

Negotiating Online Privacy Boundaries: Self-Revelation in the Facebook Generation

By Katherine Bies

A senior thesis submitted to
the Department of Communication Studies
of the University of Michigan
in partial fulfillment of the requirements
for the degree of Bachelor of Arts (Honors)
April 2012

Thesis Committee:

Professor Nicholas Valentino (Honors Program Advisor)
Professor W. Russell Neuman

©Katherine Jean Bies 2012

All Rights Reserved

ABSTRACT

Social media sites, while facilitating the collection and sharing of personal information online, have had negative consequences for personal privacy. Policy makers have yet to define which aspects of online communication on social media sites, if any, can be legally considered “private”, leaving many users with a false sense of security online. This study compares the offline behavior of 381 survey respondents to their behavior on social media sites in order to determine if offline privacy law can be applied to cyberspace. An analysis of these responses finds that: 1) social media users have negotiated a privacy boundary online; 2) online privacy protection is similar to the privacy protection used offline; 3) older generational cohorts are less likely than the Net Generation to closely guard their privacy online. Because generational cohorts do vary in their online behavior, it appears that privacy boundaries on social media sites have not been firmly settled. However, privacy standards online are beginning to take shape. This study has important implications for privacy law. By empirically determining whether or not social media users have a “reasonable expectation of privacy” on social media sites, this research may contribute to the development of a new legal standard that protects privacy both online and offline.

ACKNOWLEDGEMENTS

This thesis would not have been possible without the patient guidance of my two advisors, Professor Neuman and Professor Valentino. I am unimaginably thankful for your constant advice and encouragement throughout this whole process. Most importantly, thank you for pushing my brain to its limit every single week.

I am also indebted to my parents, friends, and co-thesis writers for their never-ending support. Thank you for being my second set of eyes and ears.

Lastly, I am grateful to the Communication Studies Department at the University of Michigan for funding my research and to all those who participated in my research.

TABLE OF CONTENTS

Abstract	ii
Acknowledgements	iii
List of Tables	vi
List of Figures	vii
Introduction	1
Literature Review	
An Overview of Facebook	4
Privacy Risks on Social Media: The Facebook Case	6
Facebook Privacy Policy and Controls	8
The Development of Privacy Law	10
Empirical Research Regarding Facebook Privacy	16
The Net Generation and Self-Revelation on the Internet.....	18
Facebook Privacy Protection	19
Variables that Predict Privacy Protection.....	20
The Net Generation	20
Gender	21
Privacy Controls Knowledge	21
Personality Variables	22
Role Heterogeneity	24
Network Size	25
A Comparison of Offline and Online Privacy Protection	26
Method	
Data Collection and Sample	28
Measures	30

Results

A Comparison of Offline and Online Self-Revelation	37
Correlates of Privacy Protection	43
A Comparison of Offline and Online Privacy Protection	50

Discussion

Do Facebook users exhibit an expectation of privacy?	57
Do Facebook users have a reasonable expectation of privacy?	60
Self-Revelation	61
Privacy Protection	64
The Role of Legislative Bodies	70
Summary of Limitations and Further Research	72

Conclusion	74
------------------	----

Appendixes

A: Demographics of Mechanical Turk Sample	80
B: Demographics of College Sample	81
C: Comparison between Mechanical Turk and College Sample	82
D: Index Measures	83
E: Complete Survey for College Sample	87
F: Complete Survey for Mechanical Turk Sample	95
G: An Independent Samples T-Test Comparing the Image Management of Net Geners and Baby Boomers	102
H: An Independent Samples T-Test Comparing the Friend Selectivity of Net Geners and Baby Boomers	103
I: An Independent Samples T-Test Comparing the Privacy Controls of Net Geners and Baby Boomers	104
J: An Independent Samples T-Test Comparing the Privacy Controls Knowledge of Net Geners and Baby Boomers	105
K: A Paired Samples T-Test Comparing Offline Privacy Protection and Facebook Privacy Controls	106
L: An Independent Samples T-Test Comparing the Offline Privacy Protection of Net Geners and Baby Boomers	107

LIST OF TABLES

Table 1: Cronbach's Alpha for Big-Five Personality Trait Indices ($\alpha =$)	36
Table 2: A Regression Analysis of the Correlates of Online and Offline Self-Revelation	39
Table 3: A Regression Analysis of the Correlates of Online and Offline Privacy Protection	46
Table 4: Correlation between Offline Privacy Protection and Facebook Privacy Protection	51
Table 5: A Regression Analysis of the Relationship between Online and Offline Privacy Protection	54
Table 6: A Summary Hypotheses and Findings	56

LIST OF FIGURES

Figure 1: Histogram of Offline Self-Revelation	38
Figure 2: Histogram of Online Self-Revelation	38
Figure 3: A Comparison of Offline and Online Self-Revelation Medians by Generational Cohort	40
Figure 4: The Relationship of Offline and Online Self-Revelation by Generational Cohort	41
Figure 5: A Comparison of Online Privacy Protection Means by Generational Cohort	44
Figure 6: A Comparison of Privacy Controls Knowledge Means by Generational Cohort	48
Figure 7: A Comparison of Offline and Online Privacy Protection Means	50
Figure 8: A Comparison of Offline Privacy Protection and Online Privacy Controls Means by Generational Cohort	53
Figure 9: The Relationship of Offline and Online Privacy Protection by Generational Cohort	55

“Can the everyday Facebook enthusiast be expected to protect privacy on an inherently social site?” -Ben Rothke, an IT manager for an information security company (Rothke, 2010).

The development of interpersonal communication technology has bridged the physical distance between individuals in modern society by facilitating the ability to gather and share information. However, these new technologies also come at a potential cost to personal privacy (Agre & Rotenberg, 1997; Moore, Jr., 1984; Caloyannides, 2003; Ware, 1986; Sylvester & Wolinsky, 1992). The contemporary legal concept of personal privacy, defined as the right to control the access and use of personal information, was established in the late 19th century by Warren and Brandeis (Warren & Brandeis, 1890). Concerned that “modern” media technologies such as instant photographs and tabloid newspapers were intruding into the private lives of American citizens, Warren and Brandeis argued that individuals have a “right to be let alone” (Warren & Brandeis, 1890, para. 1). However, is this right to personal privacy, defended by Warren and Brandeis, “truly a legally protected right or just a philosophical statement of wish?” (Caloyannides, 2003, p. 100).

The Fourth Amendment, which protects the right of citizens against privacy intrusions by the government, has served as the constitutional safeguard of personal privacy. The Supreme Court has defined and redefined the boundary between public and private, reconciling the capabilities of new technologies with a constitutional right developed before these technologies were even imaginable. In general, the Supreme Court has expanded the Fourth Amendment to protect against the greater risk of privacy invasion made possible by new technologies. However this has not always been the case. For the first half of the 20th century, privacy was limited to the

physical space of the home. The 1928 Supreme Court case *Olmstead v. United States*, 277 U.S. 438, allowed law enforcement to wire-tap phone conversations as long as they did not physically enter the suspect's house. The Supreme Court deviated from this trespass-based approach in a later case, *Katz v. United States*, 389 U.S. 347 (1967), which involved law enforcement recording conversations in a public telephone booth. Due to the development of technologies that allow a person to communicate privately while outside the home, the Supreme Court ruled in *Katz* that regardless of physical location, a person with a "reasonable expectation of privacy" is protected from unreasonable search and seizure under the Fourth Amendment, 389 U.S. 360 (1967). In this case, the creation of a "reasonable expectation of privacy," even when in a public space, involved shutting the door to a phone booth.

The Internet, because access is widely available and increasingly inexpensive, has facilitated the collection and sharing of personal information on an even greater scale (Calyionnides, 2003). Technological innovations in cyberspace, such as the development of social media including Facebook, Myspace, and Twitter, are communication platforms used by tens of millions of people to share personal information online. As Mark Zuckerberg, founder of Facebook explained at a 2010 interview at the TechCrunch awards, "In the last 5 or 6 years, blogging has taken off in a huge way and all these different services that have people sharing all this information. People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. That social norm is just something that's evolved over time" (Popkin, 2010, para. 9).

However, while users reveal more and more information on these social media sites, many still consider their personal content to be private. Even though these individuals find themselves in a new technological environment, they are relying on previously developed

expectations of privacy (Ware, 1986). Since a privacy standard has not yet been legally defined online, the role of negotiating the boundary between public and private space on social media has been thrust upon social media users themselves. While many users apply the privacy controls developed by these sites, others self-monitor their content by deleting or refraining from posting comments and photos that may be considered inappropriate in order to manage their image online. Do these behaviors represent an expectation of privacy on social media? Without confirmation from policy makers or the courts, the answer to this question is, at present, anyone's guess.

The Internet poses a significant challenge to legal doctrine regarding the definition of the private sphere and protections against privacy intrusions afforded to the American public under the Fourth Amendment of the United States (Semitsu, 2011). The *Katz* expectation-of-privacy test "rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations," writes Justice Alito in the recent Supreme Court decision *United States v. Jones*, 565 U. S. ____ (2012), (p. 10). This case concluded that police officers violated the Fourth Amendment when they attached a physical GPS device to the defendant's car, 565 U. S. ____ (2012). Justice Alito argues that dramatic changes in technology can significantly alter popular privacy expectations. During times of rapid technological development, some have argued that legislation is needed for initiating solutions to privacy concerns since legislative bodies are not constrained to court precedent or the text of the constitution and are more directly accountable to public preferences (Kerr, 2004; 565 U. S. ____ (2012)).

Since private communication on social media sites has yet to be defined, legal scholars have attempted to analogize interactions on social media sites to offline interactions in order to

apply offline privacy definitions and laws to these online sites (Hodge, 2006; Semitsu, 2011). However, social media interactions differ from face-to-face friendships in several ways. Social media users interact with a much larger group than most people interact with offline. For example, the average Facebook user has 130 friends (“Statistics”, 2011) and the average Twitter user has 126 followers (Arthur, 2009). Social media sites also allow users to do the impossible: gather these friends into the same “room” and share any aspect of their private life, sometimes several times per day. Semitsu (2011) argues that this difference between interactions offline and on social media does not automatically disqualify an expectation of privacy. Thus, the question becomes, do social media users act in a way that guarantees an expectation of privacy? This is best answered by comparing offline behaviors that have been decided by the Supreme Court in *Katz* to ensure an expectation of privacy with privacy protection on social media sites. And, more generally, asking the American public to reflect on how much privacy is expected on these sites.

Literature Review

An Overview of Facebook

Facebook was chosen as the focus of this study for a variety of reasons. First, Facebook is the world’s largest social media site with over 800 million users worldwide- 1 in every 13 people on earth use Facebook. (“Facebook”, 2011; “Facebook Statistics”, 2011). Also, while 48% of its users are 18 to 34 year olds, the 35 and older cohort, currently 30% of the user base is growing steadily, demonstrating that Facebook is not solely limited to a specific group of people. Lastly, Facebook has a diverse array of opportunities for sharing private information with both text and photos, and similar privacy controls to other social media sites like Myspace, Twitter, Facebook and LinkedIn. The ubiquity of Facebook use in today’s society may have substantial

implications for current social privacy norms upon which developments in online privacy law will be based.

Facebook, launched in February 2004, allows a registered user to create a personal profile and to add other users as friends. Originally the site was limited to Harvard students, but it quickly extended access to students at all Ivy League schools, then to students at all universities, and eventually to anyone over the age of 13. Facebook invites users to disclose private information which appears on their profile and can be shared with their Facebook friends. Users are asked to include their favorite books, movies, music, and television shows, interests, activities, employment history, educational history, email address, phone number, political views, and sexual orientation. Users share content by exchanging “wall posts” which are posted onto a friend’s profile, sending “Facebook messages” which, like an email, are sent to a friend’s Facebook inbox, creating “statuses” which are broadcasted to a users’ friends, uploading photos, and “tagging” others in photos which allows that photo to be posted to a friend’s wall. Facebook users can interact with others’ posts and uploads by “liking” them or commenting on them. Users then receive notifications when their content is liked or commented on. Users can also use their “News Feed” to track their friends’ posts and uploads.

Facebook has played an important role in developing and maintaining relationships with friends and may even affect social capital more generally. The site allows users to remain in contact with a large social network, including friends who have moved away, or to encourage relationships with recent acquaintances (Debatin et al., 2009; Ellison et al., 2007). This facilitation of friendship networks is correlated with the maintenance and creation of social capital (Ellison et al., 2007). Facebook users are also able to “participate in intimate yet distanced voyeuristic practices and to watch the gossip and rumor mill through the news feed and

friends' pictures" (Debatin et al., 2009, p. 19). In general, the benefits Facebook provides seem to override the potential loss of privacy, and this seems to hold even among those who have experienced privacy invasion (Debatin et al., 2009).

Privacy Risks on Social Media: The Facebook Case

While Facebook has obvious social benefits, Facebook users do not always have control over or even knowledge about the many individuals with access to their personal information. Facebook users therefore must "continually negotiate and manage the tension between perceived privacy risks and expected benefits" (Debatin et al., 2009, p. 87). Privacy breaches may bring unintended negative consequences. For example, college students have faced scrutiny from potential employers, school officials, and law enforcement based on the material they post on social media (Smith and Kidder, 2010; Stone, 2006; Kornblum and Marklein, 2006; Kornblum & Marklein, 2006; "The Fuzz", 2006; Welsh 2008). Facebook content which these groups find inappropriate, or even illegal, can result in serious consequences.

Employers have admitted using Facebook for recruiting and assessing applicants (Smith and Kidder, 2010; Zeidner, 2007). To gain access to a user's private information, employers can "friend" the job applicant, ask current employees who may know the applicant to gain access to the applicant's page, or ask the applicant in an interview to surrender his or her Facebook login password (Brandenberg, 2008; Duncan, 2012). A study by Reppler, an online image management company, which surveyed 300 different "hiring types", found that 91% are doing social media screens of job applicants and that 69% had rejected at least one candidate based on that process (Hill, 2011). Anecdotes include a New York-based nonprofit organization rejecting an applicant because of "extensive romantic exploits" cited on his Facebook page or a company withdrawing an internship offer after viewing a Facebook profile picture of an underage

candidate holding a bottle of vodka (Smith and Kidder, 2010; Stone, 2006). The Reppler study also asked these employers why they had rejected applicants. They found the following reasons for rejection: 11% for posting inappropriate photos, 11% for posting inappropriate comments, 9% for posting content about drinking, 10% for posting content about drug use, 11% for posting negative comments about a previous employer, and 10% for posting discriminatory comments (Hill, 2011). These examples illustrate the significant consequences that social networking can have on an individual's professional life.

Universities are also adapting Code of Conduct policies that cover social media use. Universities such as the University of Wisconsin Madison, the University of Minnesota, Penn State, the University of Colorado Boulder, and Ohio State University all maintain disciplinary policies for behavior on social media which is considered to be "dangerous and damaging to the reputation of the school" (Beckstrom, 2008-2009, p. 273). Students at several schools have been disciplined for making negative comments about professors or for posting inappropriate photos (Kornblum and Marklein, 2006). Even though most schools claim that they do not actively monitor students' conduct on social media, if a school becomes aware of behavior that violates its policies, the school administration often takes action (Lipka, 2008).

Police officers also may receive training about Facebook as a way to investigate and reduce crime (Kornblum & Marklein, 2006). On college campuses, police officers have used Facebook to investigate harassment complaints, to identify offenders who run off, or to shut down parties with underage drinking (Kornblum & Marklein, 2006; "The Fuzz", 2006; Welsh 2008). Facebook users other than college students have also encountered legal trouble because of their Facebook content. For instance, Anthony Wilson of Detroit was indicted on bank robbery charges after the FBI compared his Facebook photos with images taken from a bank surveillance

video (Snell, 2011). Police officers access Facebook profiles by viewing information set to public settings, creating fake profiles, voluntary disclosure from a third party such as an Internet service provider (ISP) or Facebook itself. In a very recent development, the FBI released an advertisement in January 2012, looking for companies with the capability to build a data-mining application for social media sites, including Facebook. A statement later released by the FBI said that the intent of the program is to view publically available, non-private, information and to focus not on specific people or groups, but on key terms relating to terrorism and illegal activities (Giles, 2012). Although this data-mining program is not yet operable, it is another important example of how online privacy concerns and law-enforcement are increasingly coming into contact.

Facebook Privacy Policy and Controls

In recent years, Facebook users have criticized Facebook's privacy policies for being "user-unfriendly" (Gabbert, 2011, para 4). For example, its previous policy, which became effective in December 2010, was much more lenient than current privacy policies about what user information it was allowed to share:

We may share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so. This may include responding to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. We may also share information when we have a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect ourselves and you from violations of our Statement of Rights and Responsibilities; and to prevent death or imminent bodily harm.

In other words, Facebook could voluntarily disclose user information if staff had "a good faith belief it was necessary to do so."




Facebook has since updated its policy to accommodate its users' expectations of privacy. Facebook's most recent revision on September 23, 2011 gives users greater control over their information in response to this criticism:

While you are allowing us to use the information we receive about you, you always own all of your information. Your trust is important to us, which is why we don't share information we receive about you with others unless we have:

- received your permission;
- given you notice, such as by telling you about it in this policy; or
- removed your name or any other personally identifying information from it.

Facebook has also taken a hard-line stance on protecting its users against privacy invasions. Facebook recently warned employers not to ask job applicants for their Facebook passwords, stating that this type of request violates both a user's privacy and Facebook's terms of service (Duncan, 2012). "We'll take action to protect the privacy and security of our users, whether by engaging policymakers or, where appropriate, by initiating legal action," wrote Facebook's chief privacy officer Erin Egan. "It is important that everyone on Facebook understands they have a right to keep their password to themselves, and we will do our best to protect that right" (Duncan, 2012, para 4).

Facebook also updated its privacy controls on August 23, 2011 in response to user suggestions. Facebook privacy controls allow users customize privacy for each item they share on their profile. Next to each item is a dropdown "audience selector" menu which gives the user the opportunity to choose from each of the following audiences:

-  **Public** (Visible to everyone- maximum audience)
-  **Friends** (Includes Facebook friends and friends of anyone tagged)
-  **Custom** (Includes specific groups of people you've specified to include or exclude)

New privacy features also give users the opportunity to "screen tagged photos before they appear in profiles and the option to tag non-friends in pictures" (Bosker 2011). Despite privacy

controls, the following information is always public: name, profile picture, gender, username, and networks.

The Development of Privacy Law

The contemporary concept of a right to privacy was first established in an 1890 *Harvard Law Review* article by Warren and Brandeis (Bratman, 2001-2002). The article was inspired by the authors' distaste of journalists' intrusion into the private lives of politicians and celebrities. Warren and Brandeis argued that new technologies such as "instantaneous photographs and newspaper enterprise [had] invaded the sacred precincts of private and domestic life" by allowing the public dissemination of information related to a person's private life (1890, para. 4). They argued that citizens had the "right to be let alone" which was protected under existing common law (Warren & Brandeis, 1890, para. 1). This right extended beyond a person's right to physical property to include his "thoughts, sentiments, and emotions" (para. 9). In other words, Warren and Brandeis believed that "'property'" [had] grown to comprise every form of possession- intangible, