access control (RBAC) models are different from MAC and DAC by placing the access control focus on the external parties requesting access [80]. External parties can represent organizational groups or in the case of online media sites, different social groups. With RBAC, the access control system grants or denies access to information by examining a set of rules when an external party makes an access request. RBAC models are related to privacy in social settings by grouping external parties by some defined attribute. Managing privacy in both physical and online social settings relates to discretionary decisions to allow access to certain role-based groups. Thus, discretionary access using a RBAC model is a good fit for access control in online media domains.

Discretionary RBAC systems rely on the user to make the sharing decision. Under most scenarios, this access control decision is a secondary task. Whitten and Tygar show that when the user interface for such tasks are confusing and hard to understand, the user is not able to successfully complete the task [101]. With online social sites, privacy is considered the secondary task and much usable security and privacy research focuses on trying to reduce user interaction and avoid distraction from the primary task. However, completely hiding privacy and security tasks is also problematic when the user needs information. Previously, developers made design decisions on security mechanisms that often obscured necessary information from the user. Doursh and Redmiles suggest the usable security context needs to be highly visible to the user in order for the user to make an informed security decision [32].

One possible usability enhancement is to increase understanding by using graphical interfaces that improve the visibility of the access policy. Zurko et al. designed Adage, an RBAC system for distributed computing systems [105]. Adage implemented both graphical and command-line interfaces to allow a user to configure an access policy. The graphical interface included the "Visual Policy Builder" to help the user create an access policy [105]. The results from a small user study on Adage suggest users preferred using the graphical tool. Cao and Iverson created an Intentional Access Model (IAM). The goal was to improve mental models and understanding of otherwise complex access control lists with intentional statements of actual access to objects. They also implemented an improved visual interface to help understanding of complex access control policies [20].

Other research provides additional visual mechanisms and usability results [73, 96]. For example, Reeder et al. presented the Expandable Grids visual mechanism for managing discretionary file access control with Microsft Windows. Expandable Grids used a matrix with objects on the top axis and groups along the left axis. In each cell, a color of red, yellow or green represented the intuitive level of access granted that each group was allowed to each object. In a lab user study, they compared the new Expandable Grids interface with the existing Microsoft configuration interface. Results of a user study show Expandable Grids performs better and people are significantly more accurate with configuring complex access control tasks and significantly faster completing the tasks with many access control configuration scenarios [73].

Previous research in usable access control attempts to provide easier mechanisms for configuring complex privacy policies. The findings support more visual access control policies are easier for users to understand and configure. These generalized principles can easily be applied to managing online privacy and are included in usable audience-centric design principles. However, this research fails to provide any specific evidence to how these mechanisms will perform if presented to online social communities. In the next section, I discuss research specific to configuring privacy in online social media sites.

2.2.2 Online Privacy

Findings in online usable privacy research intersect with related research in usable access control. Researchers find that the some of the same design principles are applicable to the specific area of online privacy management. Visible interfaces and granular control over settings improve user understanding and lessen configuration burden. These principles provide a good start, however, users still struggle to manage complex privacy settings even when provided with comprehensive and visible mechanisms.

Research suggests users of online social sites desire control but often do not form a complete mental picture of how information flows in online domains. Websites that collect personal information create privacy policies to convey limits of how the organization plans to use collected information. SPARCLE is a tool to help author these policies using a natural language interface [53]. Reeder et al. provide results from a user study with SPARCLE and find users struggle with design challenges with policy authoring, especially when trying to visualize who from multiple groups is allowed access to collected data [74]. Additionally, even when presented with privacy policy interpretation aids, users are not able to understand or achieve desired privacy when disclosing personal information to websites [26, 72].

People seem to understand managing disclosure when configuring privacy to a few articles of information to the public. Joseph Dominic performed a study before the onset of social media sites that analyzed personal web pages [31]. He found only 25% of these pages contained family or other private information [31]. These were early adopters of having a social web presence and likely understood posting a web page was intended to be seen by the public. After the explosion of online social media sites, research findings suggest users desire to group friends and manage privacy at the group level [65, 70]. Dimicco and Millen find privacy control challenges when online social media users maintain self-presentation for professional and non-professional audiences [29]. These findings suggest interacting with different social groups challenge the ability for users to exercise control over personal information as the number of distinct social audiences grow.

Lipford et al. suggest users understand more if information flows are more visible and within the context of the user's sharing behavior [58]. Previously, I collaborated on research to test a prototype AudienceView interface designed to allow users to view Facebook profiles from the perspective of predefined social groups [77]. Results of this study suggest users prefer to visually see their profile data from the audience perspective and they feel more comfortable and in control of their sharing [77]. In Chapter 3, I present research on audience-centric designs that is an extension of this previous work.

It is important to consider both the user's understanding of information disclosure and the user's ability to configure privacy settings. Lederer et al. suggest that common privacy designs "...inhibit peoples' abilities to both *understand* the privacy implications of their use and to conduct socially meaningful *action* through them [57]." Thus, another usability goal for privacy in online social systems is to enhance socially meaningful action by providing usable mechanisms. Some research has been established to explore various interface designs for enhancing privacy configuration in online social interactions. For example, Egleman et al. present a privacy setting mechanism using Venn diagrams representing audiences for configuring Facebook privacy settings. Their findings suggests users struggle to configure privacy settings to different social groups when people exists in multiple groups [33]. Using Venn diagrams improved the user's ability to configure group-based settings, however, Venn diagrams are a limited solution that may not enhance socially meaningful action.

Privacy settings can be more difficult to configure when default settings are overly permissive. The purpose on online social media sites is to provide a distributed mechanism for people to share information with friends, family and acquaintances. People desire to share appropriately with different social groups by controlling disclosure within a sharing context [15]. Many online social media sites provide privacy controls to limit unintended disclosure, however default settings are generally open and permissive [43, 44]. Earlier research suggests social media site users report not modifying privacy setting defaults [43]. Gross et al. actually mined Facebook data and found only a small percentage had changed default settings and restricted information [44]. More recent research finds users are more likely to report modifying default privacy settings [15, 16, 52] and might suggest a change in awareness of privacy attitudes. What seems to be consistent in various forms of online social media is users are concerned with privacy and desire usable privacy control mechanisms [9, 25, 95].

People are using online social sites to share information with various social groups. Many sites provide comprehensive and granular privacy control, however many of the mechanisms are complex and hard to use. Previous research suggests design guidelines—providing granular control and visible mechanisms improve understanding and reduce configuration burden. Audience-centric designs provide early evidence of an additional increase in user understanding and comfort with online disclosure.

2.2.3 Community Feedback and Social Navigation

Community feedback is a process of using community data to provide meaningful feedback for others. For usability, this often is using feedback to enhance or make a user interaction process easier. Social navigation describes specifically using community decisions to provide suggestions for others when presented with a task [27]. I consider community feedback to be a more general term that better describes the intentions of my research. Most usability research related to community feedback is specifically focused on social navigation techniques. In this section, I present a brief review of other community feedback examples and then present a detailed review of social navigation in the human-computer interaction research area.

Research related to community feedback dates back to the early 1990s. Goldberg et al. present an electronic document management system call Tapestry [41]. Tapestry uses collaborative filtering to annotate electronic mail and other electronic documents to help others more quickly query and retrieve related material [41]. Hill et al. present early work that suggests using community feedback as a “social strategy” for improving user choices in human-computer interaction [47]. Recommender systems use similar techniques and are present in many electronic commerce sites today [76]. General community feedback research exemplifies a common theme of using the knowledge of a community to enhance decisions and decision-making for other people. Today, there are many applied examples of community feedback. Commercial shopping sites use community feedback to provide smart recommendations of additional items to purchase as items are added to a shopping cart. Online music sites such as Pandora use community feedback to recommend songs and build a listening profile.

Social navigation was termed at the International Conference on Computer-Human Interaction (CHI) in 1999 [27]. Since, social navigation has been extensively studied in a variety of domains [48]. Dieberger et al. originally proposed using social navigation to help users make privacy related decisions in online systems [27]. In usable security and privacy, various researchers have tried to explore how social navigation can help users understand and make more appropriate decisions [28, 38, 39]. For example, configuring a personal firewall can be a difficult task for many home users. They may not have enough security knowledge to know how or when to block network access. When a user is presented with a firewall configuration choice, social navigation provides aggregated information on if other people chose to allow or block the access request. Much of this research only shows a minimal impact in changing user behavior and it is still unclear on how much social navigation affected user decisions. Thus, it is difficult to understand if the theoretical benefits of social navigation actually help users make more informed privacy and security choices.

Goecks et al. discuss some challenges in using social navigation for security and privacy systems [38, 39]. They reflect on lessons learned from the deployment of two social navigation systems: Acumen and Bonfire. Acumen is a browser toolbar that helps users manage website cookies. Website cookies are useful for remembering user preferences and providing customized web interfaces. However, cookies have the capability of storing personal information that can be used to monitor users' browsing activities. As the user browses a website, Acumen controls cookie settings by allowing or blocking cookie creation and provides visible community settings for the website. For example, if a user visits Amazon.com, Acumen will show Amazon.com in the toolbar with a color indicator that represents how the community has handled Amazon.com's cookies. If the color is green, most community users have allowed Amazon to create and store cookies. Yellow is used to show the community is mixed and red indicates most users have blocked cookies from that site. The user can click on the toolbar and see more details about the community choices and then make a decision to block or allow the cookie. Acumen provides community data from mavens—users that are deemed expert by augmented usage—as well as the rest of the community. Results from a limited deployment show Acumen helps users make better decisions. However, many participants reported following the general community decisions against the advice of the mavens. This represents an example of *herding* and is a challenge when presenting community data to help with decision-making.

Home computer security is another domain where research explores social navigation solutions [98, 97]. Bonfire is a personal firewall system that functions similarly to many commercial personal firewalls by providing a user popup alert when a program needs a firewall decision to be made [38]. Bonfire makes use of social tagging to help users understand the function of the application asking for access to the Internet and also provides community feedback in the form of the number of community members that allowed and denied access. If a user is using Bonfire as a personal firewall and the iTunes service needs Internet access, Bonfire shows a dialog with a choice to allow or deny *itunes.exe* access to the Internet. The user would see how others chose to configure the firewall rule for *itunes.exe* and related social tags such as apple, ipod and music. Social tagging helps mitigate negative herding effects by helping inform the user's mental model of the firewall's function. Rick Wash examines user understanding of home security and finds security experts form different mental models of security threats than those of home users [97]. His findings suggest using community contributed free-text comments to help home users make firewall decisions [98]. Previous social firewall research shows promise in using community feedback to improve user understanding of security decisions with technology. User similarly struggle to understand information disclosure and privacy in online social sites.

Facebook users configure application permissions to access profile information when they choose to install an application. Besmer et al. use social navigation cues to help users configure access controls for Facebook social applications [10]. They used an indicator bar on the interface to show how many community members had granted the application access to a particular data item. For an even stronger cue, the whole data item line was highlighted to further emphasize a strong majority of the community had denied access. The results of their study show users are only significantly influenced by very strong visual cues. Shehab et al. deployed a similar mechanism that provided real user data with similar navigation cues but their study did not specifically examine the effectiveness with a control group [82]. Wu and Bowles present some design principles for using social navigation in collaborative systems by helping users manage access control [104]. They propose three core values added by social navigation:

discovery of new features, predicting consequence of actions and decisions based on previous users and conveying cultural context to meet expectations of a collaborative environment [104].

My thesis statement explores using community feedback to enhance default privacy settings. Shehab et al. suggest PolicyMgr, a formalized approach to using machine learning to automate default privacy policy creation. This approach suggests using a subset of trusted friends to provide a community data source for machine learning training [81]. Other research exists that explore canonizing default policies to provide a user default choice in location sharing [71, 78, 93], however, these works are in early stages and do not provide empirical results related to how defaults enhance user configuration. Additionally, I have not found any research that comprehensively explores using community feedback to personalize complex privacy settings for online social media systems.

2.3 Conclusion

Privacy is a boundary regulation process that creates tension between our desire to be private and our desire to be social. People desire to intentionally share with others and be able to control the recipients of the information. When people share using online social sites, technology introduces new challenges that make it more difficult for users to understand disclosure and to adequately configure privacy controls. As more people create and share within many social contexts, online privacy management becomes even more complex. Online social site users desire to group friends and want to share appropriately within these various social contexts, however, complex policies are difficult to configure and most users rarely modify default privacy policies.

In this dissertation, I use audience-centric design and community feedback to help users manage complex privacy policies. Related research demonstrates users prefer visual interfaces to help configure complex policies. Audience-centric design techniques show promise in helping users better understand disclosure in online social sites [77]. I intend to build on this research and find out how users react to configuring privacy with audience-centric configuration mechanisms.

In Chapter 3, I present my research with using audience-centric design to help users configure complex privacy policies. I also discuss a comparison of using an expanded and visual configuration mechanism with a more visually compact configuration mechanism. I then look at a new online social media site that uses audience-centric design techniques and present early adopter impressions of using audiences to control online disclosure.

Community feedback is a process of using peer decisions to provide recommendations on how to configure privacy settings. Related research shows community feedback can improve user's mental understanding of privacy and security decisions. Although community feedback shows some promise, it also suffers from some limitations and pitfalls. In Chapters 4 and 5, I present research that provides better understanding for how community feedback can be used to reduce burden for configuring complex privacy settings.

CHAPTER 3: AUDIENCE-CENTRIC DESIGN

A variety of applications allow people to post and share photos and documents, personal and contact information, relationships with people and organizations, location and activities, and even health status. With many of these applications, users are charged with acting as administrators for their personal information, controlling what gets shared with whom. They must determine appropriate and desired privacy policies for a wide variety of data and contexts.

A popular example of this situation is social network sites. Hundreds of millions of users now use social network sites to communicate with friends and family, strengthen social relationships, and keep in touch with old friends and acquaintances [14, 52]. To accomplish this, users post large amounts of personal data, such as photos, friend lists, activities, relationship status and much more [44]. And users must also manage a potentially large and complicated set of privacy settings for all this information.

A number of policy mechanisms have been proposed to protect people's information in this and other settings. Yet many of the existing and proposed mechanisms rely on explicit input from the user, with little investigation into how users are able to understand and perform policy creation tasks. Policy interfaces can be time consuming and difficult to use and comprehend [73, 88]. As a result, users under-utilize privacy policies, misunderstand the privacy implications of their activities, and are at risk for a variety of privacy or security problems [3, 88].

End users have to make many privacy policy decisions regarding their own information: whether photos are public or private, who has access to a music list, or which friends can subscribe to status updates. In this regard, privacy can be thought of as a process of boundary management [68], where people determine the boundaries between what is private and what is public based on the social situation. Indeed, information sharing is highly governed by the social norms of a given context [63] and privacy problems will arise when information is shared beyond the social expectations of the context. Managing the privacy of one's personal information can be challenging, as users must decide a priori how to create policies that reflect the perceived future contexts for that information. Users tend to underestimate the size of their audience [3, 88], or misunderstand the information flows and implications of privacy settings, resulting in information being shared out of the intended social context.

In security terms, privacy decisions can be thought of as discretionary access control—determining who can have access to particular information and in what circumstances. Many researchers in the information security and privacy community are examining access control mech anisms to allow users to protect their information on social network sites and other collaborative and social applications (e.g. [21, 22, 94]). Yet many access control mechanisms still rely on an end user to determine the policies. Thus, understanding user-policy interaction is critical to creating end-user access control mechanisms that really work.

The related research reveals the importance of the audience in users' perceptions of their information sharing. In real world interactions, users present different facets of their identity to different audiences. Online, users attempt this same identity management task by tailoring their information for various and broad audiences [14]. Users' awareness of the broad audience of their information does initially influence them during their profile creation as they explicitly decide what they were comfortable sharing publicly. However, that awareness is reduced in day-to-day interactions with friends. Users often did not think through the consequences of their regular activities until reminded of the various audiences of their information, such as after unwanted messages from strangers [88]. Thus, I propose to improve privacy management by structuring privacy settings around the notion of the audience to help users better conceptualize the impact of information sharing and protection, enabling them to more accurately construct appropriate privacy policies for their information.

This chapter presents a series of three research studies to examine how audience-centric design impacts the user. The first study compares AudienceView—a prototype audience-centric privacy setting interface—to the current privacy setting interface used by Facebook. In the second study, AudienceView is compared with a more compact policy configuration interface: Expandable Grids [73]. The third study examines early adopters of a new social networking site introduced by Google that employs an audience-centric design for controlling information flows.

3.1 AudienceView

Much privacy related work has focused on the particular social network site of Facebook. Facebook profiles include many disclosure categories and in order to create a descriptive and accurate impression on viewers, users often respond honestly and complete the majority of disclosure categories [43]. Facebook also offers extensive privacy controls to manage all profile information. A number of studies have examined Facebook to demonstrate the wide-scale disclosures of personal information such as dorm rooms and phone numbers, and the general lack of alteration of the default and permissive privacy settings [3, 44].

Strater and Lipford interviewed 18 undergraduate students about their use of Facebook and privacy concerns and management [88]. They learned that users do have privacy concerns, but often struggle with privacy management and can accidentally and unintentionally disclose personal information. Another problem is the usability of the current privacy settings; users reported that the privacy interface was confusing and time consuming [88]. Additionally, the current interface has limited visual feedback, confusing language, and promotes a poor mental model of how the settings affect the profile. Even after modifying settings, users can experience difficulty in ensuring that their settings match the actual desired outcome.

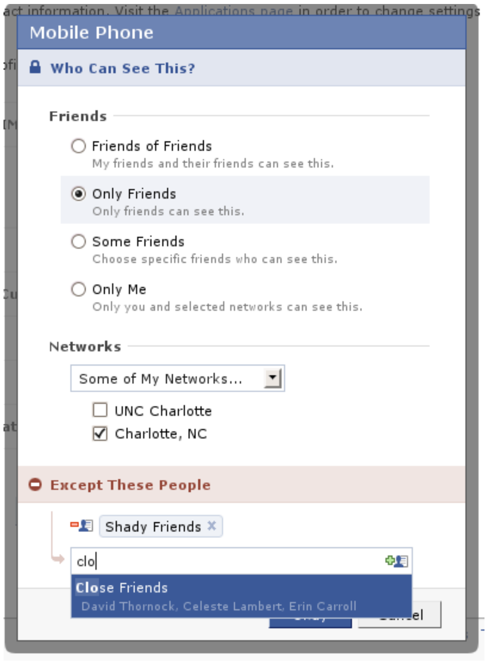
Based on this formative research, Richter et al. a created simplified prototype that visualized the outcome of privacy settings from the point of view of different audiences on Facebook [77]. They performed a pilot evaluation, asking users to answer questions about who could see what information based on Facebook's privacy settings and our prototype. The results showed that the visual feedback of the prototype improved users' understanding and confidence. The study also showed how Facebook users can misunderstand settings and feel confident that information is protected when it actually is not. Overall, this study demonstrated that visualizing privacy settings as audience views have potential to improve usability. Yet, the prototype was simplified with only three audiences, and did not provide any mechanisms for actually modifying settings. Thus, while this work introduced the concept of an audience view, it did not explore at all the benefits and tradeoffs in actually creating and modifying privacy policies using such an interface.

In this section, I present a more functional AudienceView prototype and a complete user study to more fully understand the impact and potential of this audience-centric design. This study examines both understanding and modifying privacy settings. I also examine a more real-world scenario, where users have a larger number of audiences that they need to maintain.

3.1.1 Interface and Mechanisms

This study compares the AudienceView prototype against the current Facebook interface. While Facebook has similar mechanisms to other sites for modifying a privacy policy, the site has a wider variety of disclosure categories and more privacy controls than many other social network sites. Facebook users can control the visibility of most profile information, determining whether to restrict information to friends or certain communities of users. Previous versions of Facebook structured information sharing around the notion of a network—the community, such as school, workplace, or city, to which a user belongs. Users can also define lists of friends, such as "colleagues" or "family", to further customize information sharing to those groups.

For each of set of information, users can choose to share information with all friends and networks, friends of friends, just friends, or to further customize the access by allowing or limiting individual friends or groups of friends, see Figure 1. In this way, users could choose to share their phone number with just close friends, share a photo



act information. Visit the Applications page in order to change settings

Mobile Phone

Who Can See This?

Friends

○ Friends of Friends
My friends and their friends can see this.

● Only Friends
Only friends can see this.

○ Some Friends
Choose specific friends who can see this.

○ Only Me
Only you and selected networks can see this.

Networks

Some of My Networks...

□ UNC Charlotte
☑ Charlotte, NC

Except These People

Shady Friends ×

clo

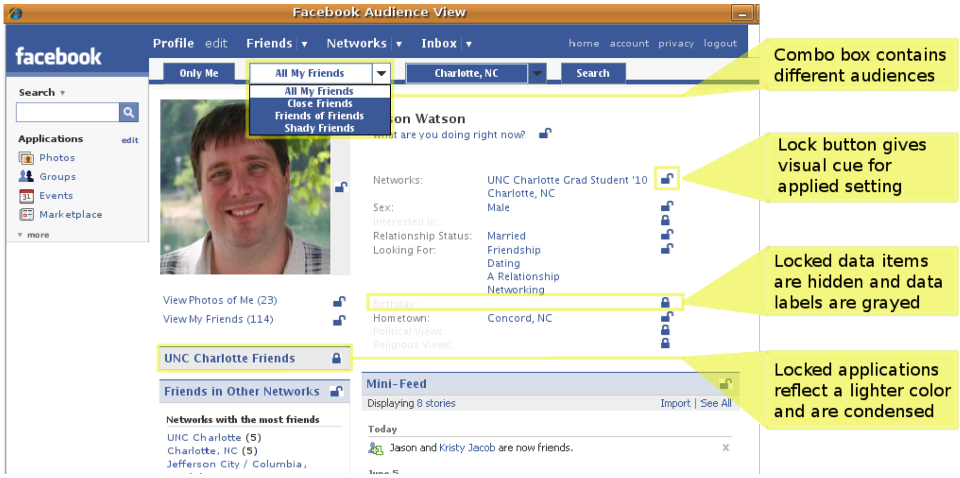
Close Friends
David Thornock, Celeste Lambert, Erin Carroll

Figure 1: Facebook's privacy settings interface.

album with friends but restrict it from work colleagues, and share their education and work information with everyone.

To address some of the shortcomings in Facebook and other sites, I propose to structure the privacy policy interface as the information that a particular audience—search, network, friend, or self—can see. Doing so will help the user associate privacy settings with how profile information is presented to different people, instead of with lists of privacy menus. In AudienceView, a series of tabbed panes presents specific views of the user's profile for different audiences, as well as controls for showing or hiding information to that group. Thus, the interface naturally provides visual feedback as to the effect of modifying privacy settings, along with an accurate mental model of what information is shared with whom.

A screenshot of the prototype is shown in Figure 2. The tabs represent audience



on Watson
What are you doing right now?

Networks: UNC Charlotte Grad Student '10, Charlotte, NC
Sex: Male
Interested In:
Relationship Status: Married
Looking For: Friendship, Dating, A Relationship, Networking
Birthday:
Hometown: Concord, NC
Political Views:
Religious Views:

Networks with the most friends
UNC Charlotte (5)
Charlotte, NC (5)
Jefferson City / Columbia,

Jason and Kristy Jacob are now friends.

Combo box contains different audiences

Lock button gives visual cue for applied setting

Locked data items are hidden and data labels are grayed

Locked applications reflect a lighter color and are condensed

Figure 2: AudienceView prototype resembling Facebook's profile information and layout.

categories—self, friend, network, and search. The chosen audiences reflect Facebook's model at the time of the study, but could easily be altered to reflect the audiences of any particular site. A combination box for each category expands downward to reveal configured friend lists or joined networks. For each category, a representation of the user's profile is shown, along with lock buttons for showing or hiding information to that audience. When an information field is locked, the field title is grayed out and the information hidden.

Within AudienceView, it is also possible for the user to protect categories of information. Locking categories grays out the title bar of the information box and the entire box is collapsed. This simple visual feedback gives the user a more visually accurate representation of how the audience would see the profile data, while still indicating the information is protected. The "Search" tab is a bit different, and instead shows the compact profile information boxes as they would appear in different group's search results. Users can then show or hide the information on those boxes, or hide themselves entirely from that audience.

Currently, the prototype also provides settings for consolidated audiences: "All My Friends" and "All My Networks." This provides the user an easy mechanism to configure settings for all friends or networks without having to configure each individual friend list or network. As the user applies settings in these categories, the setting is propagated to all individual audiences within the group. After applying such a setting, users are still able to visit a specific friend group or network and override any propagated setting. For example, Bob can choose to hide his address from all friends by locking that field on the "All My Friends" audience page, but then go to "Close Friends" and allow them to see his address.

3.1.2 Methods

This study compared the prototype AudienceView interface against the existing privacy settings interface in Facebook. Two profiles were used during this study which were controlled and populated with a variety of profile data and settings and replicated in both interfaces. During the study sessions, participants configured privacy settings for the actual profiles on Facebook and within the prototype AudienceView application.

I recruited students and staff at our university through word of mouth and soliciting volunteers in several courses. I sought both experienced Facebook users, and those with little or no familiarity with Facebook. Because I recruited both experienced and novice users, I discussed the concepts of Facebook networks, friends, and friend lists with all participants to ensure some understanding of Facebook audiences. For each interface, I also provided a short overview of the setting locations and allowed the participants additional time to further examine the interface, if desired.

The participants performed the same 10 tasks for each interface. Both profiles and interfaces were counterbalanced. I asked participants to not configure settings for both task one and two, but to examine the current profile state and determine what privacy settings were applied. I considered these warm up tasks to provide users with additional time to become familiar with the interfaces. For the remaining eight tasks, I asked the participants to modify the privacy settings to show or hide particular information from audiences. For each task, I also asked users how confident they were in their actions on a seven point Likert scale.

It should be noted that it might be faster and easier to configure settings for a particular interface based on the design of the question. For example, if a person is asked to configure five items of profile data for one particular audience, such as hiding several pieces of contact information from work colleagues, this might be more easily configured using the AudienceView interface because settings are grouped by audience on one page. Alternatively, if a person is asked to configure one piece of data for multiple audiences, such as sharing an email address with close friends and family but no one else, Facebook's setting mechanism appears faster. To examine the effects of these interface biases, I presented tasks designed in both ways. From the eight configuration-type tasks, I asked five users to configure the privacy of one data item for multiple audiences. Two questions required the participant to configure multiple items for only one audience. For the seventh task, I asked participants to configure multiple search items for multiple audiences.

My thesis is that audience-centric designs improve visual feedback and provide the user with a better mental model of privacy settings and their outcomes. Therefore, I formed several hypotheses prior to the study:

- Hypothesis 1. Users will more accurately configure privacy settings using AudienceView than Facebook.
- Hypothesis 2. Users will have higher confidence in their task completion in AudienceView than Facebook.
- Hypothesis 3. Users will configure privacy settings faster using AudienceView than Facebook.

I also expected that experienced Facebook users would be more familiar with the Facebook interface and already have a better mental model than the novices. Thus, I expected that AudienceView would provide even greater improvements for novice users than for experts. Consequently, final hypothesis for this study is:

- Hypothesis 4. Novice users will experience bigger improvements in speed, accuracy, and confidence with AudienceView.

I audio and video recorded all of the participant sessions. Additionally, I utilized usability software to record mouse events and capture the screen. I used the audio and videos to analyze the time and accuracy of the participants completing the tasks.

3.1.3 Results

I recruited 28 participants for the study. Facebook's site was experiencing slowness and timeouts during the second participant's session, so we could not gather valid

Table 1: Comparison of Facebook and AudienceView performance.

	Average Accuracy		**Average Reported Confidence**		**Average Duration (Seconds)**	
Task	**Facebook**	**AudienceView**	**Facebook**	**AudienceView**	**Facebook**	**AudienceView**
Task 3	37%	41%	**5.67***	**6.93***	**110.7***	**55.7***
Task 4	93%	78%	6.15	6.74	65.7	67.7
Task 5	81%	78%	**5.85***	**6.70***	74.8	51.1
Task 6	78%	74%	**5.37***	**6.74***	**111.7***	**57.7***
Task 7	85%	74%	5.89	6.56	75.8	38.0
Task 8	74%	89%	**6.00***	**6.70***	**83.0***	**59.3***
Task 9	93%	93%	**6.19***	**6.89***	**157.0***	**37.8***
Task 10	85%	93%	**5.93***	**6.81***	**131.4***	**43.9***

*** Statistically significant differences at the 0.01 level using the Student's t-test**

data. Due to this anomaly, we removed that participant's data from the study. Of the 27 remaining, 15 participants were male and 12 were female. Twenty two participants were between the ages of 18-24, three were between 25-34, and two were 35 or older. Eight of the participants were computer science students and the remaining 19 were students of varying majors. Eleven participants reported having a Facebook account for less than six months and had rarely used Facebook. These we classified as novice users. The remaining had used Facebook for longer and most reported frequently using Facebook and were categorized as the expert participants. Ten novice participants and one expert participant reported not ever configuring privacy settings and only two experts reported frequently modifying privacy settings on their Facebook accounts.

Since tasks one and two were considered warm up tasks, I do not report any statistics for either in our results. Results over all participants for the configuration tasks three through ten are shown in Table 1 with significant differences in bold.

The average accuracy represents the average number of correct responses for each task. Overall, the average accuracy for all tasks was 78% for the Facebook interface and 77% for AudienceView. We found no significant accuracy differences between the Facebook and AudienceView interfaces. Thus, hypothesis 1 was not supported.

The average confidence is the average Likert score for each task, where 7 represents "Very Confident." For all tasks, users reported higher confidence in task completion when using the AudienceView interface, with a significant difference for 6 tasks. Thus, hypothesis 2 is supported.

The duration was calculated from the video analysis and reported in seconds. For all but one task, users completed their tasks faster in AudienceView, with a significant difference for 6 tasks. Comparing total durations for all tasks, users completed tasks in a significantly shorter period of time. Thus, hypothesis 3 is supported, users can configure settings more quickly in AudienceView than Facebook.

To further explore task completion times, Figure 3 shows a variability gauge graph for tasks 3-10 durations. Box plots add structure to visualize the differences in duration data between the Facebook and AudienceView interfaces. For a better visual representation, a line connecting the means across the different tasks has been included. This graph visualizes a consistency trend we noticed with the AudienceView interface. The grouped mean line shows an improvement of almost one half for the Facebook interface. More importantly, the connected means across task vary much less with AudienceView's interface. It appears that with AudienceView, respondents were able to apply learned skills from previous tasks to help with subsequent tasks. The Facebook interface did not exhibit this same attribute. For example, learning how to configure privacy in AudienceView for a data item such as the mobile phone uses the same method as applying the privacy setting for a photo album. However, with Facebook, these two items are on completely different pages and use different methods to apply a setting. Additionally, Facebook offers multiple paths to reach the privacy page for photo albums and no path was easy for respondents to locate.

Earlier, I mentioned different ways of formatting task questions that could appear to be configured easier with a particular interface. This was determined by classifying the tasks by identifying the number of data items to configure for the total number of audiences. Applying settings for single data item with multiple audiences would mechanically favor the Facebook interface, while multiple data items for a single audience would mechanically favor AudienceView. For example, I asked respondents for task eight to configure the profile to only show status updates to all of the owner's friends except the“Shady Friends” group, and to not show status updates to any network. When starting from the privacy settings page in Facebook, the respondent would need to execute three mouse clicks, type three letters and execute two additional mouse clicks. In AudienceView, the respondent would need to check each audience page to configure and then verify that status updates were viewable by all friends, except “Shady Friends” and not viewable by any networks. This could be done with a minimum of 13 mouse clicks using AudienceView's interface. Even with additional clicks needed to complete a task in AudienceView, participants were able to execute the tasks faster. Figure 3 also highlights the large differences that occurred in task completion time for tasks 9 and 10, which mechanically favored AudienceView.

I then examined the results for any ordering effects of interface presentation. The only evident effect we found was with confidence levels. Participants who started with Facebook reported significantly higher confidence for Facebook than those who started with AudienceView ($F = 18.03, p < 0.0001$).

I then examined the differences between novice and expert participants in our study. I found no differences between novices and experts in accuracy. However, for confidence, I did find that the mean difference in confidence between the two interfaces was significantly higher for novices than experts ($F = 22.04, p < 0.0001$). This is because novice participants were significantly less confident with Facebook than the experts ($F = 23.05, p < 0.0001$), although there was no difference in confidence between novices and experts for AudienceView. This indicates that novices did experience a greater improvement in confidence, as they were equally confident with AudienceView and less confident with Facebook than the participants with much greater familiarity with Facebook. Finally, novices were slower at completing tasks in both interfaces, but they did not experience greater improvements with AudienceView. So, overall hypothesis 4 is not supported for accuracy and duration, but is supported for confidence.

After close analysis of the respondent sessions, I noticed a general trend that most respondents seemed to put forth more effort when asked to "configure" as opposed to only "observe" settings. As a result, few respondents "gave up" on the configuration tasks early and occasionally would spend large amounts of time to accomplish the tasks. This varied from Richter el al.'s study [77], where, if respondents could not quickly observe the correct answer, they would guess and report a lower confidence. However, several participants using the Facebook interface did discover settings locations in later tasks that were needed previously, where they had either configured the setting incorrectly or not at all. These participants then temporarily abandoned

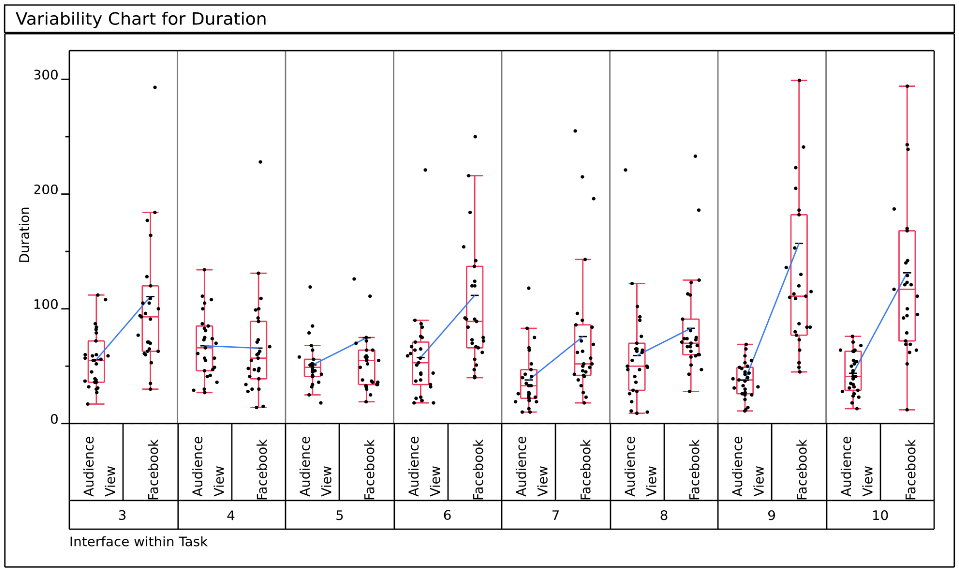


Figure 3: Box plots of task durations (in seconds) for each interface.

their current task and reverted back to the previous task to correct the answer. These situations are not represented in our numerical results, as we reported accuracy and confidence for the final answer, and calculated the overall duration of the task. None of the respondents needed to address previous tasks with the AudienceView interface.

There were several prominent causes for longer task completion times with the Facebook interface. Many respondents had difficulty actually finding the setting that corresponded to a particular data item. More specifically, participants found it difficult to locate settings for applications and photo albums. While Facebook provides multiple links to access the application privacy settings page, many respondents struggled to quickly find how to access the page. Some of the more experienced Facebook users were able to remember where the links were and did navigate more quickly to the settings page.

In contrast, I noticed smaller duration times when users were able to quickly find the location of a setting in the Facebook interface. For instance, participants configured privacy for the email address rather quickly in task four. This was likely because I asked participants about the email address in task two. They appeared to remember the setting's location. However, I noticed this was not true for all tasks and data items. For example, task three and task ten involved participants modifying settings for two separate photo albums. Several participants who correctly completed task three by accessing the photo album settings page struggled to find that same page while working on task ten.

I observed another difficulty as participants hesitated while trying to determine how to properly configure sets of friend groups. For some data items, the customized setting's pop up window has fields for "All friends except..." and "Only these friends..." where users can include or exclude friends or friend groups. Some respondents with a more technical background appeared to be more proficient at making this calculation quickly, but most paused noticeably to construct a mental model of the sets of friends. AudienceView's propagation method appeared to be easier to understand, as users seemed to have little trouble applying a setting to all friends or networks, then adjusting a specific audience page for exceptions.

In a post-session interview, I asked respondents to comment on which interface they preferred and why they preferred that interface. All participants indicated a preference for the AudienceView interface. Additional comments supported their preferences. For example, a participant wrote:

> *P15:"I definitely liked the prototype interface. I felt I had more control over my privacy settings."*

Another participant remarked:

> *P14:"I think the prototype was more straightforward than Facebook's interface."*

While I attempted to recruit a variety of participants, the majority who volunteered were college students. Thus, the results may not generalize to a wider population. In addition, because I was comparing against an existing interface, users may have been biased by their knowledge that AudienceView was my experimental interface, and been more positive about the prototype. Follow up studies would be needed to further generalize our results.

3.1.4 Discussion

To summarize these results, users configured their privacy policies faster and with improved confidence with AudienceView. I was surprised, given how much users seemed to struggle in Facebook, that accuracy did not improve in AudienceView. Unlike the study by Richter el al. [77], users did not give up on completing a task, and instead took a longer amount of time in Facebook, with several participants even returning to previous questions. Thus, users are capable of using the existing policy interface if they take enough time and effort. However, the more time and effort required to create privacy policies, the less likely users will be to do so. Many inaccurate answers for both interfaces appear to have been caused by misreading or reading the question too quickly, so the participant would forget to configure one of the audiences before completing the task. This happened frequently in both interfaces, but would not likely be a factor when an individual is modifying controls for their own desires.

Participants' comments after the sessions also reflected that their improved confidence impacted the preference for the AudienceView interface. Thematically, participants expressed that AudienceView provided less uncertainty and more control, as P16 comments:

> *P16:"I thought the prototype was easy to use and very effective. It didn't have the uncertainty that the Facebook interface does."*

I believe this confidence is provided by the visual feedback that an audience-centric view affords. To prepare the study, I frequently used multiple Facebook accounts in an attempt to verify the outcome of applying different privacy settings. AudienceView provides that immediate visual feedback, which improves the user's model of how information is viewed and hidden to their configured audiences. Simply providing a passive audience view to check on the outcome of settings is helpful, but not sufficient. Facebook does have a feature to allow users to view their profile from the perspective of an added friend, and while this feature was already available during the study, none of our participants actually used it to aid in completion of the tasks. Users might not have noticed the location of this feature, but it is also one more step they would have needed to perform on top of what was already a lengthy configuration process.

In comparing the novice and expert participants, it was also interesting that the experts did not perform much better than the novices. Even with years of Facebook experience, many participants were not that familiar with the privacy settings interface. There are several explanations. Users might never have tried to modify their privacy settings. While this seemed to be the case early in Facebook's history [44, 88], later surveys have indicated that most users report modifying at least some of their settings [52], as our experts did. However, Facebook is evolving rapidly and making frequent modifications to the interface, reducing familiarity. Facebook's interface also appeared to be difficult to learn and remember. While remembering the location of a setting did improve performance, these participants had difficulty remembering the locations of some settings even within the same 20 minute session! The location of a privacy checkbox or menu, even when grouped thematically, does not appear as memorable as the very visual layout of the information on the profile page and AudienceView. Additionally, if the layout on AudienceView is very similar to the layout users see every day, such as while viewing other users' profiles, their regular activities will inform their use of the privacy policy interface. This is not the case with Facebook's current settings interface.

AudienceView tested the effectiveness of a common HCI tradeoff. While it might require users to execute more mouse movement and clicks to perform certain tasks, less cognitive effort is needed to complete the tasks. Facebook's current interface forces users to hunt for pages and carefully think about the implications of menu choices and customized setting options. This represents a transfer of a Facebook cognitive problem to a slightly more complex mechanical method used by AudienceView. Designers should consider this tradeoff in proposed interface designs and evaluate even simple cognitive costs associated with interface mechanisms.

AudienceView is not without limitations. The effectiveness of the design depends on having a relatively small number of audiences. Even with the implemented propagation of settings, it might be overbearing for a user to click on many views just to verify who can see what information. There is also another limitation with the propagation/override model. By allowing overrides, the user could experience a false sense of applying a setting to an aggregated group. For example, if a user were to override the "Close Friends" friend group, but want to apply that same setting to "All Friends" later, the user would need to manually undo the override. Implementing a third state to the aggregated group lock icon with a partially configured state would give additional visual feedback to the user indicating not all composite audiences are configured.

Users should be able to fully participate in the benefits of sharing personal information by having full control over sharing and protecting their personal information. Applications need usable privacy controls to enable users to more fully reflect the nuanced privacy we exhibit in physical social situations. We have examined and evaluated a novel interface for managing personal information on social network sites. Our results indicate that the improved visual feedback in the form of information sharing to different audiences does lead users to more quickly and confidently modify privacy settings. These results might have two consequences. First, for users who desire greater privacy, a more usable interface may help them increase their privacy protection, reducing their risks and helping them feel more comfortable sharing information. Second, for those who already have restrictive settings, the interface might encourage them to more selectively share certain pieces of information with wider audiences, improving their social experience. Ideally, all users would have an increased and accurate understanding as to what information they are sharing with whom.

While these results are encouraging, I have only examined one audience-centric design against one particular social network site. To generalize these results, I more fully examine the range of privacy policy interfaces, and how well the audience view concept will work across a range of applications. The next section describes research that compares AudiencView with another proposed prototype interface to help users configure complex settings.

3.2 Expanded and Compact Designs

Many access control mechanisms represent a policy as a set of rules governing the permissions that various groups or roles are granted to various data. Some interfaces simplify the rules into sets of checkboxes or menus, such as choosing whether certain data items are public or private. A number of studies have demonstrated that users struggle to understand and properly manage privacy and security policies [20, 86] and need simpler mechanisms and more usable interfaces.

In this section, I seek to compare two of these representations: Expandable Grids and AudienceView. For this comparison, I chose the domain of privacy policies on social network sites, particularly Facebook. These access control policies are available to hundreds of millions of users who maintain profiles filled with personal information.

3.2.1 Expandable Grids

The Expandable Grids interface, shown in Figure 4, was created by Reeder et al. as a general method for representing and modifying access control policies [73]. Expandable Grids show precisely what a policy allows or does not allow in a matrix with hierarchical axes that can be expanded or contracted to show more or less policy detail. For this study, the set of principals, shown along the top axis, were the groups of people that Facebook allows for privacy policies: “All My Friends,” “Friends of Friends,” and “All My Networks” categories. Friends had subgroups of “Best Friends,” “Family,” and “Shady Friends” while specific networks represented the institution and city.

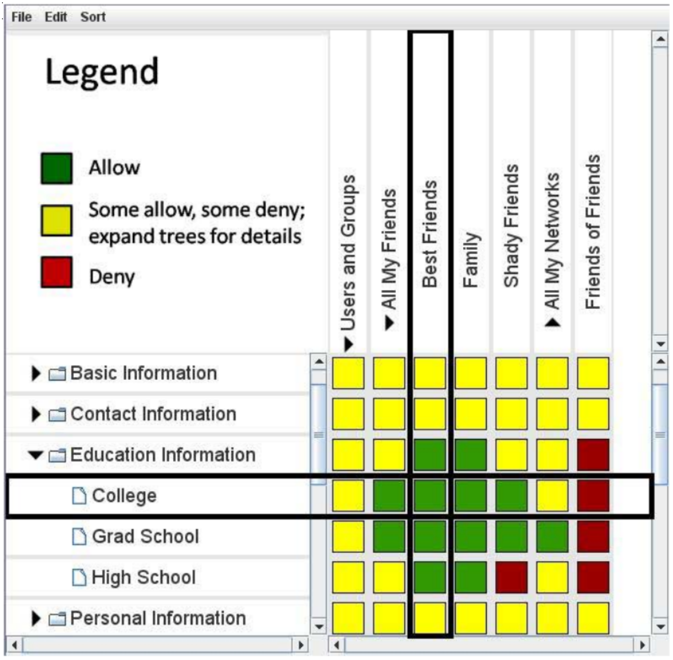
The set of resources is shown along the left. These are the categories and individual information fields provided in Facebook, such as “Basic Information” which includes fields such as “Birthday” and “Hometown.” In this domain, permissions are simple access—allow or deny. Thus, a red box indicates that access is denied, a green allowed, and yellow that the category has a mixture of allow and deny permissions. The user clicks on the box to set the permission for the particular information and user group. When setting a permission on a category of resources or principals, the rule is then applied to all of the individual pieces of information or people in that group.

3.2.2 AudienceView

AudienceView was implemented as described in Section 3.1. Expandable grids uses three colors to visualize the access control states: red, yellow and green. For this study, we slightly modified AudienceView to include a yellow lock icon to indicate a mixed privacy settings. The updated prototype interface is displayed in Figure 5.

3.2.3 A Comparison

Both interfaces have previously been positively evaluated against existing policy interfaces in different domains and employ an audience-centric design. The grid visualization of Expandable Grids is more general, able to represent any kind of resource



Legend

🟩 Allow

🟨 Some allow, some deny; expand trees for details

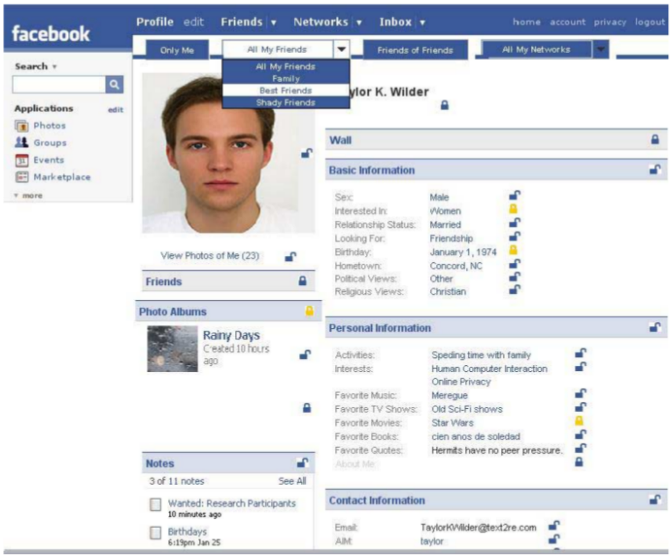
🟥 Deny

	Users and Groups	All My Friends	Best Friends	Family	Shady Friends	All My Networks	Friends of Friends
Basic Information	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Contact Information	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Education Information	🟨	🟨	🟩	🟩	🟨	🟨	🟥
College	🟨	🟩	🟩	🟩	🟩	🟨	🟥
Grad School	🟨	🟩	🟩	🟩	🟩	🟩	🟥
High School	🟨	🟨	🟩	🟩	🟥	🟨	🟥
Personal Information	🟨	🟨	🟨	🟨	🟨	🟨	🟨

Figure 4: The Expandable Grids interface.

and principal, with multiple levels of hierarchy, for a range of permissions. The grid can provide an overview of all settings at once, with the ability to drill down to more specific ones. In comparison, AudienceView is more limited because it is strongly tied to the visual representation of a set of information, making the interface more difficult to reuse across domains. The metaphor may also be more difficult to convey for permissions beyond simple access control. The representation inherently limits the number of potential audience groups, as too many would be difficult to display and interact with. These differences would obviously influence in which domains either interface could be used.

