

Human Communication. A Publication of the Pacific and Asian Communication Association.
Vol. 14, No. 1, pp.39–55.

Privacy Setting Awareness on Facebook and Its Effect on User-Posted Content

Elizabeth Butler
King's College
133 North River Street, Box 8015
Wikes-Barre, PA 18711
570-590-6557(cell) elizabethbutler@kings.edu

Elizabeth McCann
King's College
133 North River Street, Box 7044
Wikes-Barre, PA 18711
610-653-8534 (cell) elizabethmccann@kings.edu

Joseph Thomas
67 Church Street
Plymouth, PA 18651
570-706-5751(cell) josephthomas@kings.edu

Abstract

This study explored the relationship between changing privacy policies on social networking site Facebook and its users' awareness of the personal privacy settings they have in place. The intricate and constantly changing privacy policies on the site require users to be extremely attentive to its updates in order to retain a true awareness of personal privacy settings. When users are unaware of these settings, the content and personal information they post could potentially be accessible by larger audiences than initially intended. This phenomenon is particularly critical in an age where social media—specifically Facebook—has become one of the most prominent forms of day-to-day communication. This research study utilized a 25 question survey to gauge the opinions and perceptions of Facebook users ages 18 and older. Upon completion of the survey, respondents were given the option to participate in a content analysis in which personal Facebook identification numbers were provided to the researchers. The researchers reviewed the respondents' Facebook profiles to determine if the perceived settings reported were consistent with the respondents' actual personal privacy settings. These results were then compared to users' awareness of Facebook's changing privacy policies to determine if a relationship existed, and to ultimately answer the research question.

Keywords: Facebook, online privacy, social media, changing privacy policies, privacy awareness

Introduction

There's no denying it: a social revolution is upon us. Throughout the past decade, social media has become so pervasive in our society that many users cannot go a day without it. This new form of media is not a fad; it is a fundamental shift in the way we communicate, and has connected the world in ways previously unheard of. Specifically, social networking site Facebook has been declared the most visited site on the web by Google Analytics as of April 2010 (Warman, 2010). While television and radio took as long as 10 years to reach 50 million users, Facebook reached 200 million in just one year (Qualman, 2009). According to Facebook (2010c), "Facebook reports having more than 500 million active users, who spend over 700 billion minutes per month on the site" (para. 1). Each of these users posts an average of 90 pieces of content per month (Facebook, 2010c). Therefore, Facebook disseminates information between users; it is a platform for sharing photos, statuses, links, videos, and just about any other content you can think of. This is clearly stated in the site's mission statement: "Facebook's mission is to give people the power to share and make the world more open and connected" (Facebook Info, 2010, para. 4). So what happens when people don't quite understand this "power to share" that Facebook provides them?

Concerns over privacy are nothing new for the social networking site. Since its inception in 2004, founder Mark Zuckerberg has acknowledged the fact that users need a way to control how and what they share (Qualman, 2009). When the "news feed" was first introduced in 2006, users were outraged. They protested relentlessly that the new feature was a violation of privacy and that they didn't want their every move to be broadcasted to the entire Facebook community. Today, it is the first thing we see when we log in – and we think nothing of it. Facebook has undergone several such "evolutions" throughout its six year lifespan, with numerous modifications and additions to its privacy policy. Each change, however minor it may be, affects the personal information and shared content of over 500 million users.

When Facebook changes its privacy policy, users are notified with a small dialog box at the top of their "home" screen, which includes a link to further information on the modification. Do Facebook users take the time to follow this link and investigate what has changed? Many users believe that they take adequate precautionary measures by simply monitoring what friends they accept, as they assume those are the only users that can see the content they post. According to Grimmelman (2010), "social networking sites activate the subconscious cues that make users think they are interacting within bounded, closed, *private* spaces" (p. 803). In December 2009, Facebook rolled out an entirely new privacy structure on the website, with "recommended" privacy settings selected as the default level of control for each user. These "recommended" settings allow statuses, photos, and wall posts created by the user to be viewed by "everyone" – the entire Facebook community. Suddenly, user-posted content was accessible by larger audiences than most people intended. According to the Electronic Frontier Foundation (2009), Facebook implemented these changes so that they "could have a better stream of content to go against Twitter in the real-time search race" (para. 10). The Electronic Frontier Foundation (EFF) purported that the changes were for the good. EFF (2009) stated the site was "forcing all of its users to actually pay attention to the specifics of their privacy settings" (para. 7). Whether or not users actually did pay attention is a different story.

What are the implications of users being potentially unaware of their privacy settings? It seems every week, there is another story of an employee losing their job over a Facebook status, a marriage breaking up due to tagged photos of a cheating spouse, or a child being cyber-bullied

on a network that was once thought to be secure. The story is similar in each instance: users weren't aware that their statuses, photos, and other posted content were accessible to a larger audience than intended; they felt a sense of protection within the boundaries of their own profiles. These stories are only of the individuals who have suffered public consequences due to their privacy settings. There may be countless other Facebook users with the same misconception about their security on the site – it just so happens that the issue has not been brought to their attention yet. These Facebook users could potentially be exposing details of their personal lives and explicit contact information to many people, unknowingly putting themselves at risk for information violation.

With so many cases of Facebook privacy issues in the news, it leads one to wonder: could these instances have been prevented if users were knowledgeable of Facebook's changing privacy policies, and adjusted their personal settings accordingly? Is true privacy even possible on a website created for sharing information? Moreover, is privacy possible at all on the World Wide Web? This research study seeks to identify a relationship between users' efforts to investigate the site's privacy policy revisions and their awareness of their current privacy settings on the site. The study surveyed individuals about their opinions and perceptions of Facebook in order to gain an understanding of how users feel about the importance of privacy, what they believe their current settings are, and whether or not they have a true awareness of those settings. The researchers then analyzed the respondents' Facebook profiles to determine if their perceived privacy settings were consistent with their actual privacy settings. The study seeks to answer the research question, "To what extent do the changing security features of personal privacy settings on social networking site Facebook allow personal postings to be viewed by a broader audience than intended by the end user?"

Review of Literature

The review of literature will lay the theoretical framework upon which this research study was designed. The researchers will first provide a background on privacy issues and how they have come to be viewed over time. Next, the history of Facebook privacy is discussed, specifically in regard to its constantly-evolving privacy policy. Finally, the researchers describe the theory upon which the research study was based and evaluated, as well as explore relevant literature to the topic.

Privacy Issues: A Background

Privacy issues in regard to human autonomy are certainly nothing new. Since the development of the printing press, humans have experienced an increased ability to share information with mass audiences. This development greatly increased the possibility of violating another individual's personal privacy, as facts could now be relayed instantly and simultaneously with an unlimited number of individuals. Facebook and other modern technological advancements have only contributed to the various ways information can be shared on a larger scale; therefore, the issue of privacy has come under increasing scrutiny within the past several years.

Despite its importance today, the word "privacy" does not even appear in the United States Constitution or Bill of Rights (Goldsborough, 2010, p. 72). Aside from the Fourth Amendment's prohibition of unreasonable governmental searches, the government early on had nothing to say on the matter of privacy. The issue was addressed for the first time nationally in 1890 when Samuel Warren and Louis Brandeis published *The Right to Privacy*, a famous Harvard Law Review (Allen, 2001). According to Allen (2001), the public now has an obsession with privacy,

As a culture, we are obsessed with privacy, and so we express outrage when others invade our privacy; but we are equally obsessed with the private, and so we are mass consumers of other people's private lives and willing purveyors of our own. How did we come to be this way? (p. 302)

Allen (2001) explained that this obsession began in the 1960s, with the Supreme Court popularizing the idea of legal rights to privacy. The Cold War, the conflict in Vietnam, and racial turmoil over civil rights raised Americans' concerns about government surveillance, espionage, and social control (Allen, 2001).

By the 1970s, some Americans came to see the newly developing high-speed computers as potential threats to their informational privacy (Allen, 2001). Because of the potential threats to informational privacy, federal lawmakers joined together to form the U.S. Privacy Protection Study Commission in 1977 (Allen, 2001). This national commission published a two-volume report, *Personal Privacy in an Information Society*, which recommended that fair information practices be implemented in the collection, storage, and use of personal information about individuals (Allen, 2001). By the 1990s, computers had become common in households and were no longer viewed as dangerous, invasive devices (Allen, 2001). Instead, computers were viewed in a positive light, as they provided new ways for humans to communicate with the outside world. Anyone with a computer and an internet connection could e-mail, chat, or join online communities that connected individuals in different parts of the world. In February 2004, the largest and most successful social networking service to date was founded—Facebook.com.

Facebook Privacy History

Facebook was created by Harvard University student Mark Zuckerberg and his roommates Dustin Moskovitz and Chris Hughes (Kinkoph Gunter, 2010). Originally called *The Facebook*, Zuckerberg, Moskovitz, and Hughes' invention was meant to be a way for college students to connect with their fellow students at Harvard, but it quickly spread to other colleges in the Boston, Massachusetts area. In 2005, the domain Facebook.com was purchased for \$200,000 (Williams, 2007). By the end of 2006, Facebook became open to the entire public—not just college students. This change allowed anyone with an internet connection and a valid email address to access the site and the information contained there. This year also saw the introduction of the “news feed”—a Big Brother-like feature that broadcasted users' actions on the site to all of their friends. Many users felt this was a violation of privacy and protested fervently, but to no avail—the news feed remains today.

Throughout the next several years, Facebook steadily decreased the default privacy settings of each user. In 2007, Facebook began its opt-out approach, informing users that they must take action if they want their privacy protected (EFF, 2010). According to the EFF (2010), Facebook's policy in 2007 read, “Your name, school name, and profile picture thumbnail will be available in search results across the Facebook network unless you alter your privacy settings” (para. 5). Therefore, Facebook dictated privacy settings to its users, which could only be changed if they opted out of the settings. By 2009, the privacy policy was updated to note that the default settings for certain profile information was now set to “everyone.” According to the EFF (2010) this meant that the information,

may be accessed by everyone on the Internet (including people not logged into Facebook), is subject to indexing by third party search engines, may be associated with you outside of Facebook (such as when you visit other sites on the internet), and may be imported and exported by us and others without privacy limitations. (para. 7)

With this update to the policy, it now seemed that no information could truly be “private” on Facebook. In April 2010, Facebook once again modified the policy to further explain the “everyone” setting, and to inform users that fan pages they “liked” were also now visible to everyone. Clearly, over time, the site intentionally altered the way users controlled their personal data to create a more open flow of information on the site.

Current Settings & Issues

In today’s ever-changing technological world, maintaining privacy is a challenging task. People may claim that it is common sense not to share personal information such as your email address, cell phone number and home address on a website. However, these sorts of information are exactly what Facebook wants its users to share. Social networking sites are purposely created so users can divulge personal information in order to connect with others. The problem is that as a society, users tend to overshare information, whether knowingly or unknowingly. This overshare could potentially lead to trouble both personally and professionally.

Creator Mark Zuckerberg has challenged our society’s obsession with privacy. Facebook is currently designed to share the majority of your information with “everyone,” all members of the site. These settings can only be modified if users take the time to opt out and set stricter guidelines for their specific profiles. This excessive openness on the site has been cause for much controversy within the past year. Canadian journalist Cowan (2010) relayed that “Critics of Zuckerberg say he is a false prophet who claims his generation values openness, and casts anyone who cares about privacy as an old-fashioned fuddy-duddy” (p. 28). Cowan (2010) reported that Mark Zuckerberg lists “openness” in his areas of interest on his Facebook profile page. While Zuckerberg might want to share all his information, it seems unlikely that every Facebook user agrees and wants to share all of their information. It could be that many Facebook users are simply unaware of their privacy settings, and Facebook’s privacy policy in general.

What began as less than 1,000 words in 2004, Facebook’s privacy policy is now longer than the U.S. Constitution (Cowan, 2010). The policy was last revised October 5, 2010 and is currently broken down into nine sections to help its users better understand how the social networking site uses their information. Within the policy, Facebook offers links back to the personal privacy settings page, where users can go in and make edits after learning what the policy entails. This is important for the average user to know so they can control their privacy settings. According to Veer (2010), “Facebook assumes you want the whole world to see your personal info until you tell it differently. Your information is at risk until you adjust your settings” (p. 209).

The issue that arises is that users often fail to control their privacy the way they’d like. The increasingly intricate privacy page now has 50 different settings, with 170 different options, so it’s no wonder some users don’t fully understand it (Cowan, 2010). Upon first creating a Facebook profile, the privacy of users’ statuses, photos, posts, current city, and hometown information is set to “everyone” by default. Facebook’s desire for user openness is also evidenced throughout the “Connecting on Facebook” page – with statements such as “Set your search options to Everyone or you could miss out on friend requests” and “Set your friend request access to Everyone to avoid missing out on chances to connect with people you know” (Facebook, 2010). Clearly, Facebook encourages users to keep the site’s default privacy settings instead of adjusting them to a stricter level. However, many users do not even know how to go about accessing or modifying this information. Instead of investigating how privacy operates on Facebook, many users simply continue to go about their daily business on the site, uploading

countless pieces of content. Facebook has become a cornerstone in so many users' lives that they cannot imagine going a day without it. Cowan (2010) stated "Facebook is different from almost any other product or service in the enormous degree of emotional and time investment it demands from its users" (p. 28). This demand is so high that users post 25 billion pieces of content each month, from photos, to links, to statuses – putting privacy on the backburner in their minds (Cowan, 2010).

Theoretical Framework and Relevant Literature

The privacy policies Facebook currently operates under can be evaluated using the Restricted Access/Limited Control Theory of Privacy (RALC). According to Tavani (2007), an individual has privacy under the RALC theory "in a situation with regard to others [if] in that situation the individual . . . is protected from intrusion, interference, and information access by others" (p. 10). These "situations," according to Tavani (2007), can be activities, relationships, or the storage and access of information in a computer environment. To have privacy under this theory, an individual need not have absolute control over information about oneself. Instead, one needs to have control with respect to three elements in a situation: choice, consent, and correction (Tavani, 2007). How can one have privacy when personal information is in the hands of another entity? Tavani (2007) described a scenario:

To see how the notion of control works in the RALC framework, consider the example of one's medical information. That information is private because a normative zone has been established to restrict people from accessing the information, not because an individual has complete control over who has access to that information within a medical setting. Doctors, nurses, financial administrators, and insurance providers may have legitimate access to various pieces of it. (p. 11)

This concept is applicable to Facebook because users do not have absolute control over the information they post; technically, Facebook does. However, users do have the power of choice, consent and correction: they make the choice to voluntarily upload information about themselves, thus giving consent to the website to display it in their profiles. Users also have the option of correction – they can alter or remove the information at any time.

