MPC MAJOR RESEARCH PAPER

HANDS OFF MY DATA!

A Comparison of Privacy Representations and Expectations on Facebook

Hayley Fuller

Dr. Wendy Freeman

This Major Research Paper is submitted in partial fulfillment of the requirements for the degree of Master of Professional Communication

Ryerson University

Toronto, Ontario, Canada

August 12, 2012

AUTHOR'S DECLARATION FOR ELECTRONIC SUBMISSION OF A MAJOR
RESEARCH PAPER

I hereby declare that I am the sole author of this Major Research Paper and the accompanying Research Poster. This is a true copy of the MRP and the research poster, including any required final revisions, as accepted by my examiners.

I authorize Ryerson University to lend this major research paper and/or poster to other institutions or individuals for the purpose of scholarly research.

I further authorize Ryerson University to reproduce this MRP and/or poster by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

I understand that my MRP and/or my MRP research poster may be made electronically available to the public.

Abstract

This MRP examines user expectations of online privacy in relation to how Facebook represents privacy in their Statement of Rights and Responsibilities. The prevalence and ubiquity of online social networking sites like Facebook have caused academics and individuals alike to reexamine their understandings and expectations of privacy in relation to online settings. As such, the specific purpose of this study is to better understand how the concept of privacy may be understood differently by social network users and the social networks themselves. In this paper I use the Fair Information Principles (FIPs) set out in the Personal Information Protection and Electronic Documents Act (PIPEDA) to analyze user comments made in relation to proposed changes to Facebook's Statement of Rights and Responsibilities. I find that both Facebook and users share a focus on concerns regarding limiting the use/disclosure/retention of personal information, and consent to have this information collected, and that users pay particular attention to Section 2.3 of the Statement of Rights and Responsibilities. I show that Facebook represents privacy conceptually in the Statement of Rights and Responsibility as in/accessibility, while users expect privacy to be enforced as data-control.

Keywords: privacy, social networking, Facebook, in/accessibility, data control, PIPEDA

Acknowledgments

I am incredibly thankful to my supervisor, Dr. Wendy Freeman, whose encouragement, guidance, and support directed me through the MRP writing process, and enabled me to gain a high understanding of the field of privacy and communication research. It was an honour and a pleasure to work closely with Dr. Wendy Freeman, and I am proud of the results she helped me achieve.

Thank you to Dr. Avner Levin, who acted as the second reader on this project. His guidance and specialty in the field of privacy research greatly enhanced this project, and always provided new avenues of exploration that I feel my MRP would be lacking without his input.

I am also appreciative and touched by the support and encouragement I received from my family, friends, and loved ones throughout this project and program. I couldn't have done it without you.

Table of Contents

List of Tables

Introduction

As online social networking becomes increasingly popular, individuals are sharing more of their personal information online. This public sharing of personal information has widespread implications, encompassing the restructuring of our communication practices, shifts in relationship formation and maintenance, our constructed identities online, and perhaps most disconcertingly, our information privacy concerns. As participation in social media sites entails intentionally broadcasting "private" information, there is increased awareness by users regarding how and with whom their personal information is being shared.

In recent years, despite extensive academic and popular literature that outlines the importance of maintaining privacy online, privacy issues have been growing on the Internet. This is largely due to the widespread implementation of new information sharing practices and policies that limit or restrict individuals' ability to fully control how their personal information is shared across the web (Benbasat, 2010). Social networking sites like Facebook can now collect ever increasing amounts of data about their users, from information willingly and consciously shared by users, to information gained by tracking individual Internet usage across the web. As a result, many individuals are becoming increasingly concerned about how their personal information may be utilized by the very social networking sites they visit daily.

With this in mind, this MRP will address the representation of privacy as policy put forth by Facebook, as well as explore user expectations of online privacy on social networking sites. My MRP will be focused how privacy is represented in the changes

made to Facebook's Statement of Rights and Responsibilities, along with user reactions to these changes. I examine these issues by analyzing these documents using the Fair Information Principles (FIPs) described in the Personal Information Protection and Electronic Documents Act (PIPEDA) (Canadian Minister of Justice, 2011). To begin, I use the FIPs to look at how privacy and personal information are represented by Facebook in its Statement of Rights and Responsibilities. To compare user expectations of online privacy in relation to how Facebook represents privacy in their Statement of Rights and Responsibilities, I will then use the FIPs to analyze user comments made regarding proposed changes to the Statement of Rights and Responsibilities. The potential tension between how privacy is represented by Facebook in the Statement of Rights and Responsibilities and user expectations of privacy online provides a rich site for analyzing shifting conceptualizations of privacy in the social networking context.

Research Context
Fair Information Principles

The Personal Information Protection and Electronic Documents Act (PIPEDA) was written by the Ministry of Industry Canada (Canadian Minister of Justice, 2011) to define a number of Fair Information Principles (FIPs) that apply to the collection of personal information by the government and other organizations. These FIPs serve to describe the responsibilities held by organizations in protecting individual data and informational rights in the electronic age.

Facebook

Facebook.com (or Facebook) is a social-network site that was established in 2004 as a way for college students to connect to one another online. The phrase "social-

networking site" is perhaps best described by danah boyd and Nicole Ellison, who define

these websites as:

> [Social network sites are] web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system (2007).

Within months of its creation in 2004, Facebook was made available to college students

across the U.S. and Canada, and has continued to grow (Cohen, 2012). Currently,

Facebook is open to any individual who wants to join the site, under the conditions that

they have a valid email address and are over the age of 13 (Facebook.com Terms and

Policies, 2012). As of April 24, 2012, there were 900 million active users of the site, with

a projected growth of 1.74% a month (Cohen, 2012; Facebook IPO Statement, 2012).

Facebook Site Governance Page

Facebook maintains a Site Governance fan page, the aim of which is to allow

users the space to "learn more about [Facebook's] site governance documents and

proposed future changes to these documents"

(https://www.facebook.com/fbsitegovernance/info). The Facebook Site Governance fan

page has been in existence since 2006, and currently has 2,329,158 likes (as of July 30,

2012). When users become fans of this page, they receive automatic push notifications

to their Newsfeed about future proposed changes to Facebook policies, and are given

access to site wide votes on documentation amendments.

The primary purpose of the page is to allow users the opportunity to express their

opinions about changes to existing documentation (Facebook Site Governance About Us

Page, 2012). In past revisions of documentation, hundreds of users have commented on

proposed changes to policies and documentation. This indicates that there is a small but vocal population of Facebook users who are engaged in the process of monitoring site policy changes.

Facebook Statement of Rights and Responsibilities

The Facebook Statement of Rights and Responsibilities is an important document that outlines Facebook's responsibilities to its users, users' data, and others who interact with Facebook. The Facebook Statement of Rights and Responsibilities is made up of 19 main sections used to describe the rules and regulations for becoming a member of the site. Each section is further divided into sub-sections, totaling 116 sub-sections that make up the SRR. When signing up for an account on Facebook, all users are required to agree to the terms of the SRR. On March 15, 2012, Facebook announced that it was making changes to its Statement of Rights and Responsibilities, and announced via the Site Governance Fan page that they were looking for user comments on the proposed changes. The announcement asking for user comments on the proposed Statement of Rights and Responsibilities was only visible to individuals who were already fans of the Site Governance page. Fans of the Site Governance page were asked to comment on a document hosted on the "Documents" tab of the Site Governance page that tracked the changes between the former SRR (written in 2011) and the proposed SRR (2012). Commenting on proposed changes to the Statement of Rights and Responsibilities was open to users on the Site Governance Page for a total of seven days, between March 15 and March 22, 2012. After the commenting period closed, Facebook representatives announced that they would consider user comments, and make a statement once they had evaluated all feedback to the proposed changes to the Statement of Rights and Responsibilities.

4

This paper examines this first round of user comments on proposed changes to the Statement of Rights and Responsibilities, along with an analysis of the proposed changes to the Statement of Rights and Responsibilities. 502 users took this opportunity to approve or critique the changes proposed in the Statement of Rights regarding how their personal information was going to be collected and used by Facebook. This situation provided a rich opportunity to examine how user expectations of online privacy may differ from how online social networking sites (specifically Facebook) represent privacy in their policies. This study will build on previous academic literature on the concept of privacy, as well as specific studies of privacy in the context of online social networking.

Literature Review

Information Privacy "Defined"

According to Marc Rotenberg, the director of the Electronic Privacy Information Center in Washington DC, in recent years privacy has emerged as one of the most important human rights of the modern age (2009). Despite this importance, however, it is also difficult to define. Our understanding of privacy, as a concept, is fragmented across different fields and disciplines, "with concepts, definitions, and relationships that are inconsistent and neither fully developed nor empirically validated" (Xu, Dinev, Smith, & Hart, 2011). Throughout the disciplines and over time, privacy has been conceived of as looking at "rights" and "entitlements" from a legalistic view (Warren & Brandeis, 1890), to defining privacy as "a state of limited access or isolation" within psychological and philosophical fields (Schoeman, 1984), to examining the meaning of "control" over personal information (Culnan, 1993; Westin, 1967). These differing conceptualizations of privacy over the years led Margulis (1977) to note, "theorists do not agree...on what privacy is or on whether privacy is a behavior, attitude, process, goal, phenomenal state, or what" (p.17). In following years, Margulis expanded upon this opinion, noting that concepts such as confidentiality, secrecy, and anonymity were increasingly overlapping and examined with privacy concepts by academics, making the field even harder to define (Margulis 2003a, 2003b; Xu, Dinev, Smith, & Hart 2011). Solove also concludes that "[p]rivacy as a concept is in disarray. Nobody can articulate what it means" (2008, p 477).