From a user's point of view, Expandable Grids is more compact, which may make it easier and faster to find and modify settings. AudienceView's settings, on the other hand, are spread across many pages. Yet, the interface provides a more concrete



Sex: Male
Interested In: Women
Relationship Status: Married
Looking For: Friendship
Birthday: January 1, 1974
Hometown: Concord, NC
Political Views: Other
Religious Views: Christian

Activities: Speding time with family
Interests: Human Computer Interaction
Online Privacy
Favorite Music: Meregue
Favorite TV Shows: Old Sci-Fi shows
Favorite Movies: Star Wars
Favorite Books: cien anos de soledad
Favorite Quotes: Hermits have no peer pressure.
About Me:

Wanted: Research Participants
10 minutes ago
Birthdays
6:19pm Jan 25

Email: TaylorKWilder@text2re.com
AIM: taylor

Figure 5: The AudienceView interface.

context by showing the specific information that is being shared, which may help users better understand the implications of a policy. Thus, the purpose of this work is to determine how these differences impact users' performance and preferences in understanding and modifying an access control policy.

3.2.4 Methods

I designed a within-subjects study to compare the tradeoffs between the AudienceView and Expandable Grids policy representations. Another investigator and myself recruited participants by handing out flyers on campus and through word of mouth on Facebook. We first gathered basic demographic information. We briefly explained the functionality of one interface and gave participants unlimited time to play with an unconfigured interface. Next, the participant opened a preconfigured interface, and we instructed the users to complete a set of tasks as described below. Participants were given a set of Likert-scale usability questions about the interface. The same process was then repeated for the second counterbalanced interface. Finally, participants were given an interview about which interface they preferred and why, and what they liked and disliked about each prototype.

Users completed 17 individual tasks for each interface. After each, the participants rated their confidence in their actions or responses on a scale of 1 (very unconfident) to 7 (very confident).

The first four tasks asked users to read and understand the existing policy. For example, “Which of the following friend groups can see your relationship status?” These tasks further introduced the user to the interface and gauged their understanding of existing settings.

The second four tasks were simple configurations of a single item or category and a single audience, such as “Deny your family from viewing your photo albums.” The next four tasks were more complex configurations involving multiple items for a single audience. For example, “Allow your best friends to view your email, mobile phone number, and work information.” The next four tasks involved a single item configured for multiple audiences.

The final task asked participants to pretend the displayed profile was their own and to take as much time as needed to configure all of the privacy settings as they deemed appropriate. For this task only, we asked them to think aloud.

We attempted to balance the audiences and information fields to be configured across the tasks. None of the tasks depended on previous tasks for successful completion. Again, we used usability software to record screen video, and a custom application to log timing and confidence.

3.2.5 Results

We recruited 23 participants. 16 were ages $18-24$, four $25-34$, one $35-44$, and two over 55, 12 males and 11 females. The background of the participants widely varied. We classified 8 participants as novice users, with less than 6 months of Facebook experience (and 1 had never used Facebook). Ten participants reported frequently modifying their privacy settings on Facebook, while 3 reported never modifying. Unfortunately, the video for 2 participants was corrupted and we were only able to analyze and report the confidence and timing data for those 2 participants.

There were no differences between the accuracy rates for the two interfaces. For AudienceView, over all participants ($n = 21$) only 13 tasks (4%) were performed incorrectly. Eleven errors were caused as participants could not find particular data items, mostly during the first 4 tasks. In Expandable Grids, there were 18(5.7%) incorrect responses. Twelve of which were while modifying privacy settings and 4 were performed by a single user.

While the difference in errors is not significant, the errors committed reveal tradeoffs between the two interfaces. In AudienceView, users initially appeared to have a harder time finding particular pieces of information. This was easier in Expandable Grids. However, participants did occasionally mis-click on the wrong box in the grid. This could either be a motor error, or an error in reading the proper row or column. In Expandable Grids, mis-clicks could be more difficult to recover from. For example, if a user allowed or denied a category of information or group of users, that rule propagated down to all sub-fields or sub-groups. If that action was not intended, the user must then re-do all the rules for the sub-fields to recover. This did occur several times, and for one participant we even reloaded the pre-configured settings to recover. An undo function, however, would solve this problem. AudienceView was not as prone to this issue, although users could still mistakenly navigate to the wrong audience page or forget which audience page they were configuring.

For all tasks, confidence was reported as 6.48 (out of 7) for AudienceView, and 6.51 for Expandable Grids. Using Wilcoxon signed rank tests, We found no evidence of a difference between the two interfaces. Overall, participants were highly confident interacting with both interfaces. This makes sense given the high rate of accuracy.

We performed four two-way repeated measures (2 X 4) ANOVAs with each grouping of similar tasks and interface as the two within-subjects factors. For each of these tests, we performed a Tukey HSD post hoc analysis and focused only on the measures between interfaces for the same task.

For the first set of tasks (tasks 1-4), the ANOVA ($F(3, 20) = 22.358, p < .001$) and subsequent post hoc Tukey HSD test revealed a significant timing difference ($p < .05$) between interfaces for task 1. In task 1, AudienceView was slower than Expandable Grids ($XG = 51.61s, AV = 94.70s$). We believe this is because participants appeared to need time to explore the interface at first and find particular data items. However, they sped up over time. Our analysis for tasks 5-8 and tasks 9-12 revealed no differences between interfaces.

For tasks 13-16 ($F(3, 20) = 8.502, p = .001$), Expandable Grids was significantly faster for tasks 15 ($XG = 46.35s, AV = 86.83s$) and 16 ($XG = 36.13s, AV = 60.57s$), which involved configuring an item for 4 or 5 different audiences. What was surprising is that there were no differences for tasks 13 and 14, which involved fewer audiences. Thus, Expandable Grids was faster as expected for configuring multiple audiences, but only for more than 3.

Fifteen participants reported preferring AudienceView, while six preferred Expandable Grids. There were no differences in the responses to the 7 usability questions between the interfaces in general. However, not surprisingly, users rated the interface that they preferred higher on each of the usability questions.

Participants liked the visual feedback in AudienceView and felt that the interface provided a more accurate depiction of their information.

> *P12:"I liked the visual aspect. It made it easier to know what you are configuring without having to go back and look."*

However, they did not like having to visit so many pages to manipulate all of the privacy settings:

> *P13:"It was time consuming going back to check for each group."*

With Expandable Grids, users liked being able to see the entire policy at once:

> *P13:"It was all on one screen..."*

and

> *P20:"...easier to see the bigger picture."*

We did notice two potentially interesting findings that may warrant further investigation. The 3 users over the age of 35 all preferred Expandable Grids. Additionally, 7 out of 8 users who reported frequently modifying privacy settings on Facebook preferred AudienceView.

Finally, we compared the behavior and resulting settings for the final task where participants were asked to create an entire policy as though it were their own profile. Once again we found few differences. Users generally took between 4 and 5 minutes to modify all of the settings. As users got tired of the task, they frequently modified only categories of settings, such as “All My Networks” and made fewer adjustments to the more detailed friend groups or data fields, to speed up completion of the task. With Expandable Grids, several users took the strategy of first setting the entire policy to either deny or allow (which can be set using one box), and then adjusted the policy from there. This did not appear to result in any efficiencies however. This capability was not available on AudienceView.

We wondered whether the added context shown in AudienceView would change the privacy policy that was configured. While we did not find quantitative differences, one participant did comment on the benefits of the context:

> *P1: “Some of that stuff on [Facebook], you know, people can steal that. And when I was doing it on [Expandable Grids], I would have probably given some of that information out So when I looked at that on [Audience View], then I realized the importance of it, ’cause I could visually see what I was doing.”*

Other participants also indicated that AudienceView did improve their confidence in the resulting policy configuration. As another participant stated, with Audience-

View

> *P13:"I was completely confident in what I was configuring. It was right there in front of me."*

Whereas P9 indicated that Expandable Grids,

> *P9:"... made me nervous to click on the beginning of a row. It made me question, did I do it right?"*

3.2.6 Discussion

Overall, both interfaces were highly usable. Considering the very different representations presented in the two interfaces, I was very surprised by the general lack of performance differences. In particular, I expected that Expandable Grids would be faster for more tasks, and that the added context in AudienceView may lead to higher confidence. Yet these differences did not materialize. However, users did have clear, and different, preferences. The participants in the study acknowledged the same advantages and disadvantages we had identified with each interface. Namely, they liked the visual feedback of AudienceView, but not all the page visits. They also liked the compact overview available with Expandable Grids with all settings in one location, even though it lacked the visual feedback.

These results indicate that either interface would be a usable option for similar privacy policies, such as other social network and personal information sharing sites. However, different representations may appeal to different users. Many participants suggested combining these two interfaces to provide the best of both worlds. For example, one participant commented that he would use Expandable Grids to first modify all his settings, and then use AudienceView to view and tweak them. Thus, users may benefit from a combination of both representations, to provide both a clear and concise overview of a policy, while still allowing for detailed visual feedback.

More generally, these results indicate that users do value both a contextual representation and a compact representation for privacy policies. Audience-centric designs enhance user understanding and provide better mechanisms for configuring privacy policies. However, results provided thus far are limited by the confinements of a lab experiment. The two previous studies help understand how users react to configuration tasks, but it is still unknown whether users will expend additional effort to manage online privacy—even with better audience-centric mechanisms. Next, I present a study on a newly introduced social networking site by Google Inc.: Google+.

3.3 User Perspectives on Audience-Centric Design

Recently, Google released a new social network site that introduces the concept of circles to enable users to easily group and classify online social network friends. Google+ circles can then be used to both filter incoming stream messages and selectively post messages to appear on friends' streams. While Facebook friend lists can provide this same functionality, the Google+ circles mechanism is more visible on the interface and is integrated in the initial setup of the user account. This paper presents an exploration into how early adopters of Google+ understand and react to circles—an audience-centric design mechanism. I sought to examine the effect produced by an audience-centric design for grouping friends. We also wanted to determine if the introduction of circles as a predominant feature influenced sharing behavior and the management of information flows.

Past research focuses on how users struggle to manage their relationship context in online social networks, particularly when they have multiple groups of friends with differing expectations [95]. Social context becomes a problem once a social network has hit a critical mass and users have one public image within multiple social contexts [13]. Decisions about sharing are impacted by a variety of factors and should be dependent on the context of the relationship.

Indeed, users express a desire to group or categorize the intended recipients of their shared information [65]. Previous research has examined using audience-centric mechanisms to control information within online social networks [33, 77]. In industry, Facebook and Orkut provide mechanisms for users to view profile information from the perspective of others. Additionally, Facebook has provided functionality of grouping friends into lists (2007) and even controlling information flow to those lists (2009). Although these capabilities have been available for some time, there is little evidence that users have adopted them. For example, Facebook users have reported that they were unaware that the functionality existed or found it too difficult to use [54]. To cope with the lack of ability to share based on relationship context, social network site users tend to self-censor based on "everyone" in their network seeing anything shared, resulting in less intimate levels of disclosure [54].

Google+ was released on June 28, 2011 by invitation only, and was released publicly in late September 2011. The primary differentiator of Google+ is circles, making this site the first with such a highly visible and integrated group-based sharing mechanism.

This level of integration of social context with the primary sharing task gives Google+ adopters a unique perspective on how they adapt to audience-centric sharing. Facebook has since responded by making friend groups more visible and supporting the automatic generation of friend lists based on attributes like location. Thus, studying early adopters of Google+ can provide a unique and valuable perspective on user behaviors and perceptions of audience-centric sharing that is timely and relevant to social network site research and development.

3.3.1 Methods

In order to understand early adopters of Google+, I designed a semi-structured interview with participants who had joined the social network site. Another investigator and myself conducted interviews during August and September 2011. We recruited participants using snowball sampling, starting with the investigators' friends of friends. We set two qualifying requirements: the participant was an early adopter of Google+ (had joined shortly after the limited release) and the investigator did not know the participant. Additionally, We required that participants be at least 18 years of age and have access to a phone, Google+ Hangout, or other video/voice communication software.

Most interviews were able to be performed using Google+ Hangouts. After the connection with the participant was made, she was directed to a webpage containing our informed consent document. The investigator quickly gave an overview of expected participation and explained that the audio, not video, would be recorded to later analyze participant data. Once the participant accepted the terms of the study, the investigator began audio recording and started the interview by asking demographic questions such as occupation, age, gender, state, and social networking site usage. The investigator then asked participants to self report their level of technical skill on a scale from 1-10 with 10 being the most technical.

We asked a variety of questions regarding reasons for use, managing information flow, audience understanding and comparison between social network sites. For most questions, we gathered perspectives on how the participants use both Facebook and Google+ in an attempt to understand how the introduction of circles impacted social network behavior. These questions served as a starting point for discussion and as the participants answered, we probed any interesting or ambiguous responses.

Once the interviewing phase was completed, we transcribed the recorded sessions and coded them using Atlas.ti. Two researchers performed open coding on the transcribed data and resolved any coding differences. We developed concepts based on the agreed coding to examine common responses and understand behavior. After we formed the categories, we had 84.1% inter-coder reliability.

3.3.2 Results

We recruited 15 participants from throughout the United States. Participants ages ranged from $22 - 50$ with $mean = 31.73$ and $median = 28$. Participants came from a wide variety of a backgrounds, however, half ($n = 7$) reported themselves as working in a technology-related profession such as computer repair. Participants reported a high level of technical skill ranging from 5-10 with $mean = 8.33$ and a $median = 9$. The high level of reported technical skill could be a result of the snowball sampling method, but we believe it is also likely related to a higher number of technically skilled early adopters of Google+.

Most participants ($n = 14$) seemed to embrace the idea of Google+ circles. Only one participant expressed a strong dislike towards circles calling them “annoying.” However, most participants talked about liking how circles could control streaming and posting information flows. Additionally, all participants were able to understand the concept of circles and how to categorize their friends.

Participants expressed a variety of reasons for liking Google+ and circles. The most pronounced reason was Google+’s clean interface ($n = 10$). Other reasons were: integration with other google apps ($n = 5$), increased information control ($n = 5$), having asynchronous relationships ($n = 2$) and the faster page load ($n = 2$). We asked the participants to express dislikes about Google+ circles and the only dislike that was common between multiple participants was the lack of a private communication mechanism ($n = 2$).

Participants in our study had varying numbers of circles from $2-12$ with a $mean = 6.7$ and $median = 6$. Participants’ circles varied widely, with some containing a single person labeled boyfriend to a participant who put everyone in either friends or family. We found many variations between these two extremes including a participant who separated church friends from church leadership, trying control information flows from smaller groups within their larger social categories.

Most of our participants ($n = 9$) talked about using G+ circles to deliberately post to different groups of friends. For example,

> *P14:"I have a lot of SEO friends at work and I find an interesting SEO vulnerability I want to share with them. I would never post it on Facebook because 90% of my friends would be like, what is SEO? I don't care, why are you telling me this? So Google+, I'm a lot more likely to share more information with a limited group based on their expectations of me."*

These participants are using Google+ circles to selectively control information by making sure they are posting to an appropriate audience. This represents a desire to control information for the purpose of posting appropriate (but not necessarily private) messages. We additionally noted participants ($n = 5$) commenting on using circles to control information for privacy purposes, such as one participant (P12) who mentioned not posting to everyone a message that she was leaving town because of fear that too many people might know her house would be empty.

Despite such a large number of participants who embraced the idea of circles and liked them, We found many ($n = 7$) participants have only rarely used them to selectively post content. Over half ($n = 9$) of the participants mentioned the concept of posting to only some of their circles, but not all of these participants had actually done so yet. We found varying reasons for this and have extracted several themes to describe this behavior below.

3.3.2.1 Facebook Mentality

Out of the 15 participants, not one used friend lists on Facebook to restrict a post to a group of friends. Despite being highly technical, very few ($n = 3$) configured friend lists. Two used them for incoming stream control, profile, or chat availability control and one found them excessively difficult to use. This lack of using Facebook friend lists combined with additional reasons—such as worrying about future employers discovering information, family disagreeing with the content, and concern of offending friends—led many users to adopt a cautious posting strategy on Facebook. In essence, participants adjusted their posting strategy to try and mitigate any potential problems by not posting problematic or very private content at all. Some participants ($n = 6$) continued to use this strategy on Google+ by simply posting to all their circles. P4 responded to a question about the process she used to post messages:

> *P4:"So, um it looks like I just shared it with everybody. Because I think it's going be the same thing. I think it's going to be the same thing with Facebook. It's like, I don't feel comfortable posting things that I'm not comfortable with everybody seeing."*

Therefore, being able to selectively choose a group of friends did not impact the decision to post, but rather only the comfort level with the post content being shared with everyone. Perhaps as users become more familiar with Google+, or use Facebook less, this mentality may change.

3.3.2.2 Lack of users

Some participants reported posting to all their circles simply because there are not enough people on Google+ to define distinct audiences.

> *P2:"So, if I post on google+, it's for everybody and right now because a*

> *lot of the people that are on google+ are my technical friends from my electrical engineering program or computer science."*

The investigator asked these users how the management of their circles would change as Google+ scales up. Many of them indicated that as it grew they would begin adding more circles. Thus, if Google+ continues to grow, the gap between the perception of how to use circles and actually using circles for this category of users may decrease.

3.3.2.3 Effort

Google+ circles enable users to manage the flow of information by selecting groups of friends. Google+ seems to have significantly reduced the effort required to configure and use circles in comparison to Facebook's friend lists. Recently (September 2011), Facebook moved friend lists to a more prominent place at the left of the news-feed interface, perhaps attempting to make this feature more usable. This data was gathered before Facebook's interface change and it may now be easier to use and/or configure Facebook friend lists.

Even though Google+'s interface reduced effort, we still encountered participants ($n = 2$) who reported that the amount of effort to use circles was still too large. For example:

> *P3:"I used to try and manage it, but it was a lot to think about, like because I felt like I was missing some... Do I post to friends? Do I post to family? But what if friends are in family category too? It just kind of got confusing so I just started posting to everyone under friends right now."*

This participant estimated that she previously created 10 distinct circles to categorize her friends. After she decided it was too much effort to manage, she went back and moved all of her friends to a single circle and deleted the remaining circles. This behavior presents some interesting questions regarding the amount of mental effort required for managing information flows to groups of friends and if this effort might be excessive. In other words, even under the most favorable usability conditions, would some people consider it too much additional effort to selectively manage friend groups and choose which groups to post to? If so, friend grouping features like circles will only ever have limited impact on privacy and sharing behavior in social network sites.

3.3.2.4 Potential Privacy Shortcomings

Google+ offers a clean interface for presenting circles that seem easy to use and understand. This could explain why the participants reported liking circles as a way of managing information flow. We observed this high level of satisfaction as well as a sense of trust that some participants ($n = 3$) explicitly expressed in Google to protect them and their data. However, this trust and satisfaction can easily be lost because of breaches in privacy from unanticipated sharing. We have identified two areas where such breaches may be likely to occur: resharing and commenting. If users do trust circles to selectively share more private information, those breaches may be more serious than similar breaches on other social network sites where users expect more public sharing.

Resharing is a popular and useful feature of many online social network sites. However, the ability to reshare posts presents two potential privacy issues. The first is the non-repudiation that occurs when a friend decides to reshare information. When the post is reshared, Google+ confirms its authenticity and identifies the original posting user alongside the content. The second is distribution potential. It is relatively easy to reshare content with a much larger audience than the original poster intended. For example, with Google+, resharing to large audience can be accomplished by simply choosing *Your Circles and Extended Circles* (all of your friends' circles). This could be more problematic for users who have repurposed streams to circumnavigate the lack of private messaging.

The potential extent of this privacy breach is unknown because of the social constraints which may prevent many problems. For example, Google+ currently provides a warning dialog when resharing a post originally intended for a limited audience. The dialog advises the user that the post was originally limited and that the user should be thoughtful about who it is reshared with. Privacy mechanisms that rely on social constraints are beginning to be studied and early findings are positive, but also suggest that they can fail when there is little perceived reason to protect the content or there is a weak social connection between people [9]. Google+ has a *post lock* feature that provides additional and adequate control for these cases. However, this feature appears as a menu item after submitting a post and might not be discovered and used unless the feature can be made more visually prominent. Even so, this would require additional user effort to configure when posting anything that is intend to be private or limited.

The second area subject to potential privacy breaches is comments. With Google+, sharing is tightly integrated around circles. Therefore, we asked the participants questions about their understanding regarding information flows and comments. Less than half ($n = 6$) of participants were able to correctly describe who could see comments to their own posts or comments they added to others' streams. We considered the correct response to be the original post privacy settings. However, a more accurate correct response would include some knowledge of the potential that others may be added via the *+Name* functionality, a feature that appears throughout many Google products. None of the participants in this study acknowledged the possibility of expanding access to a post by friends who have added additional people in comments.

Most participants ($n = 13$) mentioned cautiously posting and self censoring on online social networks. This strategy works well in situations where the recipient audience is large and consists of many groups of friends. However, we speculate that as people continue to embrace circles and start to take advantage of managing information using groups, users might develop a false sense of security and potentially fall victim to unintended additional comment sharing.

3.3.3 Discussion

This study offers insight into the behavior of Google+ early adopters and their use of audience-centric designs. We found participants had strong positive attitudes towards using circles and understood the intended purpose of them. Yet, despite user understanding, I still saw a disconnect in users' stated desires and behavior. Despite Google+ lowering the level of effort required to interact in contextually appropriate ways, many continued using strategies for privacy management they had formed by using Facebook and simply posting to all circles. In addition, some participants found that circle use increased the mental demand required for social network interaction. Similar to previous studies, the increased effort lead some of our participants to bypass the privacy mechanisms. In the case of this study, this meant collapsing friends into a single circle. Thus, early adopters are not yet taking full advantage of the capabilities provided by circles for greater control over information flow.

Additionally, while users understood circles, there was still a general lack of understanding and concern about how information may spread beyond the intended audience through commenting and resharing. This may, in turn, lead to privacy breaches which reduce trust in the site and the positive impact of circles.

Google+ offers an interesting case study in providing users with a strongly desired feature—namely the ability to control how information is shared with different groups of friends. And indeed, our early adopters almost universally appreciated and liked this feature. This exploratory study shows users welcome audience-centric design to help control social information. It remains unclear if additional burdens associated with audience-centric design are too much effort. For example, the grouping of audiences is additional effort; will users accept these additional burdens to benefit from audience-centric design? The next chapter focuses on further reducing this configuration burden by using community feedback to modify unchanged privacy settings.

3.4 Conclusion

In this chapter, I present three user studies that examine audience-centric designs. First, I test the AudienceView prototype application to see if Facebook users configure privacy settings faster and with more confidence than with the Facebook mechanism. AudienceView demonstrates better performance over the traditional combo-box interface, but does not significantly lessen user burden. Users did feel more confident about their settings with AudienceView, however, the time needed to configure privacy settings was still excessive.

Next, I presented a study that compares two different audience-centric designs: the visually expanded AudienceView and the more compact Expandable Grids. Results from the study highlight a common design trade-off—visual versus compact—and suggest both designs are effective at improving access control understanding. User preference was split between the two designs suggesting people prefer one type, but the preference is subjective. This study suggests audience-centric designs can be visually compact and expanded, yet both improve understanding.

Google+ recently introduced an online social site with circles—an audience-centric design. I presented a study that examined user reaction to a deployed audience-centric mechanism. Results indicated users still struggle to manage privacy with audience-centric designs. Thus, audience-centric designs seem to improve understanding and comfort, but only marginally reduce configuration burden. Community feedback may be used with audience-centric design to create better default settings and reduce configuration burden with automated changes. However, it is important to understand how users will react to automated changes in privacy settings. In Chapter 4, I examine user reactions to privacy setting changes from community feedback.

CHAPTER 4: USER REACTIONS TO AUTOMATED PRIVACY CHANGES

As more people use online social sites, users experience sharing with an increased number of distinct social groups. Forming audience groups and managing access control to these groups requires additional and significant configuration burden. As the amount of information and sharing features increase, managing many privacy settings becomes even more difficult. Yet, people still want to socialize over the Internet and share information to appropriate audiences. In this chapter, I begin to explore using other people's decisions from a community of information as feedback to help configure privacy. These automated changes may better reflect user privacy attitudes and require fewer configuration changes from the user. Although these changes might reduce user configuration burden, it is important to explore how users will react to automated changes in privacy settings. This chapter qualitatively explores user reactions to automated privacy changes.

Community feedback can be used in several ways to reduce burden for configuring complex privacy settings. Initial privacy default settings can use community information to customize a privacy policy to user preference. Another method of using community feedback is to evaluate community settings over time and respond to recommended changes from community data. This chapter investigates how users react to a change in their privacy settings after the creation of a default policy. To gather this reaction, the details of the automated system are abstract and the user is informed of a privacy setting change recommended by other people.

Any automated change reduces configuration burden, but likely generates negative user reactions—especially if the change contradicts the user's preference. Privacy settings on online social networks represent a user's configured policy to control access to personal information. If privacy setting configuration is completely automated, any change that does not match the user's privacy attitude can be problematic. Automated changes that restrict information contrary to preference reduces social interaction and social connections leading to detrimental effects to healthy online social networks. People use online social networks to share information and restrictive changes that limit social interaction may frustrate users as they seek to primarily use a social networking site to share information with large social networks. More permissive changes can also produce negative user reactions. If personal information is exposed to a larger audience, the user might experience some negative consequences. Such cases of unintended disclosure can result in possible loss of employment, strained relationships and embarrassment. Thus, it is important to explore how users react to automated changes to privacy settings in these varying situations.

Automated changes based on community feedback use other people's decisions to guess a privacy setting that better fits another user's privacy preference. It may be difficult for people to understand automated changes and how a system can determine preferences from community information. Thus, methods for conveying information about automated changes can help provide additional information on user reaction and how people perceive automated changes. Social norms can be used to influence reaction to social changes [42, 75] and may also impact user reactions to automated changes in privacy settings. Descriptive social norms are formed from how most people would behave in a social situation. Injunctive social norms represent how other people approve or disapprove of behavior within a specific culture or community. To explore the impact of social norms, I include descriptive and injunctive social norm language to better understand how this might impact the user's perception of such changes.

In this chapter, I present an exploratory qualitative study to examine how users will react to automated changes in privacy policies. If users accept automated changes in privacy policies, privacy settings can be configured without user interaction. However, notification and/or consent may be necessary for users to accept any change in privacy settings. Notifications can be provided either before or after the change giving users the option to undo automated changes. This study captures how users react to a change with a notification after the change occurred with no option to undo the change. This study also provides results on what conditions are necessary for users to accept automated changes in privacy settings. The exploration of this concept will inform the community feedback process for reducing user burden to configure complex privacy settings.

4.1 Methods

User reaction to changes in privacy settings is challenging to study, especially in a lab environment. When study participants are aware of the privacy aspect of a study, they tend to react differently to privacy tasks [17]. To reduce such bias, simple deception of the true nature of the study can distract the participant and gain a more realistic reaction to privacy questions and tasks. This study used deception to gather reaction to a spurious message about an automated privacy setting change made by Facebook. The purpose of this deception was to observe a genuine user reaction to a change in privacy settings void of any informed consent. This study followed an approved Institutional Review Board (IRB) protocol from the Office of Research Compliance at UNC Charlotte.

This study used an exploratory qualitative design that gathered participants' reaction to an apparent Facebook message informing the user that their privacy settings had been automatically changed. Each session used standard recording utilities to record the laboratory computer screen and simultaneously record audio and video of the participant's face using a web camera attached to the computer. I used javascript code injection to generate the spurious privacy setting change message. The study included a preliminary demographic questionnaire and a post task/deception debriefing semi-structured interview about the reaction to the message and other privacy-related topics. These materials are available in Appendix A.

I recruited participants using convenience sampling methods. In an effort to reduce sample bias, I posted recruitment flyers in multiple locations including local libraries in the Charlotte area and on the campuses of the University of North Carolina at Charlotte and Winthrop University in Rock Hill, South Carolina. I also distributed the recruitment flyers in the downtown area of Charlotte, North Carolina at the common lunchtime hour to coordinate future appointment times.

To qualitatively study the effect of social norms on automated changes in privacy settings, I used a control with two different treatment conditions. The conditional messages were:

- Control - Facebook has *changed some of your privacy settings.*

- Descriptive Norm - Facebook has *changed your privacy settings* to match other people who are similar to you.

- Injunctive Norm - Facebook has *changed your privacy settings* because other people like you have determined that your privacy settings *were not appropriate.*

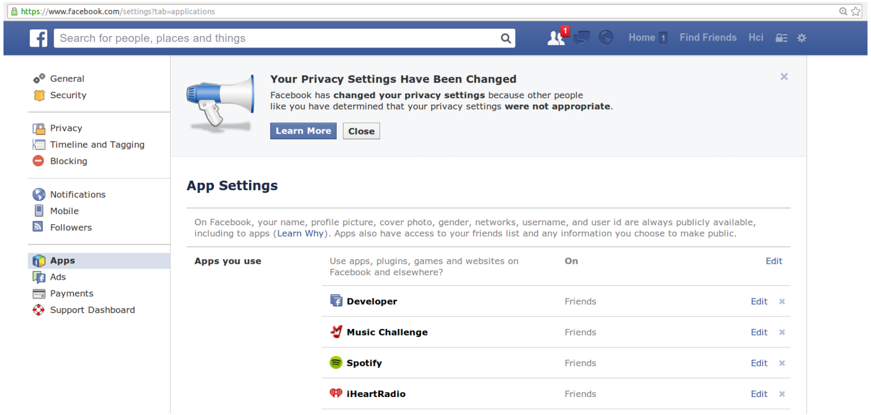
Chrome is a widely used Internet browser developed by Google. Google Chrome is extensible and allows arbitrary code to be included as an extension on the local computer and injected into any webpage. For this study, I developed different Chrome extensions for the control and treatment conditions and used javascript to inject the message when the participant clicked on the icon to remove an application from their Facebook profile. Before each study session, I prepared the laboratory computer with the Chrome extensions and rotated activation to the extension for the next treatment.

At the beginning of the study session, I presented the participant with an informed consent document that described the deceptive purpose of the study—to gather user perceptions on features that make a good social music application. I told each participant they would have the opportunity to use several different Facebook social music applications and then I would ask them questions about each application and its features. After the particpant consented, I instructed them to answer the demographics questionaire and I navigated to Facebook.com on the study computer. The participant then logged in to Facebook with their Facebook username and password. After a successful login, I took control of the computer and started the screen recording and the web camera for audio and video recording of the participant. The participant then followed my instructions for the deception task.

For the deception task, I wanted to maintain as neutral emotional effect as possible. Social games might potentially seed positive or negative emotions, so I chose to use a social music application to reduce the possibility of introducing any emotions before observing the privacy setting change message. It is possible that a social music application could generate an emotional effect, however, this seemed the most likely type of application to reduce extreme emotional responses. During pilot tests, I asked the study participants about the emotional effect of the music application and they all reported little to no emotional reaction to the social music application. Thus, I decided to use a common Facebook music application called SoundCloud [1] for the deceptive task.

Immediately following the login to Facebook, I instructed participants to navigate to the Facebook application page and install SoundCloud to their Facebook profiles. After the application install, each participant spent between five to seven minutes exploring sound bits that other users had uploaded to the SoundCloud website. The social aspects of the application allowed users to browse recommendations based on the music preferences of their Facebook friends. I instructed the participants to browse through the recommendations and talk out loud about any music choices they seemed to like from the available recommendations. After browsing the music application, I told them that I needed to remove the SoundCloud application as part of the study regulations.

[1] *SoundCloud - Hear the world's sounds* (accessed January 29, 2014); available from https://soundcloud.com/



Your Privacy Settings Have Been Changed

Facebook has **changed your privacy settings** because other people like you have determined that your privacy settings **were not appropriate**.

App Settings

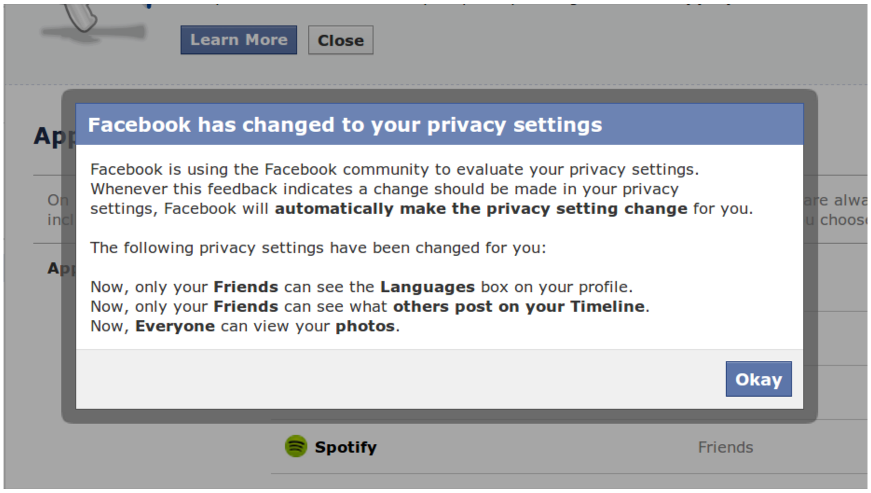
On Facebook, your name, profile picture, cover photo, gender, networks, username, and user id are always publicly available, including to apps (Learn Why). Apps also have access to your friends list and any information you choose to make public.

Apps you use	Use apps, plugins, games and websites on Facebook and elsewhere?	**On**	Edit
	Developer	Friends	Edit ×
	Music Challenge	Friends	Edit ×
	Spotify	Friends	Edit ×
	iHeartRadio	Friends	Edit ×

Figure 6: Injected automated privacy change message for the injunctive norm treatment condition.

To make the injection message sufficiently salient to the participant, I took control of the laboratory computer and navigated to the Facebook application removal screen. I removed the SoundCloud application from the participant's Facebook profile which triggered the injection code and produced the study message on the page. I pretended to first notice the message and told the participant that I had never seen such a message and that it looked important. Next, I explained that this was a good time for me to go and retrieve the gift card for participation and the participant could spend time to interact with the privacy setting message. I left the room for about five minutes to allow the participant time to view and interact with the message. A screenshot of the injected message is displayed in Figure 6.

During the time alone, the participant could click on a "Learn More" button that was part of the injection code. This button included more details about what privacy settings Facebook had modified. This message was the same for each condition and is shown in Figure 7. I chose only three privacy setting changes attempting to expose a wide range of potential reactions with as few profile items as possible to avoid



Facebook has changed to your privacy settings

Facebook is using the Facebook community to evaluate your privacy settings. Whenever this feedback indicates a change should be made in your privacy settings, Facebook will **automatically make the privacy setting change** for you.

The following privacy settings have been changed for you:

Now, only your **Friends** can see the **Languages** box on your profile.
Now, only your **Friends** can see what **others post on your Timeline**.
Now, **Everyone** can view your **photos**.

Figure 7: Automated privacy change "Learn More" dialog box and message.

making the message length excessive and discouraging the participant from reading the message. The three privacy setting changes were:

- Languages to Friends - Intended to be a benign change of a non-sensitive profile item.
- Posts to Timeline to Friends - Intended to restrict social activity that many might consider important to be widely available.
- Photos to Everyone - Intended to expose a potentially sensitive profile item to a large audience.

Upon return to the study room, I informed the participant of the deception. I explained that Facebook had not made any privacy changes and that I generated the message to see how they would react to automated changes in their Facebook privacy settings. Each participant was given the option to withdraw from the study and receive the full compensation or continue to answer privacy questions related to the injected message. If the participant agreed to continue, I administered the privacy debriefing semi-structured interview. The interview included general questions about Facebook usage and attitudes. I also asked participants to describe their reaction to the privacy change message. In addition to the reaction to this privacy change, I asked how they would react in two hypothetical privacy setting change scenarios:

- How would you react to an automatic change to your privacy settings if the change matched your preference?
- How would you react to an automatic change to your privacy settings if the change did not match your preference?

If necessary, I discussed some more concrete examples of automated changes to privacy settings that represented the hypothetical situations described above.

After each participant session, I quickly reviewed the participant's reaction on the session video and recorded any notable expressions or verbal reactions to the message. Two independent researchers reviewed participant facial reaction to the automated privacy setting change. The reactions were categorized as concerned or not concerned. The coders also rated whether the participant read both the initial change message and the additional information about the change using the "Learn More" button. Accounting for the probability of agreement, an interrater reliability analysis using Cohen's Kappa statistic was performed to determine consistency among raters [23]. Once the interviewing phase was completed, two researchers transcribed the recorded audio and coded them using Atlas.ti. The researchers performed open coding on the transcribed data, then resolved any coding differences, resulting in an overall intercoder reliability of 86.6% agreement between the two independent coders. I developed concepts based on the agreed coding to examine common responses and better understand behavior.

4.2 Results

I recruited a total of 19 participants from the Charlotte area with the participant age range from $18 - 49$ and $mean = 25.2$ and $median = 22$. Eight participants were female and the remaining eleven were male. Eleven participants were students at either UNC Charlotte or Winthrop University while eight worked in various disciplines in the Charlotte region. As part of the demographic questions, I asked the questions associated with the Facebook Intensity Scale. This scale ranges from a possible range from $0 - 5$ with higher scores representing a more intense connection with Facebook including representation for emotional connectedness and daily integration with Facebook [34]. The scale values ranged from $1.98 - 4.19$ with $mean = 3.27$, $sd = 0.61$.

During the debriefing interview, I asked participants about general Facebook usage and concerns. Not surprisingly, ($n = 16$) participants used Facebook to keep in contact with friends. Only half ($n = 8$) had any concerns using Facebook with no consistent reasons for concern. Participants views toward Facebook were mixed and some ($n = 6$) mentioned disliking Facebook because other people share too much personal information about themselves. These participants mentioned not wanting to know about every daily detail of their friends' lives.

Over half ($n = 10$) of the participants claimed to have modified Facebook privacy settings. Only one participant claimed to use privacy settings often. In all cases, I asked what privacy settings they remembered modifying and many claimed to have only filtered the newsfeed to limit updates from friends that engage in excessive posting. Two ($n = 2$) participants mentioned using Facebook grouping mechanisms to selectively post to a limited audience. The remaining ($n = 7$) participants responded that they had never modified Facebook privacy settings.

For the purposes of this study, I categorized the boundary (see Section 2.1.2) each participant seemed to make sharing decisions [68]. Almost half ($n = 8$) mentioned making sharing decisions at the disclosure boundary indicating that they only share information considered appropriate for a very large or even public audience. For example, P6 said:

> *P6:"Not really since I don't really post anything bad nowadays, like anything that would embarrass me or anything like that, because I know, for example, now employers look at it. If I did have something that was bad in my profile that now would be a concern.... I guess [I've] grown up and matured, I post a lot less. I think about it a lot more like who's going to read this.... If you post something I guess I think about like everyone can see this."*

The remaining ($n = 11$) participants at least made some sharing decisions at the identity boundary—disclosure to multiple audiences for the purpose of regulating an identity associated with different social groups. Of these, three participants only changed the entire profile to "Friends" only and it was not clear if they ever managed privacy with more than one audience. These results are consistent with previous studies that indicate larger percentages of online social network users making more decisions at the disclosure boundary [8, 99].

4.2.1 Reaction to Automated Privacy Setting Change

As previously mentioned, I overtly drew attention to the change message and then let each participant examine the message in private. Notwithstanding my coercion to pay close attention to the message, some ($n = 5$) participants immediately dismissed the message. One of these participants immediately commented that the message was not important and just to close it. However, the remaining ($n = 14$) participants seemed to at least partially read the message. At least ($n = 13$) ($Kappa = .76$, $SE = .162$, 95% $CI = .439 - 1.0$) participants had a visibly unconcerned expression immediately following my acknowledgement of the message.

The video analysis indicated only a few participants ($n = 5$) ($Kappa = .66$, $SE = .17$, 95% $CI = .326 - .992$) carefully read the initial message. Participants could choose to either dismiss the initial privacy change message or click on the "Learn More" button shown in Figure 6. When a participant clicked the "Learn More" button, the modal dialog message in Figure 7 appeared. Many ($n = 11$) participants clicked on the "Learn More" button and carefully read ($n = 10$) ($Kappa = .89$, $SE = .106$, 95% $CI = .682 - 1$) the text displayed in the information box. It is interesting to note that more participants carefully read the "Learn More" message than the initial message notifying the participant of an automated privacy setting change.

Some ($n = 6$) participants examined their privacy settings while they were alone in

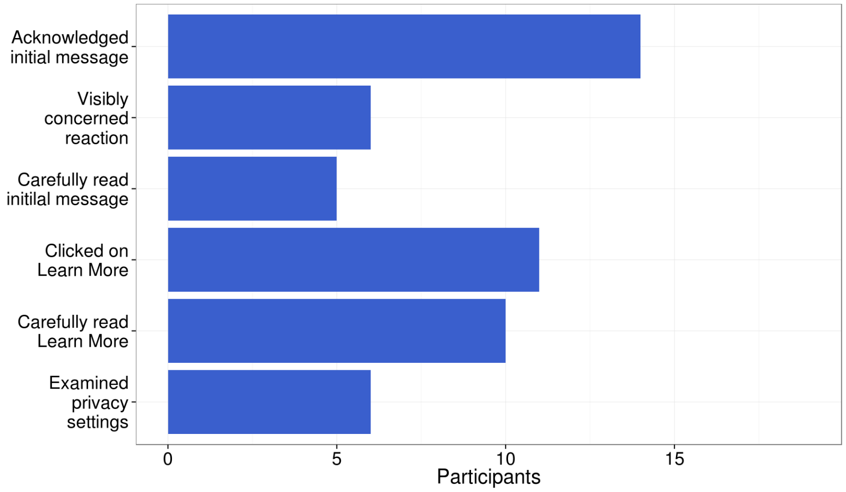


Figure 8: Reaction to automated privacy setting change.

the study room. Interestingly, only one ($n = 1$) participant accessed the exact location within Facebook's privacy setting pages related to one of the supposed automated privacy setting changes (P13 reviewed "Timeline" privacy settings). It appeared that many of the participants were attempting to locate privacy settings related to photos, but were unable to find the page. One participant (P6) even entered the phrase "photo settings" in the Facebook search box that seemed to yield unsatisfactory results.

The emotional reaction to a privacy setting change seemed clear for participants to characterize, however, explaining reasons for their feelings seemed more complex and participants experienced some difficulty in articulating the source for their reactions. Participants' comments about their reaction to the message were widely varied. Often, participants struggled to understand exactly how they reacted to the privacy setting change. For example, P1 commented:

> *P1:"I think I'd be a little, I don't know whether to say, concerned or alarmed, but I can't think of the word, ... I almost want to say annoyed.*

> *Yeah, that you would click on something and it would change your privacy features by clicking on something like that. I think I'd be a little irritated with it."*

In the debriefing interview, ($n = 12$) participants claimed to have read the initial message, differing from the video observations of ($n = 5$) that carefully read and ($n = 14$) that at least acknowledged the message. Two ($n = 2$) participants mentioned dismissing the message because they were participating in a study. Some ($n = 6$) participants confirmed that they were not initially concerned with the privacy change message. Half ($n = 3$) of these participants indicated that the lack of concern was because they only posted content that was acceptable for any audience. Other reasons for lack of concern cited were: trust in Facebook to make good decisions with privacy changes ($n = 1$), acclimation to any Facebook change ($n = 1$), and being confused about the message ($n = 1$). When discussing the level of concern about Facebook automatically changing privacy settings, many ($n = 7$) of the participants commented they would not be concerned enough to stop using Facebook.

Participants ($n = 7$) who were most concerned mentioned only being concerned about the photos being set to public. P6 commented:

> *P6:"I don't want just anyone being able to see my pictures and private stuff like that. Other things I don't really care about like languages on my profile that everyone can see. I wouldn't really care.... I mean something like what kind of language that I speak would be something that if someone is trying to find me as a friend or something they could see that and it*

> *wouldn't really matter. I wouldn't really regard that as something private, but all of my pictures and stuff I ever had would be something that I don't want just anyone out there to be able to see and stalk me."*

For most participants, it was unclear if the lack of concern for the other profile items was a result of the profile item itself or the change of audience to "Friend." However, those participants that read the message and commented about the profile items mentioned a lack of concern about the "Languages" and "Timeline" profile items.

After discussing the reaction to the message, I asked participants questions about how they would react to two hypothetical automatic privacy setting changes. Over half ($n = 11$) of participants reported some level of concern if a setting changed and it matched their preference. Of these 11, ($n = 5$) mentioned being concerned because of a lack of control. Other concerns mentioned were skepticism that Facebook could ever guess their preference ($n = 5$) and any automated change would be pointless ($n = 1$). Most ($n = 7$) participants who were concerned even when the change matched their preference would feel comfortable with such changes if Facbook notified them prior to making the automated change. Almost all ($n = 17$) participants said they would be concerned if Facebook made a change that did not match their privacy preference. The remaining two ($n = 2$) participants both explained they would blame themselves for posting anything embarrassing if Facebook changed a setting that contradicted their preference. P14 commented about posting embarrassing content:

> *P14:"I guess I would have to be mad at myself for putting something on*

> *there on accident.... I've always been told ever since I was little; even now, not just on the Internet, but even on paper don't even write down anything that you don't want somebody to know. I mean, if it's an accident. It's not [Facebook's] fault that it goes to thousands of people and it's a picture of me butt-[expletive] naked. That's my fault."*

4.2.2 Other Reactions

An interesting finding was that participants ($n = 8$) associated Facebook privacy setting changes with other general Facebook changes. These participants mentioned the frequency that Facebook changes and seemed generally disenfranchised with all Facebook changes. Thus, these participants mentioned being less concerned about any single Facebook change and said it was a natural consequence of using online social networking sites. Of these eight participants, some ($n = 5$) participants commented that they felt indifferent about any change Facebook decides to make. For example, P5 commented:

> *P5: "The change itself doesn't bother me that much, because I feel like Facebook has changed stuff before, not necessarily in privacy settings, but just, 'Hey, we changed this on your profile. We've reformatted this. We gave you a cover picture, something.' "*

4.2.3 Social Norm Reactions

Participants were assigned to one of three treatment conditions to evaluate both descriptive and injunctive norm effects on reactions to automated privacy changes.

The treatments were rotated at the beginning of the study session. Six participants were in the control treatment; five received the injunctive norm message and eight received the descriptive norm message. P19 should have been assigned the injunctive norm condition, but was given the descriptive norm message in error. Only one (P3 in the injunctive treatment group) participant mentioned noticing the injunctive norm language that their setting was determined inappropriate by others. This participant described the norm language as the reason she clicked on the "Learn More" button.

P3:"That's why you click on the learn more. Why is it not appropriate?"

Over half ($n = 12$, $n = 5$ in descriptive treatment, $n = 4$ in injunctive treatment) the participants claimed to have read the initial message, however, during my video analysis, I could only confirm that a few ($n = 4$, $n = 1$ in descriptive treatment, $n = 3$ in injunctive treatment) read the message carefully. The injunctive norm language described the change as being a community judgement that the user preference was deemed inappropriate. Thus, it is interesting that three participants in this treatment that carefully read the message did not mention any negative or positive reaction to the norm language.

4.3 Limitations

As with any study, this study suffers from certain limitations. To understand how people will react to an automated privacy setting change, it is crucial that participants understand information about the change. Despite my measures to adequately draw attention to the message, some participants ignored the message and were not aware of a privacy setting change. Only ($n = 2$) participants mentioned dismissing the message because they were engaged in a study, however, more participants may have dismissed the message because of the study environment. If participants failed to explicitly mention any effect on reaction caused by the study, it would be difficult to determine the true distraction from the laboratory study.

For this study, I used two raters to determine if the participant read the messages on the screen. The raters were instructed to use techniques such as time focused, mouse movement and facial expressions to best determine if the participant was reading. Eye tracking software would provide better evidence of reading and more definitively specify if the participants actually read the text. Thus, it is possible that other participants read the message, but gave little visible indication in the video analysis.

Another limitation of this study is how people perceive changes in online social networks that are constantly updating and changing. During the three months it took me to recruit and run study participants, I had to modify my injection code twice to react to Facebook changes. Privacy setting changes affect who has access to information posted by users. Other Facebook changes only change the appearance of the interface and likely have no impact on how information flows through the social network. Thus, it can be problematic when users perceive all Facebook changes similarly.

4.4 Discussion

These results began to explore understanding of how people reacted to automated changes in privacy settings. Many participants ($n = 13$) reacted with little concern when notified of an automated privacy setting change but almost all ($n = 17$) responded with concern for hypothetical automated changes. After seeing the privacy setting change message, eleven participants clicked learn more, but only six attempted to visit or confirm their privacy settings. However, eleven mentioned being concerned with a hypothetical automated change that matched their preference. This exposes the complexity of understanding general privacy attitudes and how hard it is to manage privacy in online social networks. Online social network privacy configuration is complex and difficult, but users still lack the trust to allow the provider to automatically aid in configuration. Furthermore, users express a desire to be notified and or provide consent for privacy setting changes, but struggle to give sufficient attention to system notifications. The reason participants immediately dismissed the initial message may provide some insight into how people will react to change messages on social networking sites.

Many ($n = 6$) participants mentioned automated changes reducing the level of control over their settings. People felt the need to control their privacy settings and they perceived the privacy settings as something similar to their profile or posting information. This might represent that they felt similar ownership for both the profile items and the privacy settings that manage access to those items. Thus, unintended access to the profile items and automated privacy changes may both be perceived as an invasion of privacy or personal space. A few ($n = 3$) participants even characterized the automated change as a privacy invasion. For example, P3 commented:

> *P3: "Just automatically changing my settings even though I didn't tell them to is kind of ... It is invading your privacy really. If somebody else is*

> *allowed to go into and change the settings on my Facebook without me telling them, I think that's kind of wrong. I think."*

Thus, any automated privacy setting change—even from community feedback—would need to explore possible ways to mitigate this user sentiment.

Social norms may be used to reduce negative reaction to automated changes. This study explored using both descriptive and injunctive norms to examine any reaction changes related to these norms. Results of any impact were inconclusive because most ($n = 13$) participants did not carefully read the initial message containing the norm language. Participants that carefully read the message may have dismissed it because of the study environment. Future research with more salient norm messages and user reaction is required to better understand how social norms affect user reaction.

One finding to help overcome the complex challenges of automation of privacy settings configuration was that many ($n = 7$) participants would not stop using Facebook if they discovered their settings were being changed. Obviously, Facebook would not want to lose 63% of their patrons, however, these findings intentionally explored a worst case scenario with making automated changes to privacy settings. Incorporating notifications and consent for privacy setting changes may significantly reduce the concern perceived by online social network users.

The purpose of this dissertation is to explore how community feedback can enhance default privacy settings. With changes in default settings, many of the confounding issues discovered in this study with automated changes are mitigated by only using community feedback for default settings. Many people lack awareness that default settings are a configured privacy policy by another party without their consent. Facebook.com developers decide the default privacy policy for each new Facebook user. If people never visit or change privacy settings, the default policy represents the user's policy without consent as P5 explained:

> *P5:"I would definitely want to be informed. First of all, if they didn't tell me, I don't think I would ever know. I don't think I would have figured it out because I don't change my privacy settings that often."*

Thus, automating changes to default or unseen privacy settings can help reduce user concerns about privacy invasions regarding profile settings. It is possible that public knowledge of varying default policies might incite concern, however these acknowledged issues are beyond the scope of this dissertation.

How people share using online social networks also affects the efficacy of privacy settings. People who make sharing decisions at the disclosure boundary are less affected by any privacy setting change. However, in this study, over half ($n = 11$) of the participants made sharing decisions—to some extent—at the identity boundary and had used privacy settings to discretely share with different audiences. P4, an identity boundary sharer said:

> *P4:"I think I would still be upset [about the change], because [Facebook] changed it without my input at all.... Because it's my personal information that they're dealing with. I feel strongly about it. I feel like I should only have to share what I want to share. As of right now, all you can see on*

> *my profile is my name, my sex, and my profile picture, just so that you know that it's me."*

Thus, enhancing complex settings can still benefit many online social network users. It may help cautious users sharing at the disclosure boundary engage in some sharing at the identity boundary if configuring complex privacy were easier.

Eleven participants were concerned about any hypothetical change even if it matched their preference. About half ($n = 5$) of these participants mentioned skepticism about any system's ability to intelligently guess their privacy preference. People consider their privacy preferences personal and unique and struggle to accept any computer system that claims to be able to estimate their privacy attitude. Despite other common community feedback systems such as purchasing recommenders, people seem unaware of the type and volume of community data available to classify user behavior. This skepticism may also be a reflection of how people perceive and trust online social network providers. Future research or implementations would need to further understand user perceptions of system capabilities regarding the use of community data.

Online social network users are aware of privacy implications for different profile data items. These differences are important for understanding how to automate configuration of individual privacy setting policies. P6 sufficiently articulated the difference:

> *P9:"I was mad [at the automated change].... I did not want everyone in the public to see my photos. The way I said it is, everything I share is*

> *fine, like the jokes and whatever. That's fine, but I don't want people to see where I'm at or what am I doing, who am I friends with, the public out there and people actually likes your photos and stalk you, like where you live and what's my phone number and that kind of thing."*

Such characterizations of privacy profile data become important for automatically changing privacy settings. An optimized system would be able to account for the sensitivity of profile items. Because online privacy tends to be complex across users, these characterizations are likely to not be the same for all individuals. Thus, a next step for optimizing how to automate privacy setting changes is understanding how people characterize profile data.

4.5 Conclusion

This study explored how users react to automated community feedback changes in privacy settings. I provided greater understanding on what circumstances online social network users are able to tolerate automated changes in privacy settings. In general, people reacted negatively to any automated change in privacy settings without notification or consent. However, the sensitivity of the profile item was important to how users reacted to automated privacy setting changes. Any process that attempts to automate these changes should first characterize profile items and exercise more caution with items that are more sensitive to people.

The results indicated that most users wanted some form of notification or consent, however, some viewed privacy setting changes the same as other changes on Facebook. Also, more users were making sharing decisions at the disclosure boundary. These users experience more neutral reactions because they choose to post only information intended for large audiences. Privacy and privacy management are important to people who share at the identity boundary. These people desire more control over their privacy settings and react negatively when any system reduces control. Consent and undo features can be added to mitigate reduced control with automated privacy configuration.

Still, users may accept automated changes under certain conditions. As online social network sites gather more information, people understand they are exposing more information. Additionally, they expect online sites like Facebook and Google to change often and this may soften negative reactions such as feeling an invasion of privacy. As P5 noted,

> *P5:"It's a little scary that Facebook can change your setting like that, but at least they told you that they changed it. I read something the other week about how Facebook and Google know you so well that they can actually keep your profile running after you're dead, so I guess it wasn't surprising."*

In general terms, the findings of this study improve understanding of user reactions to changes based on other people's behavior. Online social network providers are the source for current privacy settings and changes to default privacy setting policies. The provider becomes a factor in considering automated changes in privacy settings because people view the provider as an important component. Privacy setting changes from community feedback does not necessarily change the role of the providers, but only determines the mechanism used to reduce user burden for privacy configuration. Users struggle to understand automated changes based on community feedback are less about the online social network provider and more about the behavior of other people in the social network community.

In summary, people conveyed very little reaction to the initial message informing an automated change in privacy settings. Yet, when discussing the change or other hypothetical changes, people responded with strong negative reactions to any automated change to their privacy settings. Users struggle to understand how community feedback could possibly be used to provide a better privacy setting. People feel their privacy settings are also private and automated changes invade this privacy and others feel automated changes significantly lessen their control of their privacy management. All of these human factors become a crucial part of using the large community data source available to online social network sites. Community feedback represents a potential to reduce configuration burdens, but negative reactions from users' lack of understanding makes solutions non-trivial.

This study contributes to enhancing default privacy settings by better understanding how people react to automated changes. These results contribute understanding that automated systems should account for varying sensitivity of different profile items, differing sharing behaviors and when and how to provide notification and/or consent for privacy setting changes. In the Chapter 5, I use these findings to inform a study designed to understand what profile items are most important to online social network users and if community feedback can be used to provide default privacy settings that more closely match users' desired privacy preferences. The study in next chapter seeks to validate using community feedback to create better default privacy setting policies for online social network profiles.

CHAPTER 5: DEFAULT PRIVACY SETTINGS

People are connecting and sharing large amounts of personal information through social media sites, cloud and health services, and other online applications. Users often manage their interactions and information disclosures on these sites using a variety of privacy settings. The use of privacy settings on Facebook has been extensively studied. Researchers have found that users have many friends and desire to selectively share with multiple audiences [15]. However, users struggle to manage their privacy settings as they are quite complex and the structure of the settings changes frequently. As a result, users can share information more broadly than intended, even within the "friend" group [50], resulting in embarrassment or regret. Rather than adjust confusing privacy settings, users may resort to various coping mechanisms such as censoring their disclosures [102].

I presented research in Chapter 3 that indicates users spend a large amount of time to initially configure a desired privacy policy even when presented with usable configuration mechanisms. However, there remains a large burden for managing these settings. Users would need to spend a large amount of time to initially configure a desired privacy policy, even when presented with usable configuration mechanisms. Beyond improving the interface mechanisms, another approach is to reduce configuration effort by generating default privacy settings that better represent user privacy preferences.

Default privacy settings on sites such as Facebook are generally open and permissive [43, 44]. For most online systems, default privacy settings are created by the developers, and are likely to emphasize the site's values for information sharing. Thus, permissive default settings may promote social interaction but may require more user burden to manage for those with greater privacy desires. While users are able to customize these settings, many do not, at least until a privacy violation occurs [88]. Surveys of end users have shown an increase in the awareness and modification of Facebook privacy settings over the years, yet many users still do not seem to be familiar with the extent of the privacy settings on Facebook or take the time to configure all possible settings [50, 60, 103].

My research seeks to reduce the gap between default privacy settings and user preference—to help reduce the burden of having to modify a large number of privacy settings and to increase the privacy of those who do not customize defaults. There is limited research on personalizing or inferring privacy settings from other users or past decisions [35, 61, 62]. I expand upon this research by exploring default policies based not only on users' setting preferences, but also on attitudes towards disclosures to alternate audiences.

In this chapter, I present a study that gathers privacy profile preferences from 184 Facebook users. Participants were asked about audience preferences for 29 common profile items and reactions to alternate audience changes for those items. Using this information I generated an optimal default policy for a training set of participants, and examine how that policy compares against three others: a completely restrictive policy, the preferred audience chosen by most participants, and the current Facebook default settings. Lastly, I explore using three different segmentation models to determine if multiple canonical policies could be used to further improve default settings. The use of segmentation models did not improve policy fit within the data. These results highlight the complexity of privacy attitudes and indicate that user privacy preferences of profile items and disclosure can be used to create default privacy settings that better represent user preferences.

The contributions of this chapter are two-fold. First, the data I gather from the survey provides characterization of user preferences for a variety of settings on Facebook, including users' discomfort with settings that do not match their preferences. Second, I demonstrate how that feedback can be used to evaluate the fit of policies against user preferences, and to calculate a policy from a community of existing users. The results show that even with a fairly simple method and a small training set, I can generate defaults based on existing users that will be closer to what users desire.

5.1 Community Enhanced Default Settings

Any set of controls has a starting point—the default configuration that the user then modifies as desired. Customizing these settings takes user effort, and users often accept the defaults rather than perform the work of modifying them to meet their needs [3, 60]. Thus, the default settings can have a large impact on the resulting privacy for users [50, 88]. Organizations who develop the applications thus choose these defaults, which may or may not take user privacy needs and desires into account.

A variety of research has examined how to automatically determine or recommend personalized privacy settings. One strand of research has investigated whether measured privacy attitudes correlate to privacy settings, and thus predict settings or privacy-related behaviors. A number of privacy indexes—ranked answers from a set of privacy questions combined together as a score or classification—have been proposed. These scores can then be used to group, or segment, people into categories. The most commonly cited index is the Westin and Harris privacy segmentation model [55]. Westin and Harris segment privacy attitudes into three categories: Fundamentalists, Pragmatists and Unconcerned. In a 2003 survey, Westin and Harris report only 10% of the U.S. population as privacy unconcerned—people who have no real concerns about how other people use information about them [55]. Other indexes include Buchanan et al. [19], Dinev and Hart [30] and Stutzman [90] which each measure privacy along multiple dimensions. However, few studies have shown that such attitudes predict or correlate to behavior. In this chapter, I explore using both the Westin/Harris and Buchanan indexes to segment the participants.

Another approach is to learn canonical policies from existing users, to determine the default settings for new users. For example, in the location privacy domain, work with the Loccacino and PeopleFinder systems seek to reduce configuration burden for dynamic and complex location privacy settings through user feedback and utilizing machine learning to generate default policies [62, 71, 78, 93]. The challenge explored by such work is to determine which policy or persona a new user should have to define default sharing settings. In Loccacino, users can explicitly choose a "privacy profile" for adoption as an initial policy. Results from a Loccacino study of 27 people over 3 weeks indicated that providing users with two to four canonical options can significantly reduce configuration burden by providing default settings that better represent the user's privacy preference [62]. I explore similar questions in this chapter within the social media domain.

Others have examined using machine learning or other algorithms to automatically determine settings based on a user's previous settings or behaviors. For example, Sinha et al. gather information about users' previous Facebook posts to predict better default policies for future posts [84]. Similarly, Shehab et al. and Mo et al. suggest using machine learning to automatically configure complex privacy settings for friends based upon configuration for an initial set of friends [61, 81, 83]. People's privacy settings and behavior often fail to represent their privacy preferences and approaches that use actual settings are limited by this paradox. These methods may help users as they make similar decisions about new content over time, but do not help with initial defaults for items or content that are relatively static.

Within the data mining community, researchers have also examined how to predict privacy settings. Closest to my work is Liu and Terzi who present a framework for computing privacy scores using profile item sensitivity and the user's social network level [59]. They test two models (Item Response Theory [7] and naive) for computing privacy scores from user privacy settings and find that Item Response Theory is a better model for predicting privacy preference. Also related to this research, Fang and LaFevre use a privacy wizard to gather user disclosure preference to provide better default privacy settings [35]. However, this research tests models with a user set that defines sensitivity using a single audience selection. In this chapter, I seek to improve defaults with similar methods by gathering more information about alternate audience disclosures.

5.2 Methods

I first gathered data about users' profile privacy preferences with a survey, asking users what their preferred setting was for 29 Facebook profile items, as well as their attitudes towards the alternate setting options. This approach allows me to not only characterize the participants' desired policies, but also their potential reactions to policies that do not represent their best preference. I decided not to query participants' actual Facebook privacy settings as users may not have taken the time or effort to configure their privacy preferences on the site for a variety of reasons. Thus, despite the limitations of a self-report survey, I felt that this would be the most accurate method of gathering participants' default preferences. The details of the survey, and the descriptive results, are presented in Section 5.3.

With the survey data, I randomly divided the sample into training and test sets to do a between-subjects comparison of different privacy setting policies. I examined four different default policies: two static policies and two that were calculated based on the reported preferences of the training sample of participants. I calculated a fit score for each participant in the test set and compared the scores for the four policies. The details of these calculations and comparison are presented in Section 5.5.

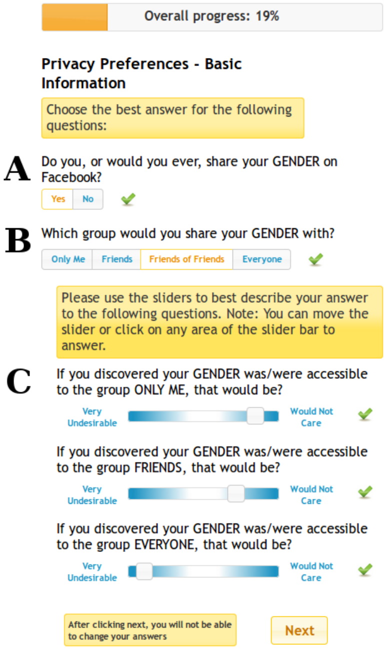
Finally, I performed two additional explorations of the calculated optimal policy. First, I explored the results of differing training set sizes on the calculation of the optimal policy. Finally, I explored differences with and without segmentation using three different privacy attitude measures from the survey. These results are presented in Section 5.6.

5.3 Survey

I designed a web-based questionnaire to gather Facebook privacy information from people in the United States. The participants were recruited using Amazon's Mechanical Turk system. Each participant or *Turker* can view a list of available Human Intelligence Tasks (HITs) and choose to participate for a monetary incentive, in this case a $2.00 incentive for an estimated 30 minute survey. The HIT was designed to only allow participants registered to Amazon.com with a valid United States address. I also restricted the HIT to *Turkers* with an overall HIT approval rate greater than 95%.

When a *Turker* accepted the HIT, she was first shown an IRB approved informed consent message that described the study and purpose. If the participant consented, she received the questionnaire. The questionnaire was divided into three logical components: a short demographics section, Facebook usage and general privacy attitude questions and specific questions about privacy preference for 29 profile items. I chose 29 profile items from those available on Facebook, but many of these items are also available as profile items on other social network sites. The profile items available on Facebook are shown in Figure 10.

The general usage and attitude questions were used to later segment participants' into preference categories. I first used the three question Westin/Harris segmentation index [55]. I also used a 16 question index developed by Buchanan et al. to measure privacy concern [19]. Finally, I surmised that perhaps general usage of Facebook may be related to privacy attitudes. Thus, I also included the Facebook Intensity Index



Overall progress: 19%

Privacy Preferences - Basic Information

Choose the best answer for the following questions:

Do you, or would you ever, share your GENDER on Facebook?

Which group would you share your GENDER with?

Please use the sliders to best describe your answer to the following questions. Note: You can move the slider or click on any area of the slider bar to answer.

If you discovered your GENDER was/were accessible to the group ONLY ME, that would be?

If you discovered your GENDER was/were accessible to the group FRIENDS, that would be?

If you discovered your GENDER was/were accessible to the group EVERYONE, that would be?

After clicking next, you will not be able to change your answers

Figure 9: Example showing three stages of a question about profile item privacy preference.

(FBI) designed to measure usage, frequency and emotional connectedness along with how the site integrates into people's daily activities [34].

I presented the privacy attitude questions before gathering the profile item privacy preferences. This introduced a privacy bias common in privacy studies [17], however, it was my intention to gather a conscientiously reported privacy preference. Still, these results likely present more restrictive default privacy preferences than users may truly desire when interacting on a social site.

The privacy profile questions were each displayed one per page in three stages, as shown in Figure 9. Participants were first shown only the question labeled A about disclosure preference—whether the participant would be willing to share the profile item on Facebook. The participant then selected a preferred sharing audience from four available options ranging from most restrictive to most permissive, "Only Me," "Friends," "Friends of Friends" and "Everyone" as shown in Stage B. If the participant selected "No," in Stage A, she would be asked the remaining questions about the profile item using hypothetical verbiage such as: "If you did share your *[item]* on Facebook, which group would you be likely to share it with?" The responses to the hypothetical questions in cases of non disclosure were discarded during analysis. The purpose for asking the additional hypothetical questions was to prevent participants from answering "No" in an effort to avoid answering additional questions. The third Stage C then queried the participant about their attitude if the profile item was somehow disclosed to the other three alternative audiences. These alternative options used sliders to gather an interval value from 0 (representing "Very Undesirable") to 100 (representing "Would Not Care"). I chose these labels to represent the strength of discomfort from alternatives that did not represent the optimal chosen audience. I settled on these labels after pilot testing.

In addition to the 29 actual profile items, I included two fake profile items as an instructional manipulation check [66]. These questions asked participants if they would be willing to share their Social Security Number (after the 12th profile item question) and their Debit/Credit Card Information (after the 27th profile item question) on Facebook. I considered any affirmative response to Social Security Number as invalid and removed the participant's data from analysis. For Debit/Credit Card information, I accepted a "Yes" response to disclosure because some people legitimately give that information to Facebook for application purchases. However, if they chose to disclose with a preferred audience other than "Only Me," I considered the response invalid and removed the participants from any further analysis.

For each page in the survey, I recorded the timestamp at the time the question(s) was/were first displayed. Thus, the time between timestamps was recorded as the amount of time in milliseconds the participant interacted with the question.

5.4 Results

During January 2014, I recruited 200 survey participants using Amazon's Mechanical Turk system. Of the 200 results, I excluded six ($n = 6$) participants with outlier responses to the instructional manipulation checks. I normalized the timing results for the remaining participants and trimmed any participant below the 2.5 percentile and above the 97.5 percentile. This excluded responses for any participant who may have not spent enough time to read the questions or that spent excessive time on the survey as to not represent the average participant. An additional ($n = 10$) cases were removed as a result of timing anomalies leaving a total of ($n = 184$) accepted cases for analysis.

Participant age ranged from $19 - 66$ with $mean = 31.4$ and $median = 29$. More ($n = 104$) participants were male than female ($n = 80$). Education levels varied between no High School diploma to Master's degrees with: ($n = 4$) having no High School diploma, ($n = 51$) graduating High School or having some college, ($n = 33$) having vocational training or Associate's degree, ($n = 57$) with Bachelor's degrees and ($n = 11$) with Master's or other professional degrees.

Facebook Intensity Scale: I asked eight questions as part of the Facebook Intensity (FBI) scale [34] to measure Facebook usage and how emotionally connected people feel to Facebook. The scale uses six likert questions about Facebook connectedness and two additional questions about social network usage—total number of Facebook friends and average time per day over the previous week. The total friends and average uses were assigned normalized ranks between 1 and 10 and the FBI score is calculated by averaging the reported ranks for all questions with a higher score ($max = 6.25$) representing a stronger connection and integration in the user's daily life. Participants scores in this study ranged from $1.25 - 5.75$ with $mean = 3.58$, $sd = 1.0$ and $median = 3.5$ resulting in average usage and a moderate distribution range.

Westin/Harris Segmentation: Privacy attitude assessment from the Westin/Harris survey was somewhat typical with a larger than expected number of participants segmented as "Fundamentalist" ($n = 82, 44.5\%$). Other participants were classified as "Pragmatists" ($n = 86, 46.7\%$) and "Unconcerned" ($n = 16, 8.7\%$). Most Westin/Harris results have resulted in: ∼25% "Fundamentalist," ∼60% "Pragmatists" and ∼15% "Unconcerned" [1]. The increased percentage of privacy "Fundamentalist" in this study may have been a result of a privacy bias caused by including other privacy indexes before the Westin/Harris questions.

Buchanan Index: The Buchanan et al. index consisted of the combined ranks of 16 Likert questions about general privacy concerns [19]. Scores range from $16 - 80$ with 80 being very strongly concerned about privacy matters. Buchanan et al. make no attempt to segment based on their index, but higher scores would correspond with "Fundamentalist" and lower scores would represent the "Unconcerned" group.

[1] *Most People are Privacy Pragmatists* (accessed February 7, 2014); available from http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Most-People-Are-Privacy-Pragmatists-Who-While-Conc-2003-03.pdf

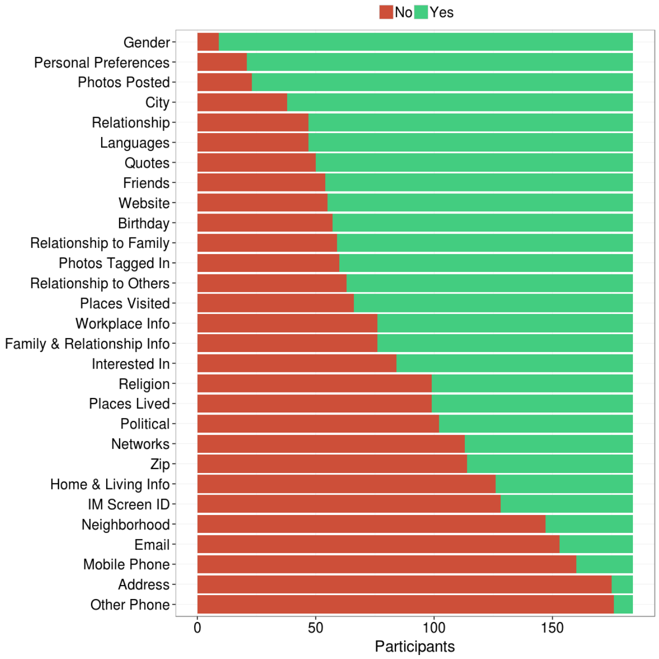


Figure 10: Disclosure choice for all participants for profile items ordered by disclosure.

Results from this scale included a wide range from 26−80 with $mean = 52.4$, $sd = 12.1$ and $median = 51$ indicating a moderate distribution range of scores.

Participants' reported disclosures of profile items is shown in Figure 10 ordered by willingness to disclose on Facebook. For most profile items, approximately two-thirds of participants were willing to share the item on Facebook. The more sensitive profile items (phone numbers, email and street address) were reported to be shared by around one quarter of participants. Items such as religion and political alignment along with previous location information were reportedly disclosed by about half of the participants. Life changes such as family and relationship information, home and living information and places lived also were disclosed by slightly more than half of the participants. More participants were willing to disclose the photos they post than disclose photos they had been tagged in possibly indicating a perceived difference in

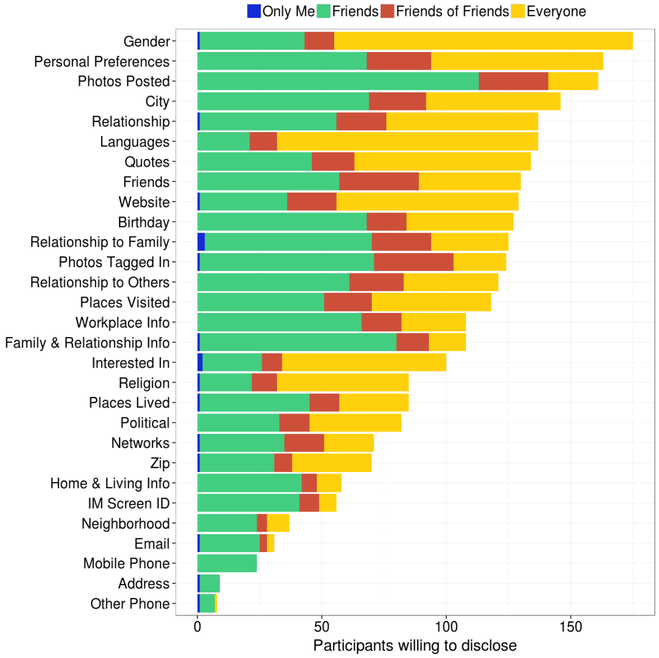


Figure 11: Preferred audience choice for all participants willing to disclose for profile items ordered by disclosure.

control over the disclosure.

Of the participants willing to disclose, the preferred audience responses are indicated in Figure 11. These results indicate most participants were more inclined to share profile information with their friends only, with the ratio between friends only and other audiences increasing with the more sensitive profile items. Of those willing to disclose the more sensitive information (phone numbers and addresses) on Facebook, only in rare cases—such as religion and political preference—was the preferred audience more permissive than friends. However, for less sensitive profile items such as gender, personal preferences and posted photos, participants reported varying audience preferences.

In addition to simply asking what the desired setting would be, I asked questions to attempt to better characterize that profile item. Participants used a slider to respond

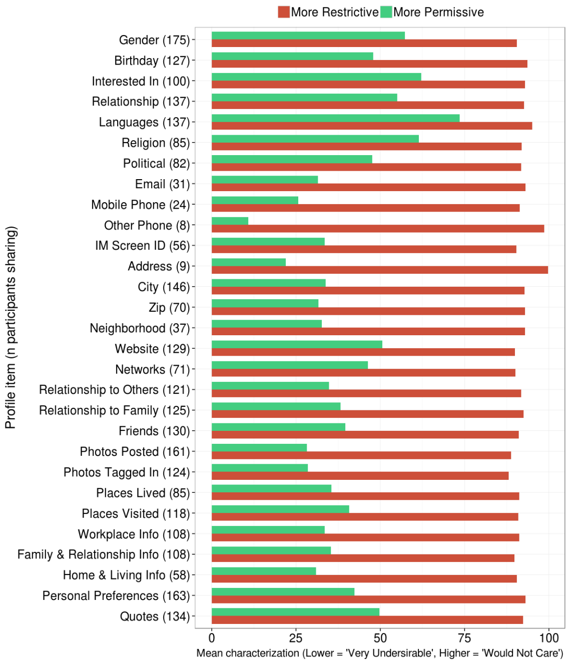


Figure 12: Reactions for changes to alternate audiences for profile items ordered as they appeared in the questionnaire.

with an interval value between 0 and 100 to characterize how undesirable it would be if they discovered the item was disclosed to the remaining audience choices. The average of these characterizations for profile items that participants were willing to disclose are shown in Figure 12. I divided the reported values for choices that were more restrictive and more permissive relative to the audience selected as the preferred choice. For more restrictive audiences, participants would be reacting to the potential that people they wanted to view a profile item would not be able to. For more permissive audiences, participants are expressing potential reaction to over-sharing with more users being able to access the information than desired. Participants reported neutral reactions to any audience that was more restrictive for all profile items. More permissive audiences were reported as moderately undesirable in most cases.

The items in Figure 12 are listed in the order presented to the participant in the survey. Some reported values for the seemingly less sensitive profile items toward the end of the survey were lower and could represent a bias concern from previous profile items that were more sensitive.

5.5 Comparing Policies

The survey described in Section 5.3 provided data to test how well different policies fit the reported user preference. In order to compare policies, I randomly divided the sample into a larger training set of participants and used the remaining participants as a test set. I then created four policies to test how well each policy fit as a default policy for the participants in the test set. For the Optimal and Mode policies, I used the training set of participants to derive a choice for each profile item. The Optimal policy used the participants' answers from profile item questions about audiences reactions to generate settings for profile items; the algorithm is described below. The Mode policy represents the most popular audience decision for all participants in the training set. The data were collected after privacy related questions and I determined that the optimal preferences might represent a somewhat restrictive policy, so I chose to include the most restrictive policy choice to compare with the Mode and Optimal policies. I also included another policy for comparison that represented the actual Facebook default settings to represent a real-world permissive default setting policy. The Restrictive and Facebook policies disregarded the training set and used the same set of randomly selected test participants for consistent comparison with all models.

5.5.1 Calculating an Optimal Policy

The training set data were used to determine the default choice for each profile item characterized as the most acceptable for all users in the training set. These choices were combined to form an optimal policy to predict acceptable settings for the sample participant responses in the test set. I calculated optimal privacy settings similar to the naive polytomous privacy scores used by Liu and Terzi [59]. Liu and Terzi used probabilities to calculate profile item sensitivity, however, in my study I gathered self reported user reaction to each possible alternative audience choice, which is an indication of users' views on item sensitivity. Thus, the probabilities were replaced with actual audience characterizations recorded from user responses and represented as a utility score for each option. An optimal policy was thus calculated by combining all participants' utility scores in the training set using the following method:

For each profile item $p \in P$ in an online social network profile,

$$P = \{name, birthday, ..., quotes\}$$

the participant chose an audience preference d from a set

$$D = \{only\ me, friends, friends\ of\ friends, everyone\}$$

The chosen preference was assigned a full utility x of 100. The alternative audience options $d \in D$ from the participant's answers using the sliders shown in Figure 9, became the utility values X_d (between 0 and 100, with 100 being "Would Not Care") for each alternative. Adding X_d for each of the four profile audience options across all participants in the training set represented the collective utility for the options. The largest of the collective utility values became the optimal audience decision o_p for that profile item such that:

$$o_p = max(\forall d \in D, \sum_{i=1}^{n} X_{di})$$

All of the optimal decisions represented an optimal policy

$$O_p = o_p \mid p \in P$$

In this study, I compared four different policies. The Optimal policy based on the training community was considered the first treatment. The training or community set was also used to calculate the second treatment condition by simply iterating through all training participants and using the mode of audience choices for each profile item. The third treatment policy was a highly Restrictive policy and consisted of the "Only Me" audience for each profile item. Finally, the actual Facebook default policy was the fourth treatment for the within-subjects variance analysis as described below [2].

5.5.2 Calculating Policy Fit

The dependant variable for the policy comparison was a fit score generated by assessing how well each treatment policy fit each participant's audience choice or utility for alternative audiences. For example, using the estimated values of the choices in Figure 9, this participant chose to disclose the "Gender" profile item to the audience "Friends of Friends" and assigned utilities for "Only Me" (90), "Friends" (75) and

[2] As of January 2014 using a new Facebook account and recording each default privacy setting.

"Everyone" (10). Suppose the treatment policy choices were: Optimal ("Friends"), Mode ("Everyone"), Restrictive ("Only Me") and Facebook ("Everyone"), then the assigned fit score for this participant would be: Optimal (75), Mode (10), Restrictive (90) and Facebook (10). Thus, for this participant and profile item, the Restrictive treatment default policy was the better fit. The individual fit scores for all items were combined to represent an overall fit score for the entire policy and the highest value is the best fit for that participant's privacy setting defaults. Overall policy fit scores had possible values from 0 (no disclosure or disclosure with no correct policy choices combined with undesirable characterization) to 2900 (disclosure for all 29 items and correct policy choices or neutral characterizations for all items). For comparisons, I divided the total fit score by the number of shared items resulting in a number between 0 and 100.

During the questionnaire, I asked the participants who chose not to disclose a profile item to consider the audience and alternatives if they were to disclose. For the fit score, I discarded any profile item the participant chose not to disclose and the overall fit score was a combination of only the profile items that would be disclosed on Facebook. For example, if a participant responded they would never share their "Address" on Facebook, that item was ignored when the overall fit was calculated. While I could potentially utilize the hypothetical answers to the audience characterizations, those tended to be quite restrictive as users often did not desire to share that information with anyone.

The participant fit scores were not normally distributed for any treatment condition. The overall fit scores were evaluated using a Friedman's test on the four related treatments. I hypothesized that the median fit scores for the treatment models would be significantly different:

$$H_0 : \theta_{Opt} = \theta_{Res} = \theta_{Mode} = \theta_{Face}$$

$$H_1 : \textit{At least one treatment population median will differ from another treatment population median}$$

For pairwise post-hoc analysis between groups, I conducted Wilcoxon signed-rank tests with a Bonferroni correction applied, resulting in a significance level at $p < .008$. Effect sizes were calculated for each post-hoc pairwise analysis result using Cohen's r [23, 24].

5.5.3 Results

Policy Settings: Table 2 lists the policies that were calculated and compared. While the Restrictive policy obviously differs vastly from the others, the Mode and Optimal policies also differ for many items. Interestingly, the Optimal policy is "Friends" for all profile items except for three items even though the Mode is more permissive. This is likely because the study participants reported stronger negative reactions to over disclosure than to under disclosure, resulting in the trained policy erring towards restricting items. I discuss the implications of this later.

Fit Variance: The training set was only used to calculate the Optimal and Mode policies, however, the same test set of participants was used to derive fit scores for all models. To determine the size of the test set, I estimated a Cohen's d medium

Table 2: Privacy settings for each test model.

Item	Facebook	Mode	Optimal	Restrictive	Item	Facebook	Mode	Optimal	Restrictive
Gender	EO	EO	Fr	OM	Website	EO	EO	Fr	OM
Birthday	FoF	Fr	Fr	OM	Networks	EO	Fr	Fr	OM
Interested In	EO	EO	Fr	OM	Relationship to Others	EO	Fr	Fr	OM
Relationship	EO	Fr	Fr	OM	Relationship to Family	EO	Fr	Fr	OM
Languages	EO	EO	Fr	OM	Friends	EO	Fr	Fr	OM
Religion	FoF	EO	Fr	OM	Photos Posted	EO	Fr	Fr	OM
Political	FoF	EO	Fr	OM	Photos Tagged In	EO	Fr	Fr	OM
Email	Fr	Fr	OM	OM	Places Lived	EO	Fr	Fr	OM
Mobile Phone	Fr	Fr	Fr	OM	Places Visited	EO	Fr	Fr	OM
Other Phone	Fr	Fr	OM	OM	Workplace Info	EO	Fr	Fr	OM
IM Screen ID	Fr	Fr	Fr	OM	Family & Relationship Info	EO	Fr	Fr	OM
Address	Fr	Fr	OM	OM	Home & Living Info	EO	Fr	Fr	OM
City	Fr	Fr	Fr	OM	Personal Preferences	Fr	Fr	Fr	OM
Zip	Fr	Fr	Fr	OM	Quotes	EO	EO	Fr	OM
Neighborhood	Fr	Fr	Fr	OM					

Only Me (OM), Friends (Fr), Friends of Friends (FoF), Everyone (EO)

effect size ($d = .49$). Compensating for multiple post-hoc comparisons, I estimated a test sample size of ($n = 51$) in order to achieve at least .80 statistical power [24]. The sample size estimation was evaluated before data collection and therefore based on parametric tests. After the data were collected and I discovered the fit scores violated a normal distribution assumption, I used non-parametric statistical tests to analyze variance. However, Tanizaki showed in a series of Monte Carlo experiments that Wilcoxon non-parametric tests have similar or more power than *t*-tests when the underlying distribution is non-normal [92].

I conducted a Friedman test to compare differences between the fit score medians of the four treatments: Optimal ($median = 99.39$), Mode ($median = 89.75$), Restrictive ($median = 96.08$) and Facebook ($median = 73.43$). The test was significant $\chi^2(3, n = 51) = 56.98, p < .001$ and the Kindall's coefficient of concordance ($W = .558$) indicated strong variance between treatments, and resulted in rejecting the null hypothesis $H_0 : \theta_{Opt} = \theta_{Res} = \theta_{Mode} = \theta_{Face}$.

To further examine differences between groups, I conducted six post-hoc pairwise

Table 3: Comparison of model fit score variance effect sizes.

Model		**Trained**	**Mode**	**Restrictive**	**Facbook**
	Md	**Effect Size (Cohen's r)**			
Trained	99.39				
Mode	89.75	**.5847*****			
Restrictive	96.08	**.4115*****	.0826		
Facbook	73.43	**.7973*****	**.7895*****	**.6025*****	

*** **Significant at** $p < .001$

comparisons using Wilcoxon tests with a Bonferroni adjustment ($p < .008$). Pairwise comparison results are displayed in Table 3. The Optimal median was significantly greater than all three other conditions, Mode ($p < .001, r = .58$), Restrictive ($p = .003, r = .41$) and Facebook ($p < .001, r = .80$). Mode and Restrictive medians were not significantly different ($p = .6, r = .08$). Both Mode ($p < .001, r = .79$) and Restrictive ($p < .001, r = .60$) medians were significantly larger than the Facebook treatment. Thus, I found statistically significant differences between the policies, with the Optimal policy representing the larger fit scores and Facebook's current policy being the lowest fit. Interestingly, despite being very different policies, the Mode and Restrictive fit scores were not significantly different.

5.6 Additional Exploration

The statistical analysis only evaluated the models at a fit training set size ($n = 133$). Thus, it was not clear how the training set size affects the variance between the different model fit scores. With evidence of significant variance at ($n = 133$), I wanted to evaluate what the minimum training set size might be to produce higher fit scores with the Optimal model. I also wanted to determine if the training set size affected fit scores with the other static models. To capture this, I ran the fit algorithm

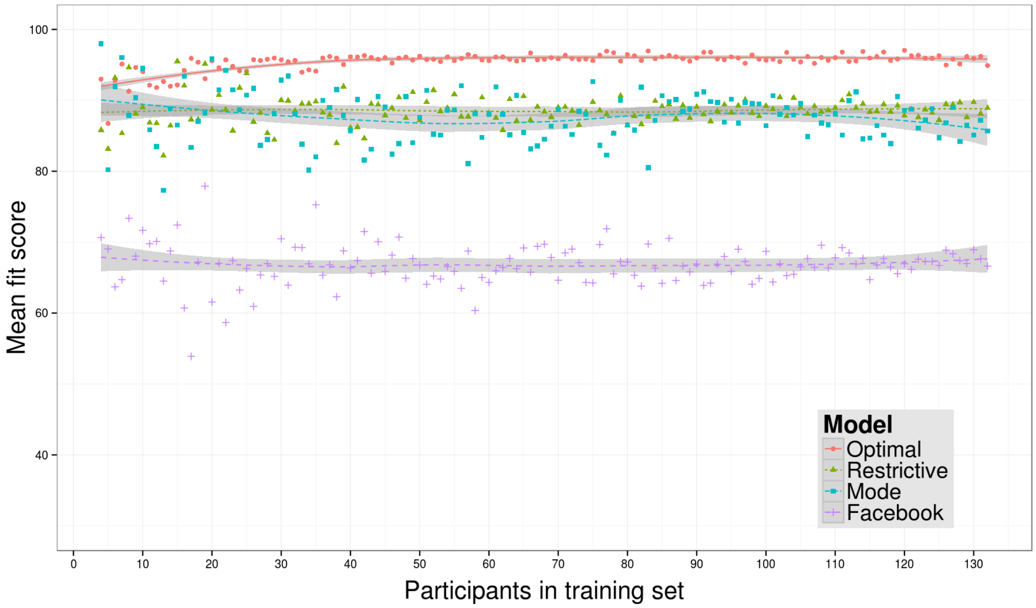


Figure 13: Model comparison of mean fit scores for varying training set sizes.

for every training set size from ($n = 4$) to ($n = 133$). The results of this analysis are shown in Figure 13. In each case represented in Figure 13, the participants were randomly split into the varying group sizes. Data item values represent the mean fit score for all participants in the test group.

Not surprisingly, the fit scores for the Optimal model have more variation with a smaller number of participants in the training set. However, as the number of training participants reached about 40, the Optimal model produced slightly higher and more consistent scores with less variation than the other models. Restrictive policy fits were close but more often slightly higher than the Mode mean fits. Facebook model mean fits were vastly lower compared to the differences between the other three models. Mode mean fits were inconsistent across the entire range of training sets and Facebook and Restrictive became less consistent with a smaller test size likely representing larger fit score variance across participants with those models. With a surprisingly small training set size ($n > 40$), the Optimal model scores appeared to corroborate the statistical analysis results for the post-hoc pairwise comparisons made earlier with a fixed training set size of ($n = 133$). Thus, the number of test set participants derived from the power calculation would not likely change the results of the statistical analysis provided the test set size was larger. The Facebook and Restrictive static policies were moderately consistent for all training set sizes.

5.6.1 Segmentation

Optimal policy fit scores were high and fairly consistent with enough data available in the training set, however, I wanted to explore if this could be improved by using a set of canonical policies based on different segmentation models. To further evaluate using privacy segmentation, I created additional policies using training data with sample sets segmented by privacy attitude and Facebook usage. During the survey, I asked questions from three different scales or indexes. For each of the segmentation methods, the training and test sets were segmented using the responses to the respective questions. The Westin/Harris responses were evaluated for each participant and segmented into categories (Pragmatists, Fundamentalist and Unconcerned) based on agreement or disagreement. I calculated index scores for the Facebook Intensity scale and the Buchanan index. For these indexes, the privacy attitude or behavior was characterized by the value of index scores. To segment participants with these scales, I also divided the participants into three groups (Low, Average and High), with the “Average” being from -1 standard deviation from the mean to $+1$ standard deviation from the mean. The “Low” and “High” groups were the participants with scores

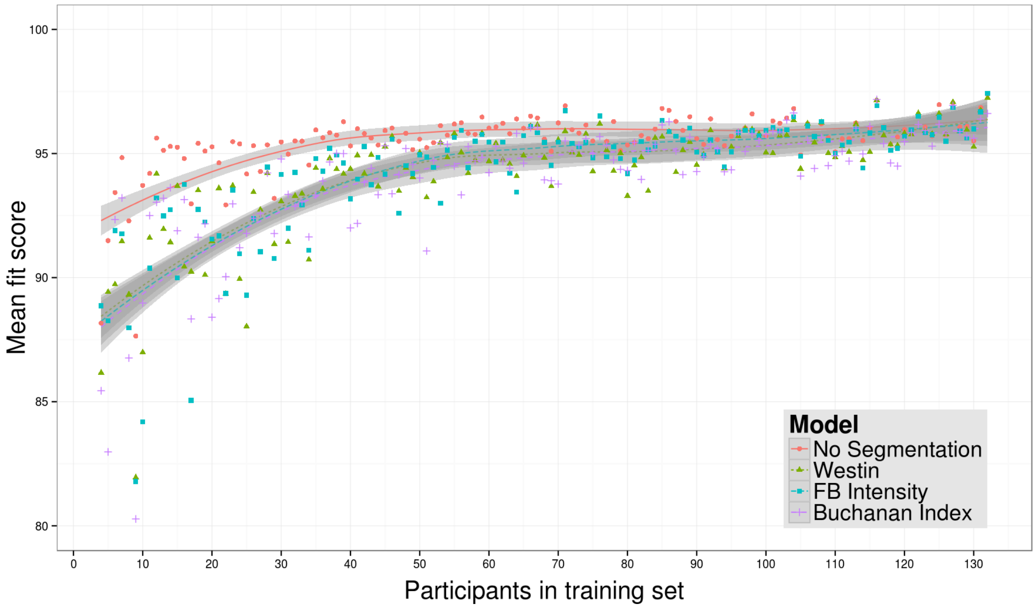


Figure 14: Segmentation model comparison of mean fit scores for varying training set sizes.

beyond the single standard deviation from the means.

I segmented both the training and test sets using the same criteria. The training set was used to calculate an optimal policy for each segment using the method in Section 5.5.1. To calculate the fit score for the segmentation policies, I applied the optimal policy representative of the test participant's segment.

For evaluation purposes, I also included the non segmented trained policy used in the statistical variance analysis to compare with the three different optimal segmentation models. This policy became a control to evaluate the differences, if any, between the segmentation models. I used the same secondary analysis described previously with varying training set sizes to produce fit scores for the control and segmentation policy fits.

Figure 14 shows the mean fit scores for all test participants for training set sizes from ($n = 4$) to ($n = 133$). To evaluate the effects of the segmentation, I included an optimal fit model with no participant segmentation for the training or test participants. All segmentation models performed equally well. Figure 14's y-axis was adjusted from $80 - 100$ to highlight small differences between the non-segmented optimal model and the models that used segmentation. Segmentation model fit scores were slightly lower with small training sets, but began to mirror the non-segmented optimal model with > 90 participants. This difference in mean scores likely represented the effect of dividing the training and test sets into segments, which did not perform well until the segments were sufficiently large. In reviewing the resulting policies, segmented policies were often very similar as long as there was sufficient data in the segment. These results indicate no improvement in fit scores for any segmentation method.

5.7 Limitations

Privacy attitude is difficult to define and measure and this study suffers from limitations associated with this challenge. Participants reported privacy attitudes in a context that lacked any of the incentives for social interaction, which may introduce a bias toward more restrictive privacy preferences. For example, participants reported neutral reactions to more restrictive audiences, but restricting information to "Only Me" is rarely useful, and would likely be less desirable than was reported by participants in this study. This survey may have also introduced some ordering effects. The question order is reflected in Figure 12. The characterization values for more permissive audiences seemed generally lower after asking about some of the more sensitive profile items such as phone numbers and address. Responses to more private profile items could have inadvertently caused participants to respond more conservatively to less sensitive profile items asked later in the questionnaire.

Participants in this study responded with a reaction to a change in audience with an interval slider from 0 – 100 with 0 being "Very Undesirable" and 100 being "Would Not Care." The chosen audience was also assigned a value of 100. This did not weight the chosen preference any higher than "Would Not Care" characterizations in calculating the optimal policy or determining fit. The chosen preference could be given more weight, which would also result in lower fit scores and less restrictive policies. Also, the calculations did not account for the cost or effort associated with the user having to adjust settings to the more desired audience—which should also be taken into account if similar methods were used to create defaults.

The segmentation of participants did not result in any improvements in this study. However, adjusting the calculations to address the above limitations may result in more room for improvement over the optimal policy. In addition, the segmented samples were rather small and a larger sample may improve these results. These results simply add to other findings that so far, segmentation has not been shown to be useful for learning such privacy settings.

5.8 Discussion

This survey indicates that users do have differing privacy preferences, particularly for personal information considered less sensitive. Facebook's current default policy is permissive and does not match closely with users' reported privacy attitudes. Despite these differences, the policy comparison indicates that I can calculate defaults to better match reported user preferences. I explored not only using the stated preference, but also the attitude towards alternative settings to calculate a policy that generates the highest satisfaction across users. This choice has several interesting implications.

The optimal policy was based upon the same assumption as the fit evaluation—both were calculated from the "utility" score from participants. Thus, this policy resulting in the best fit over the test set of participants was not surprising. However, examining the differences and similarities across the policies reveals insights into various methods. While the mode choice better matched the stated preference for more users, over multiple iterations the fit scores showed inconsistency and would cause more users to be unhappy with that default setting. Interestingly, the Optimal policy was almost entirely a "friends-only" policy. For a time, Facebook had a "friends-only" global setting, which was a common and simple option users chose [91]. The results for the Optimal policy imply that was a reasonable option for many users, and it may be useful to resurrect a global "friends-only" privacy setting.

Interestingly, the fit score of the Restricted policy was also quite high. This demonstrated a limitation in how the participants characterized alternative audience choices. People reported being very tolerant to unmatched policy decisions if the decision change was to a more restrictive audience. Thus, default policies formed from reported privacy preferences may naturally err with more restrictive audience choices. Not every profile item was characterized the same; some had high disclosure rates while other items were reportedly disclosed by only a few people. By gathering information that characterizes the sensitivity of profile items, default policies can use this to select more restrictive audiences for those users that decide to disclose. This has the benefit of defaults providing additional privacy protections, but there is little social utility for posting personal information that is never shared. Thus, while an "Only Me" default may not concern most users, it may not be useful for social interaction. Similarly, if a default setting is more restrictive than the user preference, but the user does not mind the restrictive setting, they are less likely to change it. Often, users modify settings after a privacy intrusion; more restrictive defaults may reduce unintended disclosure because users will only modify settings when information is truly needed by additional people. While this may better follow the principle of least privilege and result in fewer privacy intrusions, it will also result in information being shared less widely than users are comfortable with and possibly reduce the value of the site.

The low fit scores for the Facebook default policy highlighted the privacy paradox with reported privacy preferences. People socialize and share information with online social communities, but report cautious sharing behavior. Thus, if people want to actually engage in more sharing, a more restrictive policy may increase effort. However, all of the data collected in this study was based on reported privacy preferences and the fit scores were generated from the same data. If training data were based on privacy behaviors, or better captured sharing desires, the optimal policies might be less private and more closely resemble the Facebook default policy. The results here showed the optimal policy calculated from training data with profile item characterizations for different audiences provided better fit scores over Mode and Restrictive policy fits. Even if the underlying data were to change and the fit scores appear different, the observation of more consistent average fit scores should improve the fit for the default policy.

A notable design implication from these results is that most policy configuration mechanisms lack capabilities to gather additional reaction information to better characterize profile items as I did in the survey. Additional information for every profile item increases profile complexity and adds configuration burden. It remains unclear if the cost of gathering the additional information to generate better default policies would be greater than the reduction of burden achieved by those policies. However, the results here showed an improvement with a small community size—possibly as few as 40 people might be enough to improve default settings for even larger populations. Designs intended to improve complex policies would be more effective if they limited the number of people used for training data to better characterize profile items.

The results of the segmentation model reflected the known difficulties of privacy attitudes and segmentation. Privacy attitudes are complex and difficult to understand, and privacy behaviors are contextual. Segmentation models like Westin/Harris lack structure to account for differing contextual privacy attitudes that often exists within online social networks. The Facebook Intensity scale [34] measures Facebook usage and connectedness to the Facebook community, but people who are very active in online social networks may also have very different privacy attitudes. The Buchanan index includes questions about more modern technologies, but Buchanan et al. [19] admittedly failed to capture different dimensions of privacy attitudes on Facebook. While the segmentation models I tested did not improve fit scores, segmentation based upon attitudes that are more relevant to social media, or on actual history of behavior, may still be worth exploring.

The segmentation techniques used for the index scores were simple deviations from the mean score. More sophisticated supervised machine learning techniques may improve segmentation, especially over time, but the training sets would need to be larger. The differences with segmentation models in this set were very small and may be improved with larger community sizes and/or better segmentation techniques. It is also possible that the privacy attitude measurement techniques are not adequate enough for any segmentation function to match user privacy preferences. Future research is necessary to explore how these might be used to improve optimal privacy policy fit. If successful, the burden of answering segmentation questions still needs to be less than the burden of customizing the settings for segmentation to be useful.

5.9 Conclusion

In this chapter, I explored using audience characterizations for SNS profile items to create a better default privacy policy. Audience characterization utility values were used to train an optimal policy from a training set and then determine how well different policies fit for a group of test participants. While gathering additional information from users required additional burden, I showed that an improvement in default settings can occur with as few as 40 people. While the algorithm may be improved upon, I believe this demonstrates that sites could better take into account user preferences without large amounts of user effort and community data. I further explored using privacy attitude segmentation to evaluate if privacy policies by attitude may improve fits, although these results were not beneficial.

Participants responded to the potential exposure of profile items to alternate audiences from the prefered disclosure audience. These results indicated that user reactions were neutral for audiences that were more restrictive, but negative for those more permissive than the preferred setting. All policy fit scores accounted for this and the Restrictive policy seemed to benefit from this neutral reaction while the Facebook permissive policy reflected this with lower fit scores. Thus, the fit score itself may not portray a completely accurate representation of how a policy matched actual user needs, but I believe is an improvement over simply measuring accuracy against just the single preferred setting. I believe these results suggest methods for improving a default policy that reduces overall effort for configuring complex privacy settings. The user privacy attitudes for profile sharing in this chapter seemed to reflect that more restrictive settings may represent an adequate starting place for users to later configure to actual preference, which at the same time is more privacy preserving than current policies often are. The results also suggest that utilizing user reaction to different audience choices may be useful in determining such default policies, especially if the limitations are addressed. While this work demonstrates how additional audience characterizations can be used for common social network audiences, I believe the concept can be extended to more granular audiences such as friend lists or circles, as well as additional types of settings beyond the ones I surveyed.

Future work can improve these findings by exploring the burden associated with gathering user reaction to alternate audiences. Additional analysis could be done with this or similar datasets to see if there are other factors that determine the impact or different weights of the audience characterizations. In particular, data from user reported preferences can be combined with actual social activity to possibly balance the privacy paradox problem. Online social network interaction is dynamic and default settings are applicable to each new social interaction. Thus, more work is needed to examine how users would actually respond to such defaults, and how much effort it would take to re-configure settings for poorly predicted default settings. Complex privacy settings continue to require excessive configuration burden and future research should explore novel methods for minimizing effort needed to manage online privacy.

CHAPTER 6: CONTRIBUTIONS AND CONCLUSION

Technology is enabling people to share more information than ever before. Privacy regulation becomes more complicated to manage when people socialize online. People have different social groups and desire to share appropriately with these groups. Most social networking sites provide adequate levels of privacy control, however the mechanisms are difficult to use. Because privacy is a secondary task, many people struggle to manage settings that represent their desired privacy attitudes. This can often result in unintended disclosure and cause embarrassing and sometimes dangerous consequences. Thus, privacy management is increasingly important as more people adopt sharing information online.

Additional social network features promote more sharing of personal information, however, the additional features come with more privacy controls. People desire to socialize online and control who sees their personal information. However, if privacy configuration creates excessive burden, users of online social networks may choose to only disclose information intended for a public audience. When people make sharing decisions based on either public disclosure or nondisclosure, the overall quality of online social interaction is diminished.

The research in this dissertation improved knowledge of how using audience-centric design can improve user understanding of information disclosure. However, using audience-centric design may increase already complex privacy configurations. Excessive configuration burden for secondary tasks discourages use of privacy controls even when people desire to share with appropriate audiences. I also presented research in this dissertation that improves understanding of how automated privacy changes can be used to reduce configuration burden. Profile default privacy settings are initially configured by online social network site developers and may not represent preferred/optimal privacy behaviors or user attitudes. Data from other users in a community can be used to configure default settings for other users that better match their privacy attitude. Community feedback from these data may create policies that better match user preference and reduce the number of configuration changes needed to represent a user's optimal privacy policy.

6.1 Audience-Centric Design

This dissertation includes research that explored using audience-centric design to improve user understanding of profile information disclosed using online social network sites. First, I presented a study that compared differences in configuring desired privacy preferences with privacy configuration mechanisms used by a popular online social network site and an audience-centric prototype design called AudienceView. I then compared AudienceView with another audience-centric prototype design—Expandable Grids. Expandable Grids represented a more compact visual mechanism that used a grid to display audiences and profile items to configure access to personal information. Finally, I qualitatively explored how users perceive and interact with Google+ circles, a currently deployed audience-centric privacy control mechanism.

AudienceView is an audience-centric privacy configuration mechanism designed to more closely integrate privacy management with the primary task of socializing using online social networks. I compared AudienceView with Facebook's privacy configuration interface to determine if the prototype improved user understanding and confidence for appropriate audience disclosure of personal information. At the time of the study, Facebook's privacy mechanisms were difficult to use and users struggled to understand who could view information they posted on the site. The excessive configuration burden coupled with diminished understanding resulted in unintended disclosure of personal information and privacy configurations that did not match user preference. The results from the comparison showed users reported more confidence in understanding audience disclosure using AudienceView than reported confidence using Facebook's privacy configuration mechanisms. AudienceView increased visual feedback by providing privacy setting indicators beside user profile information in the primary profile view. This increased visual feedback improved user confidence in understanding audience disclosure of profile items. Facebook has since included features that allow users to view their profile from another audience perspective and privacy configuration mechanisms that are more closely integrated to the main profile items. Similar to AudienceView, these new controls placed the access configuration mechanism next to the profile data items. However, AudienceView allowed users to view the profile data from the perspective of audiences and Facebook's current mechanism can only be used to view timeline settings from either public or a single friend's perspective. If these new features are used, Facebook users may benefit from some improved understanding, but it may be difficult to connect a single friend to audience groups used for selective disclosures of personal information.

AudienceView expanded the visual representation of privacy settings to accompany the profile items in the primary profile view. Other research has shown to reduce burden for complex settings with other more compact mechanisms. The Expandable Grids prototype used a grid mechanism to reduce burden to configure complex access control to file system objects. More visual systems often reduce cognitive burden of mapping the effective change of a privacy setting, but may increase the amount of clicks and mouse movement to configure settings. Compact systems like Expandable Grids reduce the amount of effort needed to configure a policy, but lack visual feedback representing what happens when a privacy change occurs. I conducted a study to compare these two different methods of improving privacy setting configuration. The results indicated that both mechanisms improve usability for configuring complex privacy settings and the user preference for the different representations was highly subjective. Thus, providing the user with both compact and visual mechanisms may prove to further enhance understanding of audience access to profile information. Facebook currently has adopted a more expanded and visual approach for configuration with no option to configure privacy with a more compact or overview method. Future research may provide useful insight in how people react to having both design methods available for privacy setting configuration.

People use Google+ circles to group their friends into social categories and then share posts to circles as a way to control disclosure to intended audiences. I developed research to better understand how people reacted to the introduction of a usable audience-centric sharing mechanism. Results from the study found that people understood the intended purpose of circles, yet their social behavior did not represent their stated desires to appropriately disclose to multiple audiences. Instead, people seemed to simply share to all circles or collapse their entire friend network into a single circle. Thus, early users of Google+ did not take advantage of an audience-centric configuration utility. It was unclear if the additional burden needed to create the distinct social groups provided any significant advantage in understanding or privacy management. However, the results of this study were representative of early users of Google+ and people mentioned the lack of users as a reason for not using circles. As Google+ has increased in subscribers and usage, the benefits of using circles may eventually provide improved understanding of information disclosure to multiple audiences.

This thorough analysis of using audience-centric mechanisms highlighted a significant problem with the growing complexity of privacy settings. Discrete sharing of personal information increased the cognitive burden for users to create audiences and make disclosure decisions with each shared item of information. Privacy settings were already complex and difficult to manage and increases in burden would likely lead to users adopting mitigating tactics to avoid configuration burden, such as only sharing to a public audience. Many of these tactics reduce the quality of online social interaction. To reduce configuration burden, I suggested using community feedback to create privacy settings that may better represent users' privacy attitudes.

6.2 Community Feedback

Online social network sites benefit from a wealth of community data including privacy configurations and sharing decisions. Feedback from this information is used for advertisements and recommending books and other activities. My research evaluates the possibility of using similar community feedback to automate changes in privacy settings. Automated changes that better represent a person's privacy attitude should reduce the configuration changes need to achieve an optimal privacy policy. In this dissertation, I presented research that explored user reactions to automated privacy changes. These results informed a quantitative evaluation of creating default settings from other user preferences within a community set.

First, I explored how people reacted to automated changes in privacy settings. Automated changes may technically reduce user configuration burden, but people may react negatively to the change. The results from my study indicated people wanted notification and consent for changes in privacy settings. However, the reaction was not the same for all profile items. Some items were considered less sensitive and people only characterized negative reactions to more sensitive profile items. Additionally, many users were cautious social network users and only posted profile information meant for disclosure to a public audience. In interviews, people responded negatively to hypothetical situations where privacy settings were automatically changed, however, during observation, few participants responded with concern to a perceived actual change in privacy settings. This study provided greater understanding in the complexity of user privacy attitudes and how people react to automated changes.

Privacy default settings for online social network profile information are often permissive to large audiences. Social network sites' primary purpose are to facilitate social connections and discover new acquaintances. Restrictive privacy settings might constrict social interaction, especially for a large public audience. However, excessive privacy configuration burden can force people to only disclose information intended for a public audience and thereby limit the effective online social interaction. I explored using community feedback to create default privacy settings as a possible method to achieve a balance by generating privacy policies that better match users' attitudes. In terms of privacy, people characterize profile items differently. I developed a study that characterized data items by gathering user response to audience changes for each profile item. Using these responses, I calculated how well a privacy setting policy fit the user preference. The study results showed default privacy settings formed from community feedback better fit user preference than Facebook's current default settings.

Privacy attitudes are complex and difficult to measure, however, segmentation on privacy attitude may provide a better privacy policy fit. I used previously established research metrics to measure privacy attitude and segment sample populations. Segmented results showed similar improvement in policy fit to nonsegmented community feedback results. However, the training sets for segmentation were small and larger community size may eventually improve the default privacy setting fit.

The results from the two community feedback studies have implicitly described a process for automating changes in privacy settings. Figure 15 represents a conceptual process of how community data can be used to refine a user's privacy policy. The process model provides an example process for using a community data store as feedback to improve complex privacy settings. The figure more visually describes a process of combining multiple facets of community data to improve privacy defaults and other automated changes in privacy settings.

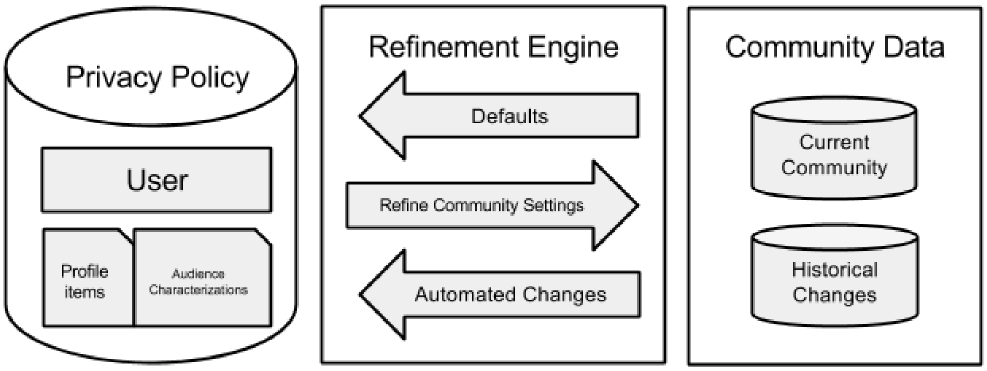


Figure 15: A process model showing how community feedback is used to enhance privacy settings.

The process shown in Figure 15 is composed of three components: community data, a refinement engine and a privacy policy. The policy consists of access control rules for a set of profile items. Access control rules are composed of a setting and the level of access allowed to an audience. In addition to the rules, audience characterizations are collected from the user to better understand the sensitivity of the profile item. The user is included in the privacy policy to indicate some level of user feedback such as notification or consent needed for automated changes as informed by the study in Chapter 4.

The refinement engine has several smaller components. The engine receives requests and formulates a response that either informs the privacy policy or provides refinement information to the community data. This component uses community feedback to inform better decisions for individual settings. For new community members, the engine determines how to deliver enhanced default settings. Chapter 5 results validate the process of providing enhanced default settings. As members of the social community modify or change privacy settings, this refinement engine uses those decisions and stores them as part of the community data. Over time, the refinement engine detects possible changes in privacy policies that may better reflect the user preference. These changes are passed to the privacy policy in the form of automated privacy changes and the user is informed based on the notification process defined by the privacy policy.

The model intends to include methods derived from collective behavior theory presented in Chapter 2. Most current community feedback methods such as social navigation and recommender systems rely on the current state of community data. Collective behavior theory describes the ongoing behavior of collectivities. Thus, the community data part of the process is intended to store both the current state of community privacy settings and historical changes made to privacy settings over time. Historical changes are monitored to detect collective behavior events that can be passed to the refinement engine for determining how to provide the feedback to users' privacy policies. The research in this dissertation explores a few aspects of this process model. Chapter 4 explored how users react to automated changes. From these results, I determined that the "User" part of the process should include some level of notification or consent. More sensitive profile items such as photos generated stronger negative user reactions. Thus, the refinement engine should consider item sensitivity when implementing an automated change. Results from Chapter 5 explored using profile items more fully characterized by exposure to different audiences to help determine better default privacy settings. These results informed both the "Privacy Policy" and the "Refinement Engine" areas of the process model. Audience characterizations were used from a community set to provide a starting privacy policy that better matches user preference. These contributions represent steps to better understanding the process for using community feedback to enhance privacy settings. Future research is needed to fully explore all components of the process for using community feedback to continuously refine complex privacy settings and reduce user configuration burden.

6.3 Contribution

Audience-centric designs can improve understanding of information flow by providing users with a view of their personal information from the perspective of different social groups. However, this improvement in understanding fails to significantly reduce configuration burden. Providing community feedback reduces user burden with complex settings. In this dissertation, I document research that contributes to understanding how audience-centric design and community feedback can be used to enhance default privacy settings. Specifically, I provide the following overall contribution to current research in three areas:

- A comprehensive review of previous privacy theory and work related to managing complex settings.
- Audience-centric design
    - Research that suggests using audience-centric designs improve user understanding and comfort.
    - Research that examines a comparison of two different audience-centric design methods and suggests both are usable and equally preferred.

  - Research that explores how early adopters of a new audience-centric online social media site react to sharing with audience-centric designs.

- Community feedback

  - Research that examines user reactions to automated changes in privacy settings.
  - Research that explores using community enhanced default privacy policies to reduce the user burden required to configure complex privacy settings.

The contributions above represent a significant addition to the existing body of research in usable privacy and security. Complex privacy settings are a secondary task and reduced user burden for configuring privacy settings is key to helping people successfully manage privacy in a new world of online socializing. If privacy configuration burden is high, users either avoid privacy management and suffer from unintended disclosure or only choose to disclose information intended for a public audience. This reduces the quality of online social interaction and diminishes the purpose of online social networks. The research I provide in this dissertation improves understanding in using improved visual feedback in the form of audience-centric design and reducing privacy setting configuration burden can be used to help users manage complex privacy settings.

6.4 Conclusion

Privacy settings have been too difficult for too long. Online social networks are becoming more relevant today as more people engage in sharing. New features provide new ways to share and friend groups become larger and more difficult to manage. Creating new audience groups for sharing coupled with many new methods for sharing have resulted in very complex privacy settings. Managing privacy is secondary to socializing online and this further discourages people from spending time to configure privacy to match their privacy attitude. In 2011, Mark Zuckerberg, co-founder and CEO of Facebook.com commented:

> When I built the first version of Facebook, almost nobody I knew wanted a public page on the internet. That seemed scary. But as long as they could make their page private, they felt safe sharing with their friends online. Control was key. With Facebook, for the first time, people had the tools they needed to do this. That's how Facebook became the world's biggest community online. We made it easy for people to feel comfortable sharing things about their real lives.
>
> We've added many new tools since then: sharing photos, creating groups, commenting on and liking your friends' posts and recently even listening to music or watching videos together. With each new tool, we've added new privacy controls to ensure that you continue to have complete control over who sees everything you share. Because of these tools and controls, most people share many more things today than they did a few years ago [1].

[1] *Our Commitment to the Facebook Community (November 29, 2011)* (accessed February 24, 2014); available from https://www.facebook.com/notes/10150378701937131.

This control technically exists on many online social network sites, however, the control is only effective if people are able to successfully configure and manage their privacy. Managing and sharing to multiple audiences increases cognitive burden and makes privacy settings more complex. This dissertation improves knowledge for improving online privacy understanding and management for multiple audiences. However, there is more research needed to understand how people have changed in an environment where privacy configuration has been difficult for several years.

A recent Pugh Internet survey shows that younger people are using entirely different social media venues for distinct audiences or contexts [2]. The same survey pointed out other strategies such as obfuscating the meaning of a private message within a broader context. These strategies are problematic as explained by a participant in my study in Chapter 4:

> *P19:"For example, if I were to write a joke on my friend's wall and it was like an inside joke, someone else would see it on the little feed right here. They might take it too seriously and won't understand, 'hey, this is just an inside joke between A and B' and then they'll see it and then jump on and it's like, 'we were having a joke with each other but way to make yourself seem like a jerk.' "*

This highlights user tactics that develop from trying to circumvent good access control mechanisms in online social networking. Usable privacy and security research attempts to provide understanding to avoid user circumventions of privacy and se-

[2] *Teens, Social Media, and Privacy (May 21, 2013)* (accessed January 30, 2014); available from http://pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy.aspx.

curity management. This dissertation seeks to contribute research that can be used to promote usable privacy management for online social network interactions. Hopefully, more research can build on this and improve usability for secondary tasks like privacy management and eventually help users share and socialize in an online world.

REFERENCES

[1] M. Abadi, M. Burrows, B. Lampson, and G. Plotkin. A calculus for access control in distributed systems. 15(4):706–734.

[2] M. Ackerman and S. Mainwaring. Privacy issues and human-computer interaction. In *Security and Usability: Designing Secure Systems that People Can Use*, pages 381–400. O'Reilly Media, Inc.

[3] A. Acquisti and R. Gross. Imagined communities awareness, information sharing, and privacy on the Facebook. In *Privacy Enhancing Technology.*

[4] I. Altman. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding.* Brooks-Cole Pub. Co.

[5] I. Altman. Privacy regulation: Culturally universal or culturally specific? 33(3):66–84.

[6] I. Altman. *Social Penetration: The Development of Interpersonal Relationships.* Holt, Rinehart and Winston.

[7] F. B. Baker and S.-H. Kim. *Item Response Theory: Parameter Estimation Techniques, Second Edition.* CRC Press.

[8] A. Besmer. Configuration of application permissions with contextual access control. Ph.D. Thesis.

[9] A. Besmer and H. Lipford. Tagged photos: concerns, perceptions, and protections. In *Proceedings of the 27th International Conference Extended Abstracts on Human Factors in Computing Systems*, CHI '09, pages 4585–4590.

[10] A. Besmer, J. Watson, and H. R. Lipford. The impact of social navigation on privacy policy configuration. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 1–10. ACM.

[11] S. Bikhchandani, D. Hirshleifer, and I. Welch. Learning from the behavior of others: Conformity, fads, and informational cascades. 12(3):151–170.

[12] H. Blumer. Collective behavior. In *New Outline of the Principles of Sociology*, pages 166–222. Barnes & Noble.

[13] d. boyd. Friends, friendsters, and myspace top 8: Writing community into being on social network sites. 11(2).

[14] d. boyd and J. Heer. Profiles as conversation: Networked identity performance on friendster. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, volume 3 of *HICSS '06*, pages 59c– 59c. IEEE.

[15] d. m. boyd and N. B. Ellison. Social network sites: Definition, history, and scholarship. 13(1):210–230.

[16] d. m. boyd and E. Hargittai. Facebook privacy settings: Who cares? 15(8):13–20.

[17] A. Braunstein, L. Granka, and J. Staddon. Indirect content privacy surveys: Measuring privacy without asking about it. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, SOUPS '11, page 1. ACM Press.

[18] R. Brown. Mass phenomena. 2:833–876.

[19] T. Buchanan, C. Paine, A. N. Joinson, and U.-D. Reips. Development of measures of online privacy concern and protection for use on the internet. 58(2):157–165.

[20] X. Cao and L. Iverson. Intentional access management: Making access control usable for end-users. In *Proceedings of the Second Symposium on Usable Privacy and Security*, SOUPS '06, page 2031. ACM.

[21] B. Carminati, E. Ferrari, and A. Perego. Enforcing access control in web-based social networks. 13(1):1–38.

[22] G. Chung and P. Dewan. Towards dynamic collaboration architectures. In *Proceedings of the 2004 ACM conference on Computer supported cooperative work*, CSCW '04, pages 1–10. ACM.

[23] J. Cohen. A coefficient of agreement for nominal scales. 20(1):37–46.

[24] J. Cohen. *Statistical Power Analysis for the Behavioral Sciences.* Psychology Press.

[25] S. Consolvo, I. E. Smith, T. Matthews, A. Lamarca, J. Tabert, and P. Powledge. Location disclosure to social relations: Why, when, & what people want to share. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, CHI '05, pages 81–90. ACM.

[26] L. F. Cranor, P. Guduru, and M. Arjula. User interfaces for privacy agents. 13(2):135–178.

[27] A. Dieberger, P. Dourish, K. Hook, P. Resnick, and A. Wexelblat. Social navigation: Techniques for building more usable systems. 7(6):36–45.

[28] P. DiGioia and P. Dourish. Social navigation as a model for usable security. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, SOUPS '05, pages 101–108. ACM.

[29] J. M. DiMicco and D. R. Millen. Identity management: Multiple presentations of self in Facebook. In *Proceedings of the 2007 International ACM Conference on Supporting Group Work*, GROUP '07, pages 383–386. ACM.

[30] T. Dinev and P. Hart. Internet privacy concerns and their antecedents—measurement validity and a regression model. 23(6):413–422.

[31] J. R. Dominick. Who do you think you are? Personal home pages and self-presentation on the world wide web. 76(4):646–658.

[32] P. Dourish and D. Redmiles. An approach to usable security based on event monitoring and visualization. In *Proceedings of the 2002 Workshop on New Security Paradigms*, NSPW '02, pages 75–81. ACM.

[33] S. Egelman, A. Oates, and S. Krishnamurthi. Oops, I did it again. In *Proceedings of the 2011 annual conference on Human factors in computing systems*, CHI '11, page 2295. ACM Press.

[34] N. B. Ellison, C. Steinfield, and C. Lampe. The benefits of Facebook "Friends:" Social capital and college students use of online social network sites. 12(4):1143–1168.

[35] L. Fang and K. LeFevre. Privacy wizards for social networking sites. In *Proceedings of the 19th international conference on World wide web*, WWW '10, pages 351–360. ACM.

[36] B. Friedman. Social judgments and technological innovation: Adolescents' understanding of property, privacy, and electronic information. 13(3):327–351.

[37] W. W. Gaver. The affordances of media spaces for collaboration. In *Proceedings of the 1992 ACM Conference on Computer-Supported Cooperative Work*, CSCW '92, pages 17–24. ACM.

[38] J. Goecks, W. K. Edwards, and E. D. Mynatt. Challenges in supporting end-user privacy and security management with social navigation. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, pages 1–12. ACM.

[39] J. Goecks and E. Mynatt. Supporting privacy management via community experience and expertise. pages 397–417.

[40] E. Goffman. *The Presentation of Self in Everyday Life.* Doubleday.

[41] D. Goldberg, D. Nichols, B. M. Oki, and D. Terry. Using collaborative filtering to weave an information tapestry. 35(12):61–70.

[42] N. Goldstein, R. Cialdini, and V. Griskevicius. A room with a viewpoint: Using social norms to motivate environmental conservation in hotels. 35(3):472–482.

[43] T. Govani and H. Pashley. Student awareness of the privacy implications when using Facebook.

[44] R. Gross, A. Acquisti, and H. J. Heinz, III. Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, WPES '05, pages 71–80. ACM.

[45] J. Grudin. Desituating action: Digital representation of context. 16(2):269–286.

[46] A. Hewitt and A. Forte. Crossing boundaries: Identity management and student/faculty relationships on the Facebook.

[47] W. Hill, L. Stead, M. Rosenstein, and G. Furnas. Recommending and evaluating choices in a virtual community of use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '95, pages 194–201. ACM Press/Addison-Wesley Publishing Co.

[48] K. Hook, D. Benyon, and A. J. Munro. *Designing Information Spaces: The Social Navigation Approach*. Springer.

[49] S. M. Humphrey. Impact of computer developments: An address before the Bendix G-15 users exchange conference, September 17, 1959. 2(12):16–19.

[50] M. Johnson, S. Egelman, and S. M. Bellovin. Facebook and privacy: It's complicated. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, page 1. ACM Press.

[51] A. Joinson and C. Paine. Self-disclosure, privacy and the internet. pages 237–252.

[52] A. N. Joinson. Looking at, looking up or keeping up with people?: Motives and use of Facebook. In *Proceeding of the 26th Annual SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, pages 1027–1036. ACM.

[53] J. Karat, C.-M. Karat, C. Brodie, and J. Feng. Privacy in information technology: Designing to enable privacy policy management in organizations. 63(1):153–174.

[54] P. Karr-Wisniewski, D. Wilson, and H. Richter-Lipford. A new social order: Mechanisms for social network site boundary regulation. In *AMCIS 2011 Proceedings*.

[55] P. Kumaraguru and L. Cranor. Privacy indexes: A survey of westins studies.

[56] S. Lederer, A. Dey, and J. Mankoff. A conceptual model and metaphor of everyday privacy in ubiquitous computing.

[57] S. Lederer, J. I. Hong, A. K. Dey, and J. A. Landay. Personal privacy through understanding and action: Five pitfalls for designers. 8(6):440–454.

[58] H. R. Lipford, G. Hull, C. Latulipe, A. Besmer, and J. Watson. Visible flows: Contextual integrity and the design of privacy mechanisms on social network sites. In *Proceedings of the International Conference on Computational Science and Engineering*, volume 4 of *CSE '09*, pages 985–989. IEEE Computer Society.

[59] K. Liu and E. Terzi. A framework for computing the privacy scores of users in online social networks. 5(1):1–30.

[60] M. Madejski, M. Johnson, and S. Bellovin. A study of privacy settings errors in an online social network. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops*, PERCOM '12, pages 340–345.

[61] M. Mo, D. Wang, B. Li, D. Hong, and I. King. Exploit of online social networks with semi-supervised learning. In *Proceedings of the International Joint Conference on Neural Networks*, IJCNN '10, pages 1–8.

[62] J. Mugan, T. Sharma, and N. Sadeh. Understandable learning of privacy preferences through default personas and suggestions.

[63] H. Nissenbaum. Privacy as contextual integrity. 79(1).

[64] H. Nissenbaum. Protecting privacy in an information age: The problem of privacy in public. 17(5):559–596.

[65] J. S. Olson, J. Grudin, and E. Horvitz. A study of preferences for sharing and privacy. In *Proceedings of the Extended Abstracts on Human Factors in Computing Systems*, CHI '05, pages 1985–1988. ACM.

[66] D. M. Oppenheimer, T. Meyvis, and N. Davidenko. Instructional manipulation checks: Detecting satisficing to increase statistical power. 45(4):867–872.

[67] L. Palen. Social, individual and technological issues for groupware calendar systems. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '99, pages 17–24. ACM.

[68] L. Palen and P. Dourish. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, CHI '03, pages 129–136. ACM.

[69] M. R. Parks and K. Floyd. Making friends in cyberspace. 46(1):80–97.

[70] S. Patil and J. Lai. Who gets to know what when: Configuring privacy permissions in an awareness application. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '05, pages 101–110. ACM.

[71] R. Ravichandran, M. Benisch, P. Kelley, and N. Sadeh. Capturing social networking privacy preferences. In *Proceedings of Privacy Enhancing Technologies*, PET '09, pages 1–18.

[72] J. Reagle and L. F. Cranor. The platform for privacy preferences. 42(2):48–55.

[73] R. W. Reeder, L. Bauer, L. F. Cranor, M. K. Reiter, K. Bacon, K. How, and H. Strong. Expandable grids for visualizing and authoring computer security policies. In *Proceeding of the 26th Annual SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, pages 1473–1482. ACM. ACM ID: 1357285.

[74] R. W. Reeder, C.-M. Karat, J. Karat, and C. Brodie. Usability challenges in security and privacy policy-authoring interfaces. In *Proceedings of the 11th IFIP TC 13 International Conference on Human-Computer Interaction - Volume Part II*, INTERACT '07, pages 141–155. Springer-Verlag.

[75] R. R. Reno, R. B. Cialdini, and C. A. Kallgren. The transsituational influence of social norms. 64(1):104–112.

[76] P. Resnick and H. R. Varian. Recommender systems. 40(3):56–58.

[77] H. Richter, A. Besmer, and J. Watson. Understanding privacy settings in Facebook with an audience view. In *Proceedings of the Workshop on Usability, Psychology, and Security*, UPSEC '08. USENIX.

[78] N. Sadeh, J. Hong, L. Cranor, I. Fette, P. Kelley, M. Prabaker, and J. Rao. Understanding and capturing people's privacy policies in a mobile social networking application. 13(6):401–412.

[79] J. H. Saltzer and M. D. Schroeder. The protection of information in computer systems. 63(9):1278–1308.

[80] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-based access control models. 29(2):38–47.

[81] M. Shehab, G. Cheek, H. Touati, A. C. Squicciarini, and P.-C. Cheng. User centric policy management in online social networks. In *Proceedings of the IEEE International Symposium on Policies for Distributed Systems and Networks*, POLICY '10, pages 9–13. IEEE.

[82] M. Shehab, S. Marouf, and C. Hudel. ROAuth: Recommendation based open authorization. In *Proceedings of the 7th Symposium On Usable Privacy and Security*, SOUPS '11.

[83] M. Shehab and H. Touati. Semi-supervised policy recommendation for online social networks. In *Proceedings of the 2012 International Conference on Advances*, ASONAM '12, pages 360–367. IEEE.

[84] A. Sinha, Y. Li, and L. Bauer. What you want is not what you get: Predicting sharing policies for text-based content on Facebook. In *Proceedings of the 2013 ACM Workshop on Artificial Intelligence and Security*, AISec '13, pages 13–24. ACM Press.

[85] N. Smelser. *Theory of collective behavior.* Free Press of Glencoe.

[86] D. K. Smetters and N. Good. How users use access control. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, pages 1–12. ACM.

[87] S. Spiekermann, J. Grossklags, and B. Berendt. E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce*, EC '01, pages 38–47. ACM.

[88] K. Strater and H. R. Lipford. Strategies and struggles with privacy in an online social networking community. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction-Volume 1*, BCS-HCI '08, pages 111–119.

[89] K. Strater and H. Richter. Examining privacy and disclosure in a social networking community. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*, SOUPS '07, pages 157–158. ACM.

[90] F. Stutzman. An evaluation of identity-sharing behavior in social network communities. 3(1):10–18.

[91] F. Stutzman and J. Kramer-Duffield. Friends only: Examining a privacy-enhancing behavior in Facebook. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 1553–1562. ACM.

[92] H. Tanizaki. Power comparison of non-parametric tests: Small-sample properties from monte carlo experiments. 24(5):603–632.

[93] E. Toch, N. M. Sadeh, and J. Hong. Generating default privacy policies for online social networks. In *Proceedings of the 28th of the International Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '10, pages 4243–4248. ACM.

[94] A. Tootoonchian, K. K. Gollu, S. Saroiu, Y. Ganjali, and A. Wolman. Lockr: Social access control for web 2.0. In *Proceedings of the First Workshop on Online Social Networks*, WOSN '08, pages 43–48. ACM.

[95] Z. Tufekci. Can you see me now? Audience and disclosure regulation in online social network sites. 28(1):20–36.

[96] N. Ueno, R. Hashimoto, M. Shimomura, and K. Takahashi. Soramame: What you see is what you control access control user interface. In *Proceedings of the Symposium on Computer Human Interaction for the Management of Information Technology*, CHiMiT '09, pages 5:38–5:41. ACM. ACM ID: 1641592.

[97] R. Wash. Folk models of home computer security. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, pages 11:1–11:16. ACM. ACM ID: 1837125.

[98] R. L. Wash. Motivating contributions for home computer security. Ph.D. Thesis.

[99] J. Watson, A. Besmer, and H. R. Lipford. +Your circles: sharing behavior on Google+. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, pages 12:1–12:9. ACM.

[100] A. F. Westin. *Privacy and Freedom.* Atheneum, 1st ed. edition.

[101] A. Whitten and J. Tygar. Why johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proceedings of the 8th USENIX Security Symposium.*

[102] P. Wisniewski, H. Lipford, and D. Wilson. Fighting for my space: Coping mechanisms for SNS boundary regulation. In *Proceedings of the 2012 ACM Annual Conference on Human Factors in Computing Systems*, CHI '12, pages 609–618. ACM.

[103] P. J. Wisniewski. Understanding and designing for interactional privacy needs within social networking sites. Ph.D. Thesis.

[104] M. Wu and C. T. Bowles. Principles for applying social navigation to collaborative systems. In *Proceedings of the 4th Symposium on Computer Human Interaction for the Management of Information Technology*, CHiMiT '10, pages 2:1–2:10. ACM. ACM ID: 1873563.

[105] M. E. Zurko, R. Simon, and T. Sanfilippo. A user-centered, modular authorization service built on an RBAC foundation. In *Proceedings of the IEEE Symposium on Security and Privacy*, pages 57–71. IEEE.

APPENDIX A: STUDY MATERIALS FOR CHAPTER 4

Facebook Application Study (Interview Script) - *Reaction to default privacy setting changed by community feedback*

A Pre-Study questions

Gender: *[just pencil in the gender of the participant]* Age:

[FII from TOIL at MSU] Can you answer the following questions on a scale of 1 to 5, with 1 being that you strongly disagree and 5 being that you strongly agree.

1. Facebook is part of my everyday activity
2. I am proud to tell people I'm on Facebook
3. Facebook has become part of my daily routine
4. I feel out of touch when I haven't logged onto Facebook for a while
5. I feel I am part of the Facebook community
6. I would be sorry if Facebook shut down
7. Approximately how many TOTAL Facebook friends do you have?
8. In the past week, on average, approximately how much time PER DAY have you spent actively using Facebook?

B Study Session

Thank you for participating in the study.

Explain the study and have the participant review and sign the [Pre] Informed Consent document about interacting with the Facebook application

We are going to start by having you logon to your Facebook account and install an application.

> *[At this point have the participant logon to their Facebook account on the provided computer. If necessary, remind them to not save their username and password.]*
>
> *[After they have logged on to Facebook, start the audio/video recording of the session. If it takes a minute to setup the recording, it is fine for the participant to interact normally with their Facebook.]*

The first part of the study will involve observing how you interact with Facebook applications. We would like to observe you as you interact with a few Facebook music applications. I will direct you to each of the applications and have you install and perform a simple tasks. Let's begin by looking at the SoundCloud Facebook application.

Please begin by searching for and installing the SoundCloud application. Click on the "App Center" link on the left side of your main Facebook page. Search for the term SoundCloud and add the application to your profile.

> *[If the user is having difficulty finding the application and installing it, it is fine for you to help install the app. The intended focus of the session is to not frustrate or unbalance the participants mood in any way]*

Please begin by attempting to find and add people or groups to follow. [If the participant has no friends who use the application, there will be no suggestions at the beginning, so direct the participant to the "Explore People" location under the People menu]. Find a few people or groups that you may be interested in and click on the Follow button to get suggested sound bites.

Now click on the Explore Tracks item under the Tracks menu. Explore the list of Hot sound bites and listen to part of one or a few to see if they interest you.

OK, now that we are finished observing interaction with this Facebook application, I would like to uninstall this application from your Facebook profile. After I finish uninstalling the app, we'll continue with the study.

> *[If the participant wants to keep the application, let them know that we need to uninstall it because of the study and they can always add it to their profile later]*
>
> *[As the application is uninstalled, you should see the Facebook message about changes to their privacy settings. Act surprised and say...]*

Wow, I have never seen this message on Facebook. It says here they have modified your privacy settings. I don't know what to do, so you can look at that, but it seems really interesting. You can look at that. I need to take a minute to close out the recording software.

> *[Try to encourage the participant to really focus on the message without being too obvious and see if they will read the message and help screens. Keep the audio/video recording going while they are interacting with the*

message and give them time to look around. Answer any questions they have as if you don't know anything about the message.]

[Give them a few minutes to interact with the message.]

Ok, although I mentioned we would have more applications to explore, that isn't really the case. The last message you saw on your Facebook account was not actually a message from Facebook. We used this computer to add that message to you screen and it really never came from Facebook. Our study is really about privacy settings and how you would react to having your settings modified automatically.

At this point, you have the option to withdraw from the study and we won't ask you any further questions. But, if you are willing to continue, we would like to ask you about your reaction to the message. Would you be willing to answer a few questions about your reaction to the message about changes to your privacy settings?

[At this point, discontinue audio/video recording and administer the post-experiment interview questions.]

C Post-experiment Debrief Interview

[Ask the following questions and feel free to probe with additional questions to gain clarification or better understand what the participant is thinking or feeling about their privacy settings. Please avoid any language that might appear judgemental or leading.]

□ *[Check here if the participant went to their privacy settings to see if something had been changed.]*

Let's talk about automated changes to your privacy settings:

What are some of your opinions on changes that Facebook has made in the past?

What are some things you like about Facebook?

What are some things you dislike about Facebook?

Do you have any concerns using Facebook?

How would you feel if Facebook modified one of your privacy settings without informing you and it matched your settings preference?

How would you feel if Facebook modified one of your privacy settings without informing you and it did not match your settings preference?

Can you describe your reaction to the message that your privacy settings had been changed?

> *[It is appropriate to ask some follow-up questions here to find out if they were agitated or apathetic. If they don't explain why they reacted a certain way, ask the question below]*
>
> Why do you think you reacted like you did to the change in your privacy setting?
>
> *[Here, if you noticed something in their reaction that they did not address, ask some probing questions to get as much information to clarify how it seemed they reacted, etc. Make sure you don't put words into their mouth, just clarify on anything you noticed and ask them why they appeared a certain way.]*

What did you think the message about the privacy change meant when it mentioned "others like you?"

[Discuss the community, what their perception is of "others like them" and how they would feel under additional hypothetical situations where things were changed according to any other group that they want to relate to.]

[Try to probe a little here and discover any situation they might be satisfied with having their privacy settings changed to reflect that community group's preference – or would they never entertain any automated change whatsoever.]