Therefore, it seems as if Facebook offers users an adequate level of privacy – so what causes the disconnect leaving so many users unaware of their privacy settings? The problem is that users don't typically view Facebook privacy as something that deserves a lot of thought or attention. This was evidenced by the latest privacy design change in December 2009, whereby only 35% of Facebook users adjusted their settings (Grimmelmann, 2010). The other sixty-five percent, some 250,000,000 users, must have fully approved of the website's changes—or were simply unaware that they took place. Users care deeply about privacy settings, but they have a great trouble achieving it. According to Grimmelmann (2010), that trouble is not their fault; rather, it arises out of the quite natural difficulty they have in understanding what will happen to their personal information once they post it on the World Wide Web. Grimmelmann declared that users of the site massively misunderstand its privacy architecture and settings, as it is difficult to know who can view each piece of content you post. "The most basic heuristic of privacy self-help-know your audience-is hard to use in an electronically mediated environment that gives you little feedback on who any given communication is visible to" (Grimmelmann, 2010, p. 802-803). Aside from the users who "like" or comment on your posted content, there is no way of knowing how large of an audience you actually reached. Even so, users aren't shy about sharing very personal information, and seem to maintain a trust that Facebook is a safe platform. According to Grimmelmann (2010),

A typical Facebook profile contains answers to most of the questions employers are not allowed to ask of job applicants: race, sex, age, national origin, religion, and marital status. People are

voluntarily uploading it all because they are social and because Facebook scratches social itches.
(p. 811)

Overall, it seems users care more about making an identity for themselves on the social networking site, than managing who can view that identity. With each update to its privacy policy, Facebook is undoubtedly revealing greater and greater amounts of its users' personal information. However, because users are so accustomed to their daily routines on the website, they often fail to investigate the changes that Facebook does implement. This growing phenomenon sparked the researchers' interest in the topic, and provided the basis for the research question. The research study sought to determine if users' perceived settings were consistent with their actual settings, and whether or not this was affected by their knowledge of Facebook's changing privacy policies.

Methods

The methods section of this research paper will address the design, procedures, and considerations of the research study. It will also detail the population and the actions the respondents took in order to participate, as well as describe the data collection and analysis.

Research Design

To answer the proposed research question, the researchers designed a study to evaluate Facebook privacy setting awareness. The research study was descriptive in nature and non-experimental, as there was no randomization or manipulation of variables. The study utilized a survey and content analysis to determine if a relationship existed between the efforts users make to keep up to date on changing privacy policies, and their awareness of current personal privacy settings. The 25 question survey and opt-in content analysis were available on the website SharePoint for participants to take voluntarily.

Population

According to Keyton (2011), "The researcher must identify the appropriate population that will best satisfy the expectations presented by the research questions or hypotheses" (p. 122). Therefore, because this study focuses on Facebook privacy settings, it was necessary for participants to be active members of the social networking site. Participants were also required to be over the age of 18, but the target age range for the survey was 18 to 30. Participants consisted of the researchers' friends on Facebook, as well as freshman and sophomore students at King's College who opted to participate. The researchers' friends on Facebook were contacted via a Facebook event invitation, and the freshman and sophomore students were contacted via a student-out e-mail. Overall, the total sample size was approximately 2029 individuals. The projected number of research participants for the study was 250-300 individuals. The final number of respondents was 235, 102 of which opted to participate in the content analysis.

Data Collection

The majority of the questions in the survey were utilized to descriptively explain users' opinions and perceptions of their privacy on Facebook, and to gain an understanding of their habits on the social networking site. Users who opted to participate in the content analysis were evaluated in two further ways. First, the researchers accessed the users' Facebook profiles from the perspective of someone who is not Facebook friends with them, but had friends in common with them. They compared the users' perceived personal privacy settings (how they answer the survey questions) to what their actual settings were (what the researchers discover upon evaluation of their profiles). The findings of this content analysis were then compared to question 21 of the research survey, which asked participants if they keep up to date on and

investigated Facebook's frequent privacy policy changes. The results were then analyzed to determine if a relationship truly did exist.

Procedure

The research study was executed in several steps. First, the researchers developed a 25 question survey and optional content analysis on the website SharePoint. Next, they created an event invitation on Facebook asking users to take part in the survey, with a description of the research study and a link to the SharePoint site. The invitation was distributed to the researchers' friends on Facebook. The researchers also sent an e-mail out to freshmen and sophomore students at King's College inviting them to participate. The survey was open to the public for two weeks, and the event invitation was taken down from Facebook when that time period had ended.

The survey results were analyzed as a whole for significant descriptive statistics. Next, the responses of the participants who chose to take part in the optional content analysis were pulled to be further examined. The researchers utilized respondents' personal Facebook identification numbers to view their profiles and evaluate their privacy settings from the perspective of someone who was not Facebook friends with them, but had at least one friend in common. These findings were compared to the participants' responses to survey questions 23, 24, and 25, asking the users what they believed their privacy settings were for their profile pictures album, their wall, and their hometown and/or current city information. This comparison determined whether or not users were truly aware of their current personal privacy settings. These findings were then evaluated against participants' responses to question 21, "When Facebook changes its privacy policies every so often and notifies you at the top of your homepage, do you take the time to investigate what has changed?" The categorical data was then analyzed descriptively, as well as inferentially by means of a chi-square statistic.

Limitations

The researchers must take several limitations into consideration when conducting this research study. First, the sample size for the research study was only a small fraction of the large number of individuals who use Facebook, so the findings are not generalizable to the entire population. Secondly, Facebook allows all ages to have profiles on the site, but our survey was distributed to those users over the age of 18; therefore, the researchers could not acquire responses from the youngest demographic that uses the service. Finally, the content analysis could only be performed on those individuals who opted to provide their personal Facebook identification numbers upon completion of the survey. Therefore, the content analysis had fewer responses than the overall survey.

Data Analysis

The data found in this research study was analyzed using both descriptive and inferential statistics. The information that the researchers uncovered in the content analysis was evaluated using a chi-square statistic on the computer software PHStat2. According to Tritschler (2000), "Chi square, which is used with nominal data, determines the significance of the pattern of the number of persons, objects, or responses that fall into two or more categories" (p. 160). The researchers chose this statistical test as it could investigate whether distributions of categorical variables differ from one another. In the case of this study, the privacy setting awareness of each respondent (Yes – they are aware, or No – they are not aware) was compared to their answer to survey question 21 regarding changing privacy policies. Possible responses to this question include "Yes," "No," and "I was unaware that Facebook changes its privacy policies." The

nominal data was then plugged into the chi square statistic to determine if a relationship truly does exist.

Validity and Reliability

According to Keyton (2011), “Researchers rely on construct validity to assure themselves that they are measuring the core concept that was intended to be measured. Construct validity rests on the arguments and supporting evidence, provided they are consistent with theoretical expectations” (p. 109). To obtain validity for the research study, the survey questions were crafted to gauge the respondents on the exact constructs the researchers were interested in. The majority of the questions focused on Facebook privacy policies and respondents’ opinions and perceptions of these policies. The researchers found the survey method to be the most reliable way of obtaining data for this specific topic.

Keyton (2011) also noted that reliability is the degree of stability, trustworthiness, and dependability that is present in a measurement. At the beginning of the survey, participants were asked not to access their Facebook profiles while responding to the questions. If they followed these instructions, the degree of trustworthiness and dependability in the study is greatly strengthened. Internal reliability, Keyton (2011) added, is “the degree to which the items invoke the same response from the person responding to the questionnaire” (p. 110). The researchers tested the internal reliability of the study by utilizing the content analysis, as each response was analyzed to determine the level of consistency in participants’ survey answers.

Ethical Considerations

Ethical issues were considered in the design and development of our research study. According to Keyton (2011), there are six areas of ethical concern to consider in the process. First, the study featured no intentional deception, as there was no need to mislead participants for this particular topic. There were also no confederates utilized in the study, and no possibility of physical or psychological harm to the respondents. The research study also did not use video or audio recording to acquire its responses. Two other areas of ethical concern, however – confidentiality and anonymity, and debriefing of participants – were relevant to our research study and must be discussed.

Because the survey required no name to participate, the anonymity of respondents was protected. For those respondents who chose to take part in the content analysis, the researchers kept all information discovered in the process strictly confidential, between the researchers and the respondents. As the study dealt with users’ awareness of their settings and could uncover inconsistencies, the researchers debriefed their findings with each participant upon completion of the study so that they could gain a true awareness of their settings. The debriefing was conducted through a Facebook inbox message which detailed the findings of the content analysis and alerted users of their privacy settings awareness.

Results

Upon examination of the survey responses and content analysis, the researchers were able to uncover an answer to the research question. The projected number of respondents for the survey was 250-300 individuals, and the final number of responses was 235. Of this number, 102 individuals opted to participate in the content analysis by providing their personal Facebook identification numbers. These responses were used to draw inferential statistics, while the total respondents (235) were utilized for descriptive statistics.

Of the 235 individuals who responded to the survey, 63% were female, and 37% were male. The target age for the survey was 18-30, and 89% of respondents fell into this range, as 42% were between the ages of 18-20, 38% were between the ages of 21-23, 7% were between

the ages of 24-26, and 2% were between the ages of 27-29. Of the other 11%, 2% fell between the ages of 30-35, 4% were between 36-40, and 5% were in the 45+ range.

After providing their age, respondents were asked if they have ever read Facebook’s privacy policy. Only 14% responded “Yes, I am aware of the latest version.” Seventeen percent responded “Yes, but only when I first created my account.” This would indicate that any participants in this segment who created their Facebook accounts prior to October 2010, the date of the policy’s last revision, are currently unaware of the latest version. Twenty-seven percent of respondents answered “I have only read parts of it,” while 29% said “No, I have never read it, but I know where to find it if needed.” The remaining 12% responded “No, I have never read it, and I don’t even know where to find it if needed.” Thus, the majority of respondents to the survey admit that they are either partially or totally unfamiliar with Facebook’s current privacy policy.

While this statistic would lead most to believe that users would admit their lack of awareness, the survey results reported just the opposite. When participants were asked how much they agreed with the statement “I am confident that I understand and am aware of my personal privacy settings on Facebook,” 21% responded that they strongly agreed, 52% responded that they agreed, and 19% said they are undecided. Only 7% reported that they disagreed, and the remaining 1% said they strongly disagreed.

Table 1
Respondents’ Awareness of Personal Privacy Settings vs. Knowledge of Changing Privacy Policies on Facebook – Observed

Observed Frequencies			
	Respondents are aware of their personal privacy settings		
Respondents are up to date on the changing privacy policies of Facebook	Yes	No	Total
Yes	13	11	24
No	11	67	78
Total	24	78	102

Note. Data analyzed using computer program PHStat2.

Table 2

Respondents' Awareness of Personal Privacy Settings vs. Knowledge of Changing Privacy Policies on Facebook – Expected

Expected Frequencies			
	Respondents are aware of their personal privacy settings		
Respondents are up to date on the changing privacy policies of Facebook	Yes	No	Total
Yes	5.6471	18.3529	24
No	18.3529	59.6471	78
Total	24	78	102

Note. Data analyzed using computer program PHStat2.

Next, users were asked if they believed Facebook protected their privacy in a suitable fashion. 70% of respondents answered yes, while the remaining 30% answered no. Therefore, it seems as though the majority of respondents to the survey believed that they were aware of their personal privacy settings on Facebook and that the site protected them in a suitable fashion, even though most admitted to being unfamiliar with the website's current privacy policy.

Respondents were next asked who they believed could view the personal content that they posted. 82% of participants answered that their postings were viewable to "only friends," meaning only those Facebook users who have been personally added or accepted by the user. If this were true, it would seem users' statuses, photos, and personal information would be relatively secure, as they would only be accessible to individuals that the user has confirmed knowing. However, when respondents were asked how well they know their Facebook friends, 58% reported that they had one or more friends that they had never physically met. These users may be exposing their personal information to complete strangers, and unknowingly putting themselves at risk. What good is it if your privacy is set to "only friends," if you don't actually know all of the friends you accept?

After reviewing the survey responses, the researchers conducted the content analysis to determine if each participant had a true awareness of their personal privacy settings. The researchers ran the findings of the content analysis through a chi-square test on the statistical computer software PHStat2. According to Keyton (2011), in a two-way chi-square such as the one utilized in this research study, "participants are classified on two variables in relationship to each other" (p. 207). As depicted in Table 1 and Table 2, the 102 participants in the content analysis were assigned to a category based on two variables: first, their answer to survey question 21, "When Facebook changes its privacy policies every so often and notifies you at the top of your homepage, do you take the time to investigate what has changed?," and second, the users' personal privacy setting awareness based on what the researchers discovered in the content analysis.

Using this information, the participants were assigned to one of the four possible categories. As illustrated in Table 1, of the 102 individuals who opted to participate in the content analysis, 13 reported that they did keep up to date on Facebook’s changing privacy policy, and they were also found to be aware of their current privacy settings. 11 respondents also reported staying up to date on Facebook’s changing privacy policy, but were found to be unaware of their personal privacy settings in the content analysis. Alternatively, 11 other respondents claimed that they did not keep up to date with Facebook’s privacy policy, but were found to be aware of their settings; while the 67 remaining respondents reported that they did not keep up to date with Facebook’s changing privacy policy, and were found to be unaware of their personal privacy settings in the content analysis.

As illustrated in Table 3, the researchers used a .05 level of significance for the chi-square test. According to Keyton (2011) the significance level is the “level of error the researcher is willing to accept” (p. 197). This indicates that the researchers had only a .05 level of error for this study. According to Keyton (2011), this means that in an analysis of 100 individuals, “5 out of the 100 findings that appear to be valid will, in fact, be due to chance” (p. 197). Setting this level of significance gave the researchers a greater degree of accuracy and validity in analyzing the outcome of the test.

Table 4 demonstrates the results of the chi-square statistical test. The test statistic was found to be 16.3723, while the critical value was 3.8415. Because the test statistic was greater than the critical value, the test indicated that the researchers should reject the null hypothesis, and accept the hypothesis they had proposed at the beginning of the research study. According to Keyton (2011), the null hypothesis is the opposite of what the researchers intended for the outcome of the study. In the case of this research study, the null hypothesis would have been that Facebook’s intricate and constantly changing privacy policies have no effect on users’ awareness of their personal privacy settings; and thus no relationship exists. However, the data clearly demonstrates that if users don’t take the time to educate themselves on Facebook’s

Table 3
Data Information

Data	
Level of Significance	0.05
Number of Rows	2
Number of Columns	2
Degrees of Freedom	1

Note. Data analyzed using computer program PHStat2.

Table 4
Results of the Chi-Square Statistical Test

Results	
Critical Value	3.8415
Chi-Square Test Statistic	16.3723
<i>p</i> -Value	0.0001
Reject the null hypothesis	

Note. Data analyzed using computer program PHStat2.

changing policies, they are often times unaware of their personal privacy settings, as well as the audience their postings can potentially reach.

As depicted in Figure 1, the results of the chi-square statistic provide an answer to the research question, “To what extent do the changing security features of personal privacy settings on social networking site Facebook allow personal postings to be viewed by a broader audience than intended by the end user?” 65.7% of participants in the content analysis admitted that they did not stay up to date on Facebook’s changing privacy policies, and they were also found to be unaware of their personal privacy settings. 12.7% of respondents said they did follow Facebook’s policy changes, and they were found to be aware of their settings. Thus, it can be inferred that a relationship exists between the efforts users make to keep up with Facebook’s changing privacy policies, and the levels of awareness they retain of their personal privacy settings.

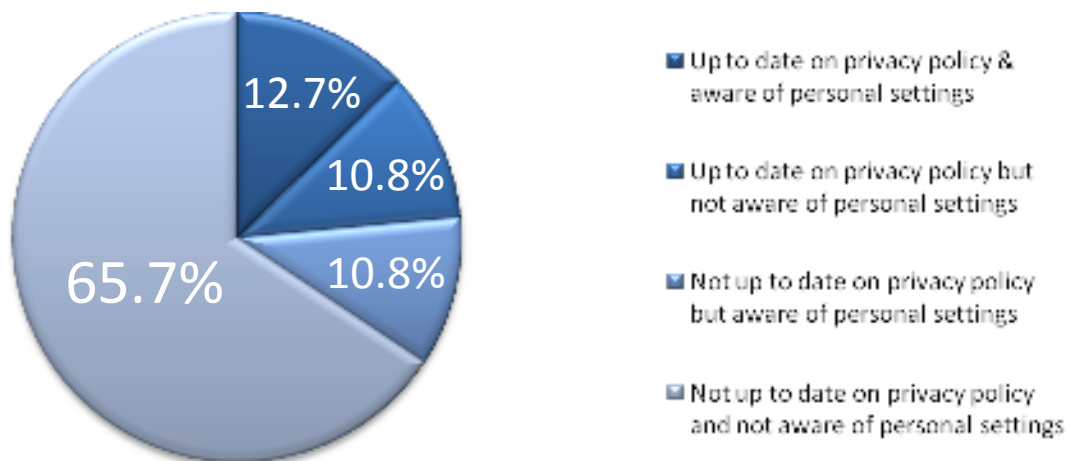


Figure 1. Pie chart illustrating results of content analysis when compared with participants’ responses to survey question 21. Chart created by Butler, E., McCann, E., and Thomas, J. using the Microsoft Office 2007 program Excel.

Discussion

The researchers embarked on this study to uncover the awareness issues that surround Facebook's current privacy policy. Due to the constant modifications and alterations to the policy, many users are unaware of how their profiles are affected. The study found that if users don't take the time to investigate and educate themselves on the changes, their perceived privacy settings are often times inconsistent with their actual settings. These findings lay the foundation for future research related to Facebook privacy settings.

The dynamic nature of the social networking site means that it is constantly evolving, thus levels of privacy are simultaneously shifting as well. Even throughout the short duration of this research study, Facebook added two new major features to its service: "Places I Check Into" and "See Friendship." The Places application allows users to virtually check-in to a real-life location, alerting all their Facebook friends of their current position on the map. This raises major safety concerns, as Facebook users could exploit this information to track down and find an individual. Future studies on the Places application could determine its level of privacy and safety and investigate users' opinions of its appropriateness on the Facebook site. The "See Friendship" feature, which replaced the "Wall-to-Wall" feature, allows Facebook users to see every interaction that has taken place between two mutual friends. Similar to the introduction of the News Feed in 2006, some users feel that this is a violation of privacy, allowing others to see all of their personal interactions. Future research could determine how people use this new feature, and whether or not they feel it compromises their privacy.

Another major issue that was not discussed in this research study is how Facebook utilizes individuals' personal information to target advertisements to them. According to Cowan (2010),

The company thrives on advertising revenue, on pooling users' information and using that data to target ads at very specific demographics. Knowing your age and gender helps somewhat. Knowing that you enjoyed the last Black Eyed Peas record, shop at the Gap, went to the University of Toronto and love to garden helps more. (para. 8)

Once users upload their personal information, Facebook uses this data to place them in a demographic and target specific ads to them. Is this ethical on Facebook's part? Do users even know this is taking place? Future research could delve into the issue of users' privacy related to these Facebook advertisements.

Another aspect of the Facebook experience that was not touched upon in this study is privacy in regard to third party applications. The countless games, quizzes, personality tests, and virtual worlds that clutter the news feed often require considerable amounts of personal information from the users in order to play. According to Cowan (2010), "these games do not necessarily adhere to Facebook's privacy rules. And even if users didn't partake in these third-party applications, their information could still be collected if friends were playing." (para. 14). Are users aware that these applications are utilizing their information? Or do they feel it is a fair tradeoff for use of the games?

Future studies may also explore the implications of the researchers' findings. How are users affected when they are unaware of their personal privacy settings on Facebook? What ages are most vulnerable to information violation? What steps can Facebook take to better ensure user awareness of their privacy policy? The possibilities for future investigation are endless, and will only increase as Facebook continues to make updates and modifications to its service.

Overall, the researchers believe that the findings of this research study offer a great degree of social significance. According to Keyton (2011), the social significance of a study is "how the results may actually be applied in real life" (p.198). In this case, the researchers

debriefed with the participants of the content analysis in order to inform them of the study's findings. Each user was alerted of their true privacy settings, and encouraged to keep up to date with Facebook's ever-evolving privacy policy. This debriefing benefited the participants by alerting them of the misconceptions they may have about their security on Facebook. It will ultimately grant them greater knowledge of the power of their presence on the social networking site, and allow them to peruse the Facebook service more safely and confidently.

References

- Allen, A. (2001). Is privacy now possible? A brief history of an obsession. *Social Research*, 68(1), 301-306. Retrieved from Academic Search Premier database.
- Cowan, J. (2010). Why we'll never escape Facebook. (Cover story). *Canadian Business*, 83(10), 28-32. Retrieved from Academic Search Premier database.
- Electronic Frontier Foundation (2009). *Facebook's new privacy changes: The good, the bad, and the ugly*. Retrieved from <http://www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly>
- Electronic Frontier Foundation (2010). *Facebook's eroding privacy policy: A timeline*. Retrieved from <http://www.eff.org/deeplinks/2010/04/facebook-timeline/>
- Facebook. (2010a). *Connecting on Facebook*. Retrieved from <http://www.facebook.com/home.php?#!/settings/?tab=privacy§ion=basic&h=fd53a94927b36bdf80bf2379d3da5762>
- Facebook. (2010b). *Facebook info*. Retrieved from <http://www.facebook.com/home.php?#!/facebook?v=info>
- Facebook. (2010c). *Press room*. Retrieved from <http://www.facebook.com/press/info.php?statistics>
- Goldsborough, R. (2010). Are you protecting your privacy online?. *Teacher Librarian*, 37(5), 72. Retrieved from Academic Search Premier database.
- Grimmelmann, J. (2010). Privacy as product safety. *Widener Law Journal*, 19(3), 93-827. Retrieved from Academic Search Premier database.
- Keyton, J. (2011). *Communication research: Asking questions, finding answers*. New York, NY: McGraw-Hill Companies, Inc.
- Kinkoph Gunter, S. (2010). *Teach yourself Facebook in 10 minutes*. Upper Saddle River, NJ: Pearson Education, Inc.
- Qualman, E. (2009). *Socialnomics: How social media transforms the way we live and do business*. Hoboken, NJ: John Wiley & Sons, Inc.
- Tavani, H. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, 38(1), 1-22. doi:10.1111/j.1467-9973.2006.00474.x.
- Tritschler, K. A., & Barrow, H. M. (2000). *Barrow & McGee's practical measurement and assessment*. Philadelphia, PA: Lippincott Williams & Wilkins.
- Veer, E. V. (2010). *Facebook: The missing manual*. Sebastopol, CA: O'Reilly Media, Inc.
- Warman, M. (2010). *Facebook most visited site on the web, says Google, in list of top 1,000 destinations*. Retrieved from <http://www.telegraph.co.uk/technology/google/7777549/Facebook-most-visited-site-on-the-web-says-Google-in-list-of-top-1000-destinations.html>
- Williams, C. (2007). *Facebook wins Manx battle for face-book.com*. Retrieved from: http://www.theregister.co.uk/2007/10/01/facebook_domain_dispute