Despite the confusion surrounding the concept of privacy, two primary ways of thinking about privacy have been explored by academics and theorists (Levin & Abril, 2009). These are privacy-as-control and privacy-as-dignity (Whitman, 2004). In the

6

online world, privacy-as-control has become the dominant paradigm with which to study privacy (Allen, 2000). In the school of thought that views privacy-as-control, one of the most widely cited definitions of privacy was put forth by Westin (1967), who defined privacy as "the ability of individuals, groups, or institutions to control when, how, and to what extent information about them is communicated to others" (p. 10). This definition is still referred to by many theorists when examining online and social media environments (Nissenbaum, 2004; Hull, Lipford & Latulipe, 2011; Stutzman & Hartzog, 2011; Houghton & Joinson, 2010; Taraszow, Aristodemou, & Shitta et al., 2010), though some theorists argue that it is becoming insufficient in capturing online privacy (Levin & Abril, 2009). However, definitions of privacy vary according to context, making it a difficult concept to understand. According to Allen, there is an increasing movement to view privacy online strictly in terms of privacy as data-control (2000). The view of privacy-as-data-control (or the privacy-control paradigm) aims to place the user as the central decision maker, in control of their own data online (Schwartz, 1999). The view that information privacy is essentially about control over one's data online has proliferated in recent years, especially as the study and reporting on social networking has increased in popularity among both theorists and in the popular media (Allen, 2000; Cavoukian & Tapscott, 2006). The conceptualisation of privacy as control has been made the basis of many privacy laws and policies around the world (Levin and Abril, 2009).

Robert Ellis Smith (2000), the editor of *Privacy*, considers a legalistic interpretation of privacy-as-control to be too narrow, as a concept, and offers a broader definition of privacy-as-dignity. With this in mind, Smith (2000) defines privacy as "the desire by each of us for physical space where we can be free of interruption, intrusion,

7

embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves". These sentiments echo Bloustein (1978), who argued that all privacy interests "share one value" (as cited in Levin & Abril, 2009, p. 1012): the protection of an individual's independence, dignity, and integrity. A conception of privacy-as-dignity emphasizes the development of the person and self, and the right of individuals to present certain aspects of their personalities to the public as they so choose (Goffman, 1959).

Some studies have taken a slightly different approach to understanding individual conceptions of privacy, beyond the privacy-as-control or privacy-as-dignity paradigms. Nissembaum (2004) approaches online privacy from a contextual perspective. She argues that as people move in and out of different social contexts, they are required to understand and navigate the norms of information sharing in these different contexts (Nissembaum, 2004). According to Nissembaum, a user operating under the assumption that a universal privacy norm exists is not taking into account the "granular contextuality of online space" (p. 115, 2004). Hull, Lipford and Latulipe build on Nissembaum's analytical framework for understanding the notion that privacy is contextual (2011). They continue Nissembaum's account that privacy with regards to information technology is based on two essential ideas: 1) that all areas of life are governed by context-specific norms of information flow, and 2) that people move in and out of different informational contexts multiple times daily (Hull, Lipford, & Latulipe, 2011).

The prior body of conceptual work on privacy, which splits the concept of privacy primarily into two separate paradigms of control vs. dignity, has led various scholars to attempt to synthesize and join these two concepts with the aim to provide common

8

ground in the field of privacy studies (Xu, Dinev, Smith, & Hart, 2011). With the opinion that privacy is just "a shorthand umbrella term" (Solove, 2007, p 760), Solove has developed a taxonomy of information practices and policies that attempt to map out different privacy problems facing individuals. Solove has advanced his taxonomy as a way to understand privacy because it "shift[s] away from the rather vague label of *privacy* in order to prevent distinct harms and problems from being conflated or not recognized" (p. 759). With this difficulty in defining privacy in mind, many scholars are examining how privacy is understood in the context of social networking.

 Privacy in Online Social Networks (OSNs)

In recent years there has been a renewed focus on the study of information privacy, especially in the context of online social network sites. The primary focus of much of this recent literature has been on the emergence of privacy concerns related to extraneous disclosure of personal information online (Acquisti & Gross, 2006; Barnes, 2006; Gross & Acquisti, 2005; Krishnamurthy & Wills, 2008; Strater & Lipford, 2008). The privacy concerns examined in these studies range from issues regarding the unauthorized collection and dissemination of user data to identity theft. However, it is important to note that all of these studies focus on the information users disclose about themselves online, and the resulting information privacy concerns experts consider users should be taking into consideration. Very few scholars examine how these privacy concerns arise and are expressed by users (Benbasat, Bulgurcu, & Cavusoglu, 2010). In fact, traditionally, there has been a general perception among academics and the popular press alike that individuals in fact *do not* value their privacy online because they continue to disclose information about themselves online (Gross & Acquisti, 2005), and thus do not have serious privacy concerns regarding the treatment of their online

9

information. However, Gross and Acquisti conducted a study in 2006 that reported seemingly contradictory user behaviour online - they found that when interviewed, users of social network sites stated that they are concerned about the privacy of their information, and how their information is distributed beyond their control, yet they continue to disclose a great deal of information about themselves online (2006). It is important to note that both of Gross and Acquisiti's studies were conducted in Facebook's infancy; however, in subsequent years, similar findings have been reported in online social networking environments by a variety of privacy specialists (Foster, West, & Levin, 2011; Stutzman & Hartzog, 2009).

Many theorists argue that, in terms of their privacy, users still struggle with what is contextually appropriate to share in OSNs (Barnes, 2006; Hull, Lipford & Latulipe, 2011; Grimmelmann, 2006; Nissenbaum, 2004; Stutzman & Hartzog, 2009), and attribute this struggle with many of the privacy concerns expressed by users in interviews and studies (Xu, Dinev, Smith & Hart, 2011; Yao, Rice, & Wallis, 2007; Young & Quan-Haase, 2009). Additionally, more focus is being placed in academic work that is centered on privacy and online social networking on *how* user privacy concerns arise in online social networking contexts (Solove, 2008; Hoadley, Xu, & Lee, 2010; Benbaset, Bulgurcu, & Cavusoglu, 2010). boyd suggests that privacy in online social networks is tied to a sense of control over personal data (boyd, 2008), and Hoadley, Xu, Lee and Rosson further discuss user privacy concerns online as arising out of an "illusory loss of information control" (2010). In their study, they discussed user privacy concerns arising out of the introduction of the Facebook News Feed, and found that many users believed the News Feed would allow much more access to their personal information than previous iterations of Facebook. Though this was not the case, the "illusory loss of

10

control" over their personal information is what caused user concern to arise. Hoadley, Xu, Lee and Rosson concluded that many instances of perceived user privacy violations online could be the result of misconceptions and misinterpretations surrounding user data when new policies are implemented by social networks (2010).

In the context of online social networks, it is not easy to tell if a certain action (whether it be on the part of the user or a social networking site) will cause privacy concerns to arise for users because, in part, users display seemingly conflicting behaviours and beliefs regarding their personal information online (Arshad & Cole, 2009). Dwyer, Hiltz, & Passerini (2007) argue that, "privacy within social networking sites is often not expected, or is undefined" (p. 4). In more recent years, academics studying privacy on social networking sites have also reported differing findings regarding how users view their privacy in online social networking contexts (Dwork, 2006; Hull, Lipford, & Latulipe, 2011; Stutzman & Hartzog, 2009; Van Eecke & Truyens, 2010). However, I hope that studying user responses to changes made in Facebook's Statement of Rights and Responsibilities will provide valuable insight into the contexts in which user privacy concerns arise. As such, my MRP will contribute to an understanding of what factors cause user privacy concerns to arise in social networking sites.

Research Questions

With previous research on conceptualizations of privacy online (and specifically privacy in the social networking context) in mind, the overarching research questions addressed throughout this MRP are:

Research Question 1: How does Facebook represent online privacy within policy, as reflected in the Statement of Rights and Responsibilities?

Research Question 2: What are Facebook users' expectations of online privacy, as reflected in user comments outlining privacy concerns in response to Facebook's Statement of Rights and Responsibilities?

Research Question 3: How do user and Facebook (as reflected in the SRR) conceptualizations of privacy compare to one another?

Method

The research questions of this study aim at understanding how Facebook represents online privacy as policy in the Statement of Rights and Responsibilities, and how this aligns (or does not) with users' expectations of privacy in an online social networking environment. To explore my research questions, I used qualitative content analysis methods. Qualitative content analysis has been described as "a research method for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns" (Hsieh & Shannon, 2005, p. 1278). Using qualitative content analysis is well suited to exploring my research questions for a variety of reasons. Qualitative content analysis emerges from an interpretive tradition, and allows me to examine individual interpretations of privacy as expressed through textual means (Hsieh & Shannon, 2005). In the case of my MRP, a qualitative approach is appropriate as this study aims to understand users' perspectives on privacy issues, which, as textual data, prove difficult to analyze using quantitative methods (Strauss & Corbin, 1994). Given the small size of my data set, I determined that qualitative content analysis was the most valuable method of approaching my data, and would allow me to engage in the richest analysis of my data given the qualitative nature of my research questions. However, incorporating quantitative research methods to augment qualitative content analysis could have proven useful had a larger data sample been used, or for the purposes of a larger, follow-up research project.

In particular, this study undertakes a content analysis of users' comments posted on sections of proposed changes to Facebook's Statement of Rights and Responsibilities, as well as the Facebook Statement of Rights and Responsibilities. Qualitative content

analysis proved useful as an introductory examination of user privacy concerns online. By examining user comments posted on the proposed changes to Facebook's SRR, this method allowed me to identify users who were generally aware of privacy issues online, and sensitive enough to these issues to comment on them. Using a qualitative content analysis method gave me access to many rich descriptions and explanations about the general informational practices of Facebook, as they were outlined quite clearly in the SRR. Finally, this method allowed me to gather specific user reactions to the proposed changes - as it has been documented that while users may not be able to strongly describe their privacy issues when they are solicited without warning, they are very good at responding to a set of proposed terms they disagree with (Benbaset, Bulgurcu, & Cavusoglu, 2011).

As such, I used qualitative methods to study Facebook's representation of information privacy, as laid out in its Statement of Rights and Responsibilities (SRR). I used these same methods to study user expectations of online privacy as expressed in comments made on the Facebook Site Governance page regarding proposed changes to the SRR. All data was collected from www.facebook.com/fbsitegovernance, and consists of documents and user generated comments. The qualitative content analysis of these data was guided by the Fair Information Principles (FIPs) described in the Personal Information Protection and Electronic Documents Act (PIPEDA) (Canadian Minister of Justice, 2011). These FIPs serve to describe the responsibilities held by organizations in protecting individual data and informational rights. I used these FIPs definitions to analyze both the Statement of Rights and Responsibilities and user expectations of online privacy regarding proposed changes to the SRR

14

Ethics approval, and consent from users whose comments were studied, was not required for this study because all documents collected were made available legally and easily to the public by Facebook.com. When comment threads take place in online environments such as Facebook, and in particular in public fan pages that any Internet user (whether or not they are a Facebook user) can view, it is considered public discourse, for which no informed consent is needed (Lindlof & Taylor, 2011). As Walther (2002) noted, "the analysis of Internet archives is not human subjects research, if a researcher does not record the identity of the message poster, and if the research can legally and easily access such archives" (as cited in Lindlof & Taylor, 2011, p. 123). As such, the identities of Facebook users who made comments on proposed changes to the SRR have not been recorded, and names have been anonymized for analysis and reporting purposes.

Data Collection and Analysis

As all the documents I studied only existed in electronic form, I had to archive them for analysis. I created PDF copies of the comment thread on the tracked changes Facebook SRR document tab in order to archive the data for close analysis. The PDF containing all user comments was created one day after the call for user comments had closed, on March 23, 2012. Finally, I downloaded the tracked changed Statement of Rights and Responsibilities in PDF form on March 23, 2012. Following collection, I analyzed these documents using the PIPEDA Fair Information Principles (FIPs). It is important to note that though the Facebook Statement of Rights and Responsibilities references other policies put in place by the site – most significantly the Data Use Policy – I only analyzed the Statement of Rights and Responsibilities and comments posted on

15

this document. I made this choice because the goal of this MRP is to study user reactions to changes made to the Statement of Rights and Responsibilities – a specific document that user attention was called to through the Facebook Site Governance page. This MRP was not intended to study the overall privacy policies of Facebook.com or user thoughts on these other documents, and as such, no privacy policies or user comments made to documents beyond the Statement of Rights and Responsibilities were analyzed.

Data Analysis

I manually coded the user comments and the SRR tracked changes document for categorical Fair Information Principles (FIPs), originally defined by the Ministry of Industry Canada in the Personal Information Protection and Electronic Documents Act (PIPEDA) (Canadian Minister of Justice, 2011). Thus, I examined comments regarding changes to the SRR according to the FIPs to understand how Facebook represents privacy in their policies.

PIPEDA and FIPs definitions are useful, as they were first applied to government handling of personal information before being applied to the private sector (i.e. Facebook). As such, the FIPs provide a rich way to understand and code Facebook's SRR in terms of Facebook's understanding of privacy responsibilities. However, PIPEDA and FIPs definitions also provide a rich way to code comments made by users, and then compare those comments with privacy understandings found from the SRR after coding. User comments can be classified according to how they correspond with the Fair Information Principles laid out for organizational handling of private information. Often, user privacy concerns are best articulated when organizational data handling practices are made visible, as through the SRR (Strauss & Corbin, 1994).

16

Data were coded according to categories derived from the FIPs. The definitions, taken from the principles set out in the National Standard of Canada Model Code for the Protection of Personal Information, are described in Table 1.

Table 1: FIPs Definitions for Coding

Code	Definition
Accountability	An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles (PIPEDA, 2011, p. 36).
Identifying Purposes	The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected (PIPEDA, 2011, p. 36).
Consent	The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate (PIPEDA, 2011, p. 37).
Limiting Collection	The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means (PIPEDA, 2011, p. 39).
Limiting Use, Disclosure, and Retention	Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes (PIPEDA, 2011, p. 39).
Accuracy	Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used (PIPEDA, 2011, p. 40).
Safeguards	Personal information shall be protected by security safeguards appropriate to the sensitivity of the information (PIPEDA, 2011, p. 40).
Openness	An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information (PIPEDA, 2011, p. 41).
Individual Access	Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate (PIPEDA, 2011, p. 42).
Challenging Compliance	An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance (PIPEDA, 2011, p. 43).

Definitions adapted from the National Standard of Canada Model Code for the Protection of Personal Information, version applicable through June 10, 2012

Facebook Statement of Rights and Responsibilities Collection and Coding

I collected the Statement of Rights and Responsibilities in full (i.e. the entire document that is available to users). However, as I was primarily examining user reactions to changes made in the Statement of Rights and Responsibilities, I also collected previous versions of this document for comparison purposes. As such, the specific documents I collected were:

1. The Facebook Statement of Rights and Responsibilities, version released on April 26, 2011

2. Facebook Statement of Rights and Responsibilities tracked changes, released by Facebook for commenting on March 7, 2012

I analyzed the proposed SRR put forth in March 2012 according to the FIPs laid out by PIPEDA. The purpose of this coding was to identify and attempt to define how Facebook represents information privacy, as they outlined in their SRR. Thus, I coded the entire document, and categorized each section according to the FIPs. The FIPs not reflected in the Statement of Rights and Responsibilities are addressed in the Facebook Data Use Policy, but this document was not included in the data set for this MRP. Table 2 reflects examples of this coding.

Table 2: Examples of Analysis of the 2012 Proposed Statement of Rights and Responsibilities According to FIPs

Code	Example
Accountability	N/A
Identifying Purposes	N/A
Consent	You give us permission to use and allow others to use such links and content on Facebook. (SRR, Section 8.2)
Limiting Collection	You will not solicit login information or access an account belonging to someone else. (SRR, Section 3.5)
Limiting Use, Disclosure, and Retention	When you or others who can see your content and information use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, read our Data Use Policy and Platform Page.) (SRR, Section 2.3)
Accuracy	You will keep your contact information accurate and up-to-date. (SRR, Section 4.7)
Safeguards	You will not upload viruses or other malicious code. (SRR, Section 3.4)
Openness	We can change this Statement if we provide you notice (by posting the change on the Facebook Site Governance Page) and an opportunity to comment. To get notice of any future changes to this Statement, visit our Facebook Site Governance Page and like the Page. (SRR, Section 14.1)
Individual Access	N/A
Challenging Compliance	N/A

I then coded the version of the SRR released in 2011 according to the FIPs in order to compare the terms with the 2012 proposed changes. This resulted in the recognition of themes within the SRR data. Changes made to the SRR were defined by myself in one of two ways: (1) *Stylistic Changes* - edits to the SRR that changed terminology or grammar or (2) *Policy Changes* - edits to the SRR that resulted in changes to previous policies and/or practices. Changes classified as *Stylistic* constituted insignificant edits to sections of the SRR - i.e. removing references to "user profiles" and replacing it with "Timeline". *Stylistic* changes did not modify the section of the SRR being described apart from the choice of language used. *Policy* changes consisted of additions or edits to the SRR that result in actual policies and practices being changed

19

from previous iterations of the SRR. *Policy* changes include the addition of new SRR sections that outline new rules or regulations, as well as modifications to previous sections that result in policies being changed. Table 3 presents examples of this coding. The edits to the SRR between 2011 and 2012 are represented in red.

Table 3: Examples of Comparison of 2011 and 2012 Facebook SRR for Identification of Themes

Category	Example
Stylistic Change	14.1.We can change this Statement if we provide you notice (by posting the change on the Facebook Site Governance Page) and an opportunity to comment. To get notice of any future changes to this Statement, visit our Facebook Site Governance Page and ~~become a fan~~like the Page.
Policy Change	17. We strive to create a global community with consistent standards for everyone, but we also strive to respect local laws. The following provisions apply to users and non-users who interact with Facebook outside the United States:

User Comments Collection and Coding

After the commenting period on the proposed changes to the SRR was announced, I monitored the process of users commenting on the document by visiting the Facebook Site Governance Fan Page and taking screenshots of user activity until the commenting period closed on March 22, 2012. At that point, the dataset of user comments contained 526 comments, where 502 users wrote one comment, and 24 wrote two or more comments. Of this set, there were 210 comments that spoke about topics that did not relate to changes made to the SRR. To identify which comments to analyze, my selection criteria were:

1. Comments must refer to the Statement of Rights and Responsibilities.

2. Comments must be written in English.

20

3. Comments that do not participate in relevant conversation (i.e. complaints about site design) were not analyzed.

While Facebook provided a proposed Statement of Rights and Responsibilities in 10 different languages and asked for user comments in each of these languages, this study only includes an analysis of comments posted in English. This is important to note, as various privacy scholars argue that privacy concerns and dialogues vary across cultures (Ess, 2005). This means that Asian cultures, for example, may be more concerned about privacy as related to dignity than North American cultures – and if users choose to express their comments in a language other than English, these comments were not analyzed within the scope of this MRP. As such, the English comments made to the Statement of Rights and Responsibilities may not reflect the privacy concerns of Facebook users worldwide, and this serves as a research limitation that should be addressed in future studies.

I analyzed user comments about the proposed changes to Facebook's SRR according to the definitions of privacy laid out by the FIPS in the PIPEDA document (see Table 1). The purpose of this coding was to identify which privacy issues were of most concern to Facebook users. Out of a total 526 user comments made on the SRR document, 316 comments were identified as being related to privacy issues on Facebook. The remaining 210 comments that were identified as *not* relating to privacy issues spoke about issues of design, site questions, or advertising a product and/or issues that made no references to changes made to the SRR. Of the 316 comments made relating to privacy issues about the changes to the SRR, 204 comments could be coded according to the FIPs definitions. It is important to note that comments that expressed "approval/disapproval statements" (i.e. "I dis/approve of these changes") were counted

21

among the 316 comments made regarding privacy, but could not be coded according to the FIPs. These 112 comments account for the difference between the total number of privacy related comments made, and the number of comments analyzed. In other words, though there were 316 user comments made on the SRR document that related to privacy, there were only 204 comments that could be analyzed according to the FIPs.

The result of this phase of analysis was identifying of a number of top user privacy concerns, discussed in Findings. Table 4 reflects examples of this coding.

Table 4: Examples of Analysis of User Comments According to FIPs

Code	Example
Accountability	N/A
Identifying Purposes	N/A
Consent	**Ian Carson** §2.3: You say in the summary that this is to reflect already existing policy "which is what you consented to when you installed the App". If this is my information that a friend shares to an app, then *I* never consented to anything when this app was isntalled [sic]. That this is already your actual policy only makes it worse..
Limiting Collection	**John Bito** Section 2.3 may reflect the current practice. If so, we need additional privacy control. Section 2.3 should be changed back and we should be able to limit what services and apps can collect information from us.
Limiting Use, Disclosure, and Retention	**Rob Taylor** Seems fine *apart from* new 2.3 "When you or others who can see your content and information...". This wholly goes against the principle that the user has control of who gets their information. It is wrong that a users [sic] information can be shared be someone else.
Accuracy	**Irene Steffen** Section 4: the bans on both providing false personal information and having more than 1 account are horrible for privacy. The courts have inferred a fundamental right to privacy from the Constitution, and anonymous speech is a recognized First Amendment right, online and offline. Facebook can try to undermine the Supreme Court all it wants, but it's not good policy and we should never accept it.
Safeguards	N/A
Openness	**Helen Austin** I think Section 3.4 should read we WILL provide notice, it is bad practice to not inform users of changes which will affect any part of the Statement of Rights and Responsibilities. Please change this and the policy which allows you to not inform us of these changes, thankyou [sic].
Individual Access	N/A
Challenging Compliance	N/A

This stage of analysis revealed that most privacy related user comments discussed Section 2.3 of the Facebook Statement of Rights and Responsibilities. As such, I chose to focus my MRP on the study of comments made about Section 2.3 of the Statement of Rights and Responsibilities.

Code Verification.

In this stage, I undertook a process of code verification. Three colleagues from Ryerson University were asked to verify exemplar data according to my coding system. These three colleagues were qualified to verify my coding system because they already had experience doing research using qualitative content analysis in the field of communication and social media. Their expertise was not in the study of privacy, but each individual was provided with background reading and research to inform their coding verification. These colleagues were given sample data and FIPs definitions, and asked to categorize the data according to the FIP definition they felt reflected the data best. No disagreements arose when categorizing the Facebook Statement of Rights and Responsibilities. When coding user comments, my colleagues agreed with my coding 87% of the time. The areas of disagreement arose around categorizing comments as *Consent* or *Limiting Use/Disclosure/Retention.* This disagreement was resolved after discussion and close study of the meaning of these related FIPs definitions, resulting in a clearer understanding of the distinctions between these two categories. Following this verification, I re-coded the user comments and SRR according to their feedback to confirm my findings.

Following this code verification, I compared the coded user comments and coded SRR to determine what user expectations of online privacy are, and to determine if these expectations of privacy were viewed differently by users than by the representation of privacy as policy laid out by Facebook in the Statement of Rights and Responsibilities.

Findings

My research findings are organized by research question and analysis stage. Once my documents were collected and my data set was established, I performed initial analysis of both the Statement of Rights and Responsibilities and the commenting thread in response to this document according to PIPEDA FIPs. I then conducted a secondary, thematic analysis of both documents to explore, more closely, how Facebook and user conceptualizations of privacy differed from one another. It is important reiterate that the focus of my MRP was user reactions and comments to changes made to the Statement of Rights and Responsibilities, not a comprehensive study of the privacy policies of Facebook.com. As such, I did not analyze any policies that the Statement of Rights and Responsibilities refers to, nor did I analyze user comments made on these other policies and documents. As stated previously, my Discussion will focus on SRR Section 2.3, but I will first report the findings of my full data set.

Facebook Statement of Rights and Responsibilities

Research Question 1: How does Facebook represent online privacy as policy, as reflected in their Statement of Rights and Responsibilities?

Using FIPs definitions, the first stage of analysis explored how Facebook represents privacy in the SRR. In total, there are 116 sub-sections of the Facebook SRR all of which were analyzed using the FIPs categories defined in Table 1. This analysis is presented in Table 5.

Table 5: Results of FIPs Coding of Facebook Statement of Rights and Responsibilities

FIPs Category	Number of Sections of SRR Coded Using FIPs Categories	% of Total Number of Sections
Consent	18	16%
Limited Collection	10	8%
Limiting Use/Disclosure/Retention	27	23%
Accuracy	8	8%
Safeguards	11	9%
Openness	15	13%
Accountability	0	0%
Identifying Purposes	2	1.7%
Individual Access	0	0%
Challenging Compliance	0	0%
		Total Sections: 116

There were 18 instances of SRR sections categorized as *Consent* (16% of 116 total sections); 27 instances of SRR sections categorized as *Limiting Use/Disclosure/Retention* (23% of 116 total sections), and 15 instances of SRR sections categorized as *Openness* (13% of 116 total sections). As such, these three categories represent the aspects of privacy Facebook places the most emphasis on in the Statement of Rights and Responsibilities. As presented in Table 5, 60 of 116 sections of the SRR were categorized as *Consent*, *Limiting Use/Disclosure/Retention* or *Openness.* Thus, these privacy categories represent the majority of sections in the SRR, at 52% of the total SRR sections.

There were 10 instances of SRR sections categorized as *Limited Collection* (8% of 116 total sections); 8 instances of SRR sections categorized as *Accuracy* (8% of 116 total sections), and 11 instances of SRR sections categorized as *Safeguards* (9% of 116 total sections). There were 2 instances of SRR sections categorized as *Identifying Purposes* (1.7% of 116 total sections). There were no instances of the categories of *Accountability,*

Individual Access, and *Challenging Compliance* in the tracked changes version of the SRR.

Themes and Patterns Among SRR Changes

The second stage of analysis of the Statement of Rights and Responsibilities examined the differences between the 2011 SRR and 2012 proposed SRR, and the proportions of changes in sections and sub-sections between these two versions. I found that the sections of the SRR that went through the greatest changes between the 2011 and 2012 SRR versions are sections that are categorized as *Limiting Use/Disclosure/Retention* and *Consent.* 58 of 116 sub-sections of the SRR were changed from the 2011 version of the SRR. This means that in total, 50% of the sections and sub-sections of the 2012 proposed Statement of Rights and Responsibilities changed from the 2011 version. Table 6 presents the sections that underwent the greatest changes. The "SRR Section" column reflects the titles of the primary sections of the SRR, before they are broken down into sub-sections.

Table 6: Type of SRR Changes Made from 2011 to 2012 versions

SRR Main Section	FIPs Categorization	Type of Change
Section 1: Privacy	Identifying Purposes	Stylistic
Section 2: Sharing Your Content and Information	Limiting Use/Disclosure/Retention; Consent	Policy
Section 3: Safety	Safeguards	Stylistic; Policy
Section 4: Registration and Account Security	Accuracy	Stylistic
Section 5: Protecting Other People's Rights	Consent; Limiting Use/Disclosure/Retention	Policy
Section 6: Mobile and Other Devices	Consent	Policy
Section 7: Payments	N/A	Stylistic
Section 8: Special Provisions Applicable to Social Plugins	N/A	Stylistic
Section 9: Special Provisions Applicable to Developers/Operators of Applications and Websites	Consent; Limiting Use/Disclosure/Retention	Stylistic
Section 10: About Advertisements	Limiting Collection	Policy
Section 11: Special Provisions Applicable to Advertisers	N/A	Stylistic; Policy
Section 12: Special Provisions Applicable to Pages	N/A	N/A
Section 13: Software	N/A	Policy
Section 14: Amendments	Openness	Policy
Section 15: Special Provisions Applicable to Software	N/A	N/A
Section 16: Disputes	Safeguards; Limiting Use/Disclosure/Retention	Policy
Section 17: Special Provisions Applicable to Users Outside the United States	Limiting Collection; Safeguards	Policy
Section 18: Definitions	N/A	Stylistic
Section 19: Other	Limiting Use/Disclosure/Retention	Policy

38% of the changes made to the Statement of Rights and Responsibilities between the 2011 and 2012 version of the document were *Stylistic* (edits to the SRR that changed terminology or grammar), and 50% of the changes made were *Policy* changes (edits to the SRR that resulted in changes to previous policies and/or practices). 12% of the changes could be classified as both *Stylistic* and *Policy* changes, which means that a

change of stylistic language acted to modify how the sub-section could be read in terms of policy.

Within the FIPs categories in the SRR, *Limiting Use/Disclosure/Retention* had the most instances of *Policy* changes between the 2011 and 2012 versions of the SRR; 31% of all SRR sections and sub-sections categorized as *Limiting Use/Disclosure/Retention* underwent a *Policy* change. The FIPs category of *Consent* had the second highest instances of *Policy* changes at 25% of all sections and sub-sections of the SRR categorized as *Consent* undergoing changes between the two versions.

Table 7 shows that the FIPs categories with the highest instances of *Policy* changes between 2011 and 2012 are the same FIPs categories that the majority of sections and sub-sections of the SRR are categorized as.

Table 7: Percentage of Majority Sections of the SRR that were Changed Between 2011 and 2012

FIPs Category	% of Total SRR	% of Policy Changes between 2011 and 2012
Consent	16% (18 of 116 sections)	25%
Limiting Use/Disclosure/Retention	23% (27 of 116 sections)	31%
Openness	13% (15 of 116 sections)	6%

52% of the sections of the 2012 Statement of Rights and Responsibilities are categorized as either *Consent, Limiting Use/Disclosure/Retention* and *Openness*. Thus, the FIPs categories that underwent the most *Policy* changes between the 2011 and 2012 versions of the Statement of Rights and Responsibilities - *Limiting Use/Disclosure/Retention* and *Consent* - are the same FIPs categories that make up the 52% of the Statement of Rights and Responsibilities. Thus, 52% of the entire SRR was

coded as undergoing changes to policy between the 2011 and 2012 versions of the document.

User Concerns About the Statement of Rights and Responsibilities

Research Question 2: What are Facebook users' expectations of online privacy, as reflected in user comments outlining privacy concerns in response to Facebook's Statement of Rights and Responsibilities?

I then explored which privacy issues were of most concern to Facebook users, as reflected in their comments on the proposed changes to the Facebook SRR. 526 comments were made on the Facebook SRR document during the open commenting period between March 15 - March 23, 2012. All 526 comments were included in the data set for initial analysis. Table 8 shows the number of comments coded by each FIP. In total, 204 comments could be coded according to the FIPs definitions.

Table 8: Results of FIPs Coding of User Comments Made to SRR Changes Document

FIP Category	Number of Comments Regarding Each Concern	% of Total Privacy Comments (out of 316)
Consent	51	16%
Limited Collection	2	0.6%
Limiting Use/Disclosure/Retention	105	33%
Accuracy	5	1.5%
Safeguards	0	0%
Openness	41	13%
Accountability	0	0%
Identifying Purposes	0	0%
Individual Access	0	0%
Challenging Compliance	0	0%
Approval/Disapproval Statements	112	36%

Comments were coded most frequently according to *Limiting Use/Disclosure/Retention* (33% of 316 total privacy comments) and *Consent* (16% of 316 total privacy comments). As such, these two categories represent the FIPs categories that Facebook users are most concerned with in the Statement of Rights and

30

Responsibilities. The code that was least frequent was *Limited Collection* (0.6% of 316 total privacy comments).

There were 113 comments that were classified as *Approval/Disapproval Statements* (36% of 316 privacy comments). These 112 comments were not categorized according to FIPs definitions because they consisted of simple opinion statements, i.e. "I agree" or "I disagree". As such, I developed a code, *Privacy Comment*, to capture these comments. While these comments coded as *Privacy Comments* do refer directly to the Statement of Rights and Responsibilities, they could not be coded according to FIPs because there is not enough description within the comments for categorization. These results are also presented in Table 8.

Section 2.3 of the Statement of Rights and Responsibilities

Within the category of *Limiting Use/Disclosure/Retention,* issues related to the disclosure of personal information to third party applications (the policy stated in Section 2.3 of the Facebook SRR) were primary privacy concerns of individuals. 92% of user concerns that were categorized as *Limiting Use/Disclosure/Retention* were related to Section 2.3 of Facebook's Statement of Rights and Responsibilities. Of the 105 comments that were categorized as *Limiting Use/Disclosure/ Retention*, 97 comments made reference to Section 2.3 in the SRR. There were only 8 comments that made reference to sections of the SRR *other than* Section 2.3.

90% of user concerns that were categorized as *Consent* were related to Section 2.3 of Facebook's Statement of Rights and Responsibilities. Of the 51 comments that were categorized as *Consent*, 46 comments made reference to issues with SRR Section 2.3. This data indicates that within the category of *Consent*, issues related to the lack of

explicit consent regarding giving permission to third party applications accessing data were the primary privacy concerns of individuals.

Of the 41 comments that were categorized as *Openness,* only 5 made reference to issues with SRR Section 2.3. The remaining 36 comments made reference to SRR Section 14. This data indicates that although *Openness* concerns were addressed by Facebook users, the bulk of these *Openness* concerns were not related to Section 2.3 of the SRR.

Between the categories of *Consent* and *Limiting Use/Disclosure/Retention,* there were 143 user comments made about Section 2.3, making it the section of the SRR that received the most attention from users. Thus, of all the comments coded according to FIPs categories, 143 of 204 comments (or 70% of all comments) were related to SRR Section 2.3. Table 9 provides examples of user privacy concerns that specifically reference Section 2.3 of Facebook's Statement of Rights and Responsibilities.

Table 9: Example of Comments Categorized as *Limiting Use/Disclosure/Retention* and *Consent* that reference SRR Section 2.3

Statement of Rights and Responsibilities, Section 2.3	Example of User Comment	FIPs Category
When you or others who can see your content and information use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, read our Data Use Policy and Platform Page.)[1]	**Cathrine Word** I echo the sentiments of many in that I object to the change in clause 2.3. If I do not use apps and/or have them turned off, then apps should not have access to any of my data through any means muchless [sic] via my trusted friends!	*Limiting Use/Disclosure/Retention*
	Woody Eadie Section 2.3 is unacceptable. If I do not explicitly give an app permission to access my information, it should not have access to my information.	*Consent*

[1] Colour coding is copied from the 2012 Statement of Rights and Responsibilities track changes document.

The *Limiting Use/Disclosure/Retention* comment example outlined in Table 9 is a typical example of this category in that it references the limiting of user control over their personal data being enacted by the changes to Section 2.3.

The *Consent* comment example outlined in Table 9 is a typical example of a Section 2.3 *Consent* concern because it specifically addresses the permission or consent on the part of the user to allowing collection of personal information.

Comparison of User and Facebook Understandings of Privacy

Research Question 3: How do user and Facebook (as reflected in the SRR) conceptualizations of privacy compare to one another?

This stage of analysis examined how the representation of privacy found in the Facebook Statement of Rights and Responsibilities compares to the privacy expectations expressed by Facebook users in comments made on changes to the Statement of Rights and Responsibilities.

As discussed above, the section of Facebook's Statement of Rights and Responsibilities that was most commented on by users with concerns about *Consent* and *Limiting Use/Disclosure/Retention* of personal information was Section 2, Paragraph 3, which reads as follows:

> When you or others who can see your content and information use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, read our Data Use and Platform Page.)

Out of the 204 privacy comments made by users on the Statement of Rights and Responsibilities coded according to the FIPs, 143 made direct reference to Section 2.3 of the SRR. Analysis of the Statement of Rights and Responsibilities also revealed that Facebook rewrote Section 2.3 for the proposed 2012 SRR, and that this rewriting was a *Policy* change as opposed to a *Stylistic* change (see Table 6). Within user comments on changes made to Section 2.3 of the Statement of Rights and Responsibilities, user concerns about data control were expressed in 86 of 143 comments (or 60% of all comments about Section 2.3). Thus, the data indicates that the issues of most concern to Facebook users - i.e. data control related to Section 2.3 of the SRR - were tied to policy changes to the Statement of Rights and Responsibilities in the 2012 version of the SRR.

34

Discussion

Analysis of both the Facebook Statement of Rights and Responsibilities and user comments to proposed changes to the SRR revealed that both Facebook and users place emphasis on the same primary privacy issues: *Limiting Use/Disclosure/Retention* and *Consent.* In particular, Section 2.3 of the Facebook SRR garnered the most direct responses from users. In this section, I will discuss the findings of *Limiting Use/Disclosure/Retention* and *Consent* in relation to Facebook's representation of privacy, and the direction the organization is taking in terms of modifying their SRR according to policy and stylistic edits. Additionally, I will also discuss two themes that emerged across the user comments: data control and threats. The theme of data control describes user comments that discussed Section 2.3 of the SRR specifically in terms of how each user could (or could not) control their own data. The theme of threats describes user comments about Section 2.3 of the SRR that threatened some form of protest or leaving the site if this policy was not changed. I will explore these themes found in user comments made on the SRR to examine what user expectations of online privacy are. Finally, this section will address how Facebook and users differ in their expectations of privacy, in particular, focusing on how Facebook and users may view the ownership of personal data differently.

Limiting Use/Disclosure/Retention

Within the PIPEDA FIPs, *Limiting Use/Disclosure/Retention* is defined as

"Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes" (PIPEDA, 2011, p. 39).

Thus, this FIP is primarily concerned with how to *limit* the use of individual data to the purposes for which it was originally collected. The act of limiting access to individual data is an important aspect of information privacy (PIPEDA, 2011) that is addressed by both Facebook in the SRR, and users in their comments. As outlined in the Findings, 23% of the total sections of Facebook's Statement of Rights and Responsibilities were categorized as *Limiting Use/Disclosure/Retention*, aligning similarly with the 33% of total user privacy comments that were categorized as *Limiting Use/Disclosure/Retention*. These findings indicate that this category is of a great deal of importance to users and Facebook alike. Within the category of *Limiting Use/Disclosure/Retention*, many users address concerns directly related to Section 2.3 of the SRR – out of 105 comments in this category, 97 were about Section 2.3. The implications of user focus on Section 2.3 will be addressed below, but it is important to note that the comments addressing Section 2.3 that were classified as *Limiting Use/Disclosure/Retention* specifically addressed the fact that individuals felt the changes to this section involved their personal data being used and disclosed for purposes other than those for which it was originally collected. The specific purposes for which user data might be utilized are not laid out in the SRR, and user concerns about Section 2.3 indicate that this is important information to users. However, more information about what data is collected from users, and how this data is used/disclosed/retained is more clearly laid out in Facebook's Data Use Policy, which is referred to in the Statement of Rights and Responsibilities. Whether or not users are aware of these ancillary policies when reading the Statement of Rights and Responsibilities and expressing their comments and concerns over changes is an issue that needs to be addressed in future studies. These findings also indicate that, as

36

reflected in the fact that 23% of the entire Statement of Rights and Responsibilities addresses *Limiting Use/Disclosure/Retention* policies, Facebook is moving its representation of privacy closer to a model where the accessibility of user information is increased. However, a comparison of Facebook's representation of privacy to user expectations of privacy is furthered by a discussion of Section 2.3 of the SRR, where most of the user attention to concerns about *Limiting Use/Disclosure/Retention* is placed.

Consent

Within the PIPEDA FIPs, Consent is defined as

"The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate" (PIPEDA, 2011, p. 37).

Thus, this FIP is primarily concerned with the necessity of obtaining permission to collect personal information about individuals. There is a very important distinction between the categories of *Consent* and *Limiting Use/Disclosure/Retention.* Issues of *Consent* deal exclusively with individuals having knowledge and approval of what information is being collected about them, whereas *Limiting Use/Disclosure/Retention* is concerned with what happens to that information once permission is given to collect it. As such, the findings regarding *Consent* in both the Statement of Rights and Responsibilities and within user comments are quite interesting. 16% of the SRR was categorized as relating to *Consent*, and 16% of user comments were also categorized as *Consent.* Thus, these findings indicate that though *Consent* was a concern of commenting individuals, they still were more concerned about *Limiting Use/Disclosure/Retention.* However, user comments categorized as *Consent* also placed a great deal of attention on Section 2.3 of the SRR – out of 51 comments in this category,

46 were about Section 2.3. The comments addressing Section 2.3 that were classified as *Consent* specifically addressed the fact that individuals felt the changes to Section 2.3 gave third party applications permission to collect their personal data when they never gave consent to this collection. The findings related to *Consent* comments, and specifically comments addressing Section 2.3, once again indicate that Facebook is shifting its representation of privacy within policy as one of implicit consent (Hashemi, 2009), where when a user consents to using Facebook as a whole, they implicitly agree to share personal information with third parties without having to provide supplementary consent for this to occur.

User Privacy Expectations: Statement of Rights and Responsibilities, Section 2.3

When discussing privacy issues surrounding the proposed SRR, 45% of all users commented on Section 2.3 of the Facebook SRR, saying that they felt it violated their privacy by providing third party applications with access to their personal data, even though they did not explicitly consent to this practice. There are two ways of considering why users would view the practices outlined in Section 2.3 of the SRR as a violation of their privacy.

Data Control

In an opinion piece regarding the introduction of the News Feed to Facebook (another instance in Facebook's history that solicited user concerns about privacy violations), boyd suggests that "privacy in the OSN [online social network] context is a sense of control over information…, and the audience who can gain access [to that information]" (boyd 2008, p 18.). In this sense, user comments about Section 2.3 like

38

the one below, categorized as *Limiting Use/Disclosure/Retention*, can be read as protesting the perceived lack of control over personal data that comes about if third party applications are allowed access to personal information.

> **Deb Anderson** Strongly disagree -- I disagree with the changes as no person/app has a right to my information without my express permission. why should I be dragged into apps my friends are involved with? Under NO circumstances will I agree with the abuse of my rights and privacy.

Hoadley, Xu, Lee, and Rosson further discuss user privacy concerns online as arising out of an "illusory loss of information control" (2010). They describe an illusory loss of information control occurring when new features of a technology are introduced to individuals that make it *appear* as through individuals have less control over their personal data than they did previously (2010). In this case, illusory loss of information control related to Section 2.3 of the SRR is troubling to users because it emphasizes that users never *had* the control they thought they had (2010). The concept of illusory loss of information control that Hoadley, Xu, Lee, and Rosson outline can be applied to understanding user concerns over third party applications accessing their personal information without their consent.

Analysis revealed that Section 2.3 of the SRR was rewritten from the 2011 version of the SRR to include the phrase, *"When you or others who can see your content and information us an application".* This constitutes a policy-type rewrite on the part of Facebook (see Table 6), especially from the perspective of the users, who were seeing this phrase included in the Statement of Rights and Responsibilities for the first time. According to Facebook Vice President of Communications, Public Policy and Marketing, Elliot Schrage, "[t]he change in [the] SRR [of Section 2.3] was intended simply to reference the explanation that had long been in our privacy policy and now in our Data Use Policy" (SRR Update, https://www.facebook.com/fbsitegovernance/app_7146470109).

39

However, as the explanation of third party information access was not originally included in Section 2.3 of the SRR, the number of users who responded to this change with comments related to *Limiting Use/Disclosure/Retention* and data control (a total of 86 comments out of 143 comments related to Section 2.3) suggests that users perceived that Facebook was increasing the accessibility of their information without their consent, which raised user privacy concerns as a whole (Hoadley, Xu, Lee, & Rosson, 2010). In terms of data control, the proposed changes to Section 2.3 provided users with the same amount of control over the information third party applications had access to as in previous versions of the SRR - but this was the first time many users were made aware of the practice.

Another way to understand user concerns about Section 2.3 - specifically in relation to data control - is to explore the conceptual lens with which users may be approaching privacy. According to Allen (2000), there is an increasing movement to view privacy online strictly in terms of privacy-as-data-control. The view of privacy-as-data-control (or the privacy-control paradigm) aims to place the user as the central decision maker in regards to the control of their data online (Schwartz, 1999). The view that privacy is essentially about control over one's data online has proliferated in recent years, especially as social networking has increased in popularity (Allen, 2000; Cavoukian & Tapscott; Houghton & Joinson, 2010; Stutzman & Hartzog, 2011; Taraszow, Aristodemou, & Shitta et al., 2010). However, in recent years several theorists have begun to study privacy from a different conceptual approach than the privacy-control paradigm (Levin & Abril, 2009). These theorists define privacy as "the degree of inaccessibility of a person or information about [themselves] to others' five senses and surveillance devices" (Allen, 2000, p. 867).

40

A thorough reading of Facebook's proposed 2012 SRR indicates that Facebook is leaning more in the direction of understanding privacy as the accessibility or inaccessibility of individuals to other individuals (or, the privacy-as-dignity paradigm) rather than through the privacy-control paradigm. This is evidenced in the proposed changes to Section 2.3 of the Statement of Rights and Responsibilities (changes between 2011 and 2012 versions indicated in red):

> When you or others who can see your content and information use an application, your content and information is shared with the application. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, read our Data Use Policy and Platform Page.)

The inclusion of the sentence "you or others who can see your content and information" represents a policy change by Facebook, as revealed through analysis (see Table 6). These changes to Section 2.3 indicate that Facebook is moving towards a representation of privacy that is based on the accessibility of user data to other people, rather than the individual control of user data. Section 2.3 does not specify how each user can control their information - instead, it provides the user with information about who can access their information.

It is impossible for users to control all of their own data - not only do typical Internet users reveal information about themselves personally, but they're also tracked by information gathering processes across the web (Allen, 2000; Arshad & Cole, 2009). According to Schwartz, "because of the unreliable and adhesive nature of privacy agreements, even people using sites that offer opportunities to pre- authorize or refuse data collection and third-party disclosures, or that give notice of such practices, do not control personal information" (Schwartz, 1999; Allen, 2000). It would appear that Facebook understands the impossibility of individual control over information online,

and instead has chosen to focus its attention on providing users with privacy as inaccessibility from unauthorized individuals (as reflected in the SRR). However, a more "traditional" understanding of privacy-as-data-control seems to persist among users of Facebook, as evidenced by the 143 comments (*Information Use/Retention/Disclosure* and *Consent* concerns about Section 2.3 combined) that mention a lack of overall control of personal data as a critical privacy issue. The comment below is representative of a user concern about Section 2.3 of the SRR that specifically references data control.

> **Don Myra Gasser** 2.3 needs to change in two ways. Friends use of me [sic] FB information can not be shared with any other applications. It should be very easy to provide an option that turns this data sharing off if I don't approve of how this information is being shared. 6.3 is another "feature" that must have an opt out provision. I am not sure that you are taking the users right to control information seriously.

If Facebook is approaching privacy from a perspective of privacy-as-inaccessibility, and users are approaching privacy from a more traditional perspective of privacy-as-control-over-data (as reflected in the above exemplar comments), tension will continue to occur between the two parties. Thus, to answer the question of how users and Facebook understand privacy in comparison to one another, a case can be made that the conceptual expectations of privacy held by users who comment on the SRR, and Facebook's conceptual approach to representing privacy, are fundamentally different. This being said, it is also possible that a conceptual shift in expectations of privacy on the part of the users did not occur; rather, that user expectations of privacy on Facebook were defied due to a change in the illusory amount of control over data that users thought they had.

Threats

The issue of data control found in user responses to Section 2.3 of the SRR is complicated by the fact that every user is required to agree to the SRR when they first sign up for an account on Facebook. Third party applications do not have to ask for explicit permission to access the information of "Friends" because each member has given them implicit consent to do so, simply by signing up to use the site. The validity of implicit Terms of Service (TOS) consent online is discussed by Hashemi (2009), who questions whether a Statement of Rights and Responsibilities is even a "binding agreement" between the site and the user (Hashemi 2009, p. 152). One of the primary tensions between users and Facebook, as revealed by this study, is that Facebook believes that consent for *Information Use/Disclosure/Retention* via an unread Statement of Rights and Responsibilities is adequate, while certainly not all users agree.

Hashemi (2009) also points out that there is a marked difference between what is offensive to individual expectations of privacy, and what is illegal. Though Facebook's Statement of Rights and Responsibilities entitles the site to share user information with third party applications (as specified in Section 2.3 of the SRR), that does not mean that users will accept this as a valid practice and see it as anything but an offensive practice (Hashemi, 2009). As long as Facebook can legally back up their position that users' personal data is available to share with third party applications through their Statement of Rights and Responsibilities, the only recourse users have to protest the lack of control over their personal information is to stop using Facebook's services altogether (Hashemi, 2009) - a threat that 25% of users made when referencing Section 2.3 in their *Information Use/Disclosure/Retention* and *Consent* concerns (see example below).

43

> **Scott Mortenson** "Sharing your contact and information" #2.3 is a violation of basic human common sense -- the applications my friends use should not have access to my information without my prior permission. If this clause indicates my (silent) prior permission, I will revoke my Facebook membership. It is plain stupid that I have no control over my info without cancelling [sic] my account.

The concern about Section 2.3 is not, according to many user comments, that users are not generally aware of Facebook's policies and privacy practices. The issue is that Facebook is not required by US law to provide "adequate" notice of changes to its users (Hashemi, 2009). This is problematic from the point of view of the user, who sees it as a betrayal of control over their own personal information (Hashemi, 2009), as well as in terms of the specifications laid out by PIPEDA. However straightforward data control and threats privacy concerns appear to be, their roots originate in a conceptual gap between Facebook and users. Section 14 of the SRR places an obligation on the user to get notice of future policy changes by "liking" the Facebook Site Governance page, and Facebook places this obligation on the user as an attempt to pass off responsibility for communicating policy changes (Hashemi, 2009). Though users may demand that Facebook inform them of changes made to official site documentation, and give them the opportunity to vote on them (something only afforded to them if over 7000 individuals comment on a document, specified in section 14.3 of the SRR), Facebook is not legally required to do this in the U.S. It is important to note that different international policies – specifically, the Statement of Rights and Responsibilities applied to German users – may put enact different legal responsibilities on the part of Facebook. However, for the purposes of this study, only the policies put forth in the English version of the Statement of Rights and Responsibilities were studied. The issue of threats seems to be less about differing conceptual expectations of privacy between

Facebook and its users, than a differing opinion on how privacy policies should be implemented (Hashemi, 2009).

Conclusion

The findings of this MRP indicate that there are significant conceptual gaps between how Facebook represents privacy in its Statement of Rights and Responsibilities, and what user expectations of privacy online are.

Overall, Facebook spends the majority of the Statement of Rights and Responsibilities (52% of the document) establishing policies related to Limiting Use/Disclosure/Retention and Consent of user data. However, these policies also represent the bulk of the changes between the version of the Statement of Rights and Responsibilities released in 2011, and the proposed Statement of Rights and Responsibilities in 2012. Additionally, analysis indicated that the changes made between the 2011 and 2012 versions of the SRR were policy changes as opposed to stylistic changes. In total, there were policy changes made to 56% of SRR sections categorized as Limiting Use/Disclosure/Retention and Consent, representing a notable departure from policies established in previous versions of the SRR.

It was the departure from the Limiting Use/Disclosure/Retention and Consent policies presented in the 2011 version of the Statement of Rights and Responsibilities that raised the most concern on the part of the user. Specifically, Section 2.3 of the SRR was flagged by users as defying their expectations regarding their privacy rights online. 45% of users who chose to comment on changes made to the Statement of Rights and Responsibilities commented on Section 2.3; these 143 of 316 privacy related comments then revealed further user concerns. When discussing Section 2.3, users primarily focused on how the new version of this section changed the data control of the user, while secondarily threatening to leave the site if Section 2.3 was not re-written. However, just because FIPs other than Limiting Use/Disclosure/Retention and Consent

were not captured in user comments on the Statement of Rights and Responsibilities does not mean that user concerns related to other FIPs do not exist. Had I analyzed Facebook's comprehensive privacy policies and user comments made to those documents, the FIPs not captured in the SRR and user comments may have been reflected.

Research has also shown that individuals have many privacy concerns online, and that not all of these concerns (especially dignity or identity related privacy concerns) are captured through the FIPs (Levin & Abril, 2009). When Facebook frames the discussion of site privacy policy changes solely in the context of changes made to the Statement of Rights and Responsibilities, users tend to focus on these specific changes when thinking and commenting about privacy, and may not respond with other privacy concerns that they have (Smith et al, 2006). In other words, just because Facebook and its users focus on certain privacy issues – in this case, Consent and Limiting Use/Retention/Disclosure issues with Section 2.3 of the Statement of Rights and Responsibilities – does not mean that those issues encapsulate the entire conversation to be had about privacy and Facebook. Although Facebook changed certain terms of their Statement of Rights and Responsibilities, and users responded to these changes both negatively and positively, research shows that there are other privacy related issues and user concerns that did not come to light in the context of my MRP.

Finally, the change of policy in relation to Section 2.3 of the Statement of Rights and Responsibilities revealed a significant fissure between Facebook's representation of privacy through policy, and user expectations of privacy online. The language and practices represented in Section 2.3 of the SRR move the policies of the site towards a conception of privacy-as-inaccessibility. However, user comments in response to Section

2.3 revealed that individuals generally continue to view privacy through the data-control paradigm, and that they expect Facebook to be operating under the same privacy paradigm. In other words, Facebook appears to be moving the policies of the site toward an understanding of privacy-as-in/accessibility, while users continue to expect privacy through the data-control paradigm. Whether approaching user expectations of privacy by looking at the privacy-control paradigm or through the disruption of expected information flow, it would appear this concern is rooted in conceptual gaps between the user and Facebook. Until the conceptual privacy gap between Facebook and users is closed, privacy tension between the two parties will remain.

Research Limitations

It is important to note that many users who commented on the changes made to the SRR may have been individuals who were always more inclined to be concerned about their privacy than others (Xu, Dinev, Smith & Hart, 2011). As the data set of this study was collected from publicly available information, I did not contact any commenters for follow-up interviews regarding their privacy concerns. Additionally, it is quite possible that the viewpoints of those with privacy concerns who were *not* fans of the Site Governance page (i.e., those users who did not "like" the page, and thus were not informed of any Site Governance announcements or changes from official Facebook sources) had no way to comment on the proposed changes. This is a function of the Facebook site infrastructure, and is an issue that could be examined at more length in a future study. Smith et al. (2006) point out that media coverage often increases the level of concern individuals feel about any particular issue; the level of media coverage regarding Facebook's changes to the SRR could have attracted commenters who would otherwise be disinclined to comment.

Epilogue

On March 22, 2012, Facebook.com closed the commenting thread on the 2012 proposed Statement of Rights and Responsibilities. On the Facebook Site Governance page, they thanks users for their participation, and stated that they "plan[ned] to review and analyze [user] comments over the coming days and [would] keep [users] posted on the next steps" (Facebook Site Governance Timeline Post, March 22, 2012). Two weeks later, on April 14, 2012, Facebook released a Statement of Rights and Responsibilities Update. In this update, Facebook addressed many of the user concerns that arose in the commenting thread, paying particular attention to comments about Section 2.3 of the Statement of Rights and Responsibilities.

In addition to directly addressing user concerns, Facebook used this update to "revise" and repost the 2012 proposed Statement of Rights and Responsibilities, along with a long letter explaining the sections that were most commented on. The site then re-opened the document to user comments, and asked for similar feedback as the first round of commenting. Despite directly addressing and answering user concerns that arose in the original commenting period, Facebook did not make any changes to the 2012 reposted proposed changes to the Statement of Rights and Responsibilities.

A record of each commenting period, along with the Statement of Rights and Responsibilities Update letter, can be found in the Facebook Site Governance Archive: https://www.facebook.com/fbsitegovernance/app_7146470109

Bibliography

Abril, P. S., Levin, A., & Riego, A. D. (2012). Blurred Boundaries : Social Media Privacy and the Twenty-First-Century Employee. *Spring, 49*(1), 63-124.

Acquisti, A., & Gross, R. (2006). Imagined Communities : Awareness , Information Sharing , and Privacy on the Facebook. *Public Policy*, 1-22.

Allen, A. L. (2000). Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm. *Connecticut law review, 32*(3).

Arshad, J., & Cole, M. (2009). Towards a Taxonomy of Privacy Concerns of Online Social Network Sites: A Case Study of Facebook Beacon. In A. Poulymenakou, N. Pouloudi, & K. Pramatari (Eds.), *4th Mediterranean Conference on Information Systems*. Athens: Athens University of Economics & Business.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9), 11–15. Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394/1312

Benbasat, I., Bulgurcu, B., & Cavusoglu, H. (2010). Understanding Emergence and Outcomes of Information Privacy Concerns: A Case of Facebook. *Thirty First International Conference on Information Systems* (pp. 1-11). St. Louis.

Bloustein, E. J. *Individual and group privacy*. New Brunswick, N.J.: Transaction Books, 1978. Print.

boyd, D.M. (2008). Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence. *Convergence*, 14 (1).

boyd, D. M., & Ellison, N. B. (2007). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication, 13*(1), 210-230. doi:10.1111/j.1083-6101.2007.00393.x

Cavoukian, A., & Tapscott, D. (2006). *Privacy and Enterprise 2.0.*

Canadian Minister of Justice (2012). Personal Information Protection and Electronic Documents Act (PIPEDA). *ReVision*. http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

Cohen, N. (2012, April 24). The Breakfast Meeting: Grilling for James Murdoch, and Facebook Tops 900 Million Users. *The New York Times*. Retrieved from http://mediadecoder.blogs.nytimes.com/2012/04/24/the-breakfast-meeting-grilling-for-james-murdoch-and-facebook-tops-900-million-users/

51

Culnan, M. J. (1993). "How did they get my name?": an exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly, 17*(3), 341-363.

Cutillo, L. A., Molva, R., & Strufe, T. (2009). Safebook : A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust. *IEEE Communications Magazine*, (December), 94-101.

Dwork, C. (2006). Differential Privacy, 1-12.

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *Americas The* (Vol. 123). Citeseer. Retrieved from http://scholar.google.com/scholar?q=intitle:Trust+and+privacy+concern+within+social+networking+sites:+A+comparison+of+Facebook+and+MySpace#0

Ess, C. (2005). "Lost in Translation"?: Intercultural Dialogues on Privacy and Information Ethics (Introduction to Special Issues on Privacy and Data Privacy Protection in Asia). *Ethics and Information Technology, 7*(1).

Facebook, Inc. (2012, February 1). Initial Private Offering. *United States Securities and Exchange Commission*. Washington, D.C. http://sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm

Facebook Site Governance Page. (2012). https://www.facebook.com/fbsitegovernance

Facebook Terms and Policies. (2012). https://www.facebook.com/policies

Facebook Statement of Rights and Responsibilities. (2012). https://www.facebook.com/legal/terms

Foster, M., West, T., & Levin, A. (2011). The Last Frontier: Targeted Online Advertising and Privacy. *Ted Rogers School of Management*. Retrieved from: http://www.ryerson.ca/content/dam/tedrogersschool/privacy/Targeted_Online_Advertising_and_Privacy.pdf

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

Grimmelmann, J. (2008). Facebook and the Social Dynamics of Privacy. *Iowa Law Review, 95*(4), 1-52. SSRN. Retrieved from http://works.bepress.com/james_grimmelmann/20/

Gross, R., & Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks (The Facebook case). *Human Factors*, 71-80. ACM Press. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Information+

[Revelation+and+Privacy+in+Online+Social+Networks+(+The+Facebook+case+)](#)
[#3](#)

Hashemi, Y. (2009). Facebook's Privacy Policy and Its Third-Party Partnerships: Lucrativity and Liability. *Boston University Journal of Science & Technology Law*, *15*(14).

Hoadley, C. M., Xu, H., Lee, J. J., & Rosson, M. B. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic Commerce Research and Applications*, *9*(1), 50-60. Elsevier B.V. doi:10.1016/j.elerap.2009.05.001

Houghton, D. J., & Joinson, A. N. (2010). Privacy, Social Network Sites, and Social Relations. *Journal of Technology in Human Services*, *28*(1-2), 74-94. doi:10.1080/15228831003770775

Hsieh, H.F., & Shannon, S.E. (2005). Three Approaches to Qualitative Content Analysis. *Qualitative Heath Research, 15*(9), 1277-88. doi: 10.1177/1049732305276687

Hull, G., Lipford, H. R., & Latulipe, C. (2011). Contextual gaps: privacy issues on Facebook. *Ethics and Information Technology*, *13*(4), 289-302. doi:10.1007/s10676-010-9224-8

Krishnamurthy, B., & Wills, C.E. (2008). Characterizing privacy in online social networks. *Proceedings of the first workshop on online social networks, 1*, 37-42. doi>10.1145/1397735.1397744

Levin, A., & Abril, P. S. (2009). Two Notions of Privacy Online. *Business*, 1001-1051.

Lindlof, T.R., & Taylor, B.C. (2011). *Qualitative Communication Research Methods*. 3 ed.

Margulis, S. T. (1977), Conceptions of Privacy: Current Status and Next Steps. *Journal of Social Issues, 33*: 5–21. doi: 10.1111/j.1540-4560.1977.tb01879.x

Margulis, S. T. (2003a), Privacy as a Social Issue and Behavioral Concept. *Journal of Social Issues*, *59*: 243–261. doi: 10.1111/1540-4560.00063

Margulis, S. T. (2003B), On the Status and Contribution of Westin's and Altman's Theories of Privacy. *Journal of Social Issues, 59*: 411–429.   doi: 10.1111/1540-4560.00071

Nissenbaum, H. (2004). Privacy as Contextual Integrity. *Washington Law Review*, 101-139.

Renaud, K., & Galvez-Cruz, D. (2010). Privacy: Aspects, definitions and a multi-faceted privacy preservation approach. *Information Security for South Africa*, 1-8. Ieee. doi:10.1109/ISSA.2010.5588297

Rotenberg, M. (2012). Marc Rotenberg: What's Privacy in the Age of Facebook?. *The Huffington Post.* Retrieved April 12, 2012, from http://www.huffingtonpost.com/marc-rotenberg/whats-privacy-in-the-age_b_299466.html

Schoeman, F. D. (1984). *Philosophical dimensions of privacy: an anthology.* Cambridge [Cambridgeshire: Cambridge University Press.

Schwartz, P.M. (1999). Privacy and Democracy in Cyberspace. *Vanderbilt Law Review. 52.*

Smith, H. J. (2008). Examining the Formation of Individual ' s Privacy Concerns : Toward an Integrative View. *International Conference on Information Systems.* Retrieved from http://faculty.ist.psu.edu/xu/papers/conference/icis08a.pdf

Solove, D. (2004). *The Digital Person - Technology and Privacy in the Information Age.* New York University Press.

Solove, D. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, *154*(3), 477-564.

Solove, D. (2008). *Understanding Privacy.* Cambridge, Massachusetts: Harvard University Press.

Strater, K. & Lipford, H.R. (2008). Strategies and struggles with privacy in an online social networking community. In *Proceedings of the 22nd British HCI Group Annual Conference on HCI 2008: People and Computers XXII: Culture, Creativity, Interaction - Volume 1.*, 78 - 88

Strauss, A., & Corbin, J. (1994). Grounded theory methodology. In N. K. Denzin & Y. S. Lincoln (Eds.),

Handbook of qualitative research (pp. 273-285). Thousand Oaks, CA: Sage

Stutzman, F. D., & Hartzog, W. N. (n.d.). Boundary Regulation in Social Media. *Media*, 1-35.

Taraszow, T., Aristodemou, E., Shitta, G., Laouris, Y., & Arsoy, A. (2010). Disclosure of personal and contact information by young people in social networking sites: An analysis using Facebook™ profiles as an example. *International Journal of Media and Cultural Politics*, *6*(1), 81-101. doi:10.1386/macp.6.1.81/1

Van Eecke, P., & Truyens, M. (2010). Privacy and social networks. *Computer Law & Security Review*, *26*(5), 535-546. Elsevier Ltd. doi:10.1016/j.clsr.2010.07.006

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

Westin, A. F. *Privacy and freedom*. 1st ed. New York: Athenaeum, 1967. Print.

Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *Faculty Scholarship Series.* Paper 649. http://digitalcommons.law.yale.edu/fss_papers/649/

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information Privacy Concerns : Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems Information Privacy Concerns*, *12*(12), 798-824.

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting User Concerns About Online Privacy. *Journal of the American Society for Information Science*, *58*(February), 710-722. doi:10.1002/asi

Young, A. L., & Quan-Haase, A. (2009). Information Revelation and Internet Privacy Concerns on Social Network Sites : A Case Study of Facebook. *Public Policy*, *5*(14), 265-273. ACM. doi:10.1145/1556460.1556499

Zhang, Y., & Wildemuth, B. M. (2005). Qualitative Analysis of Content by, 1-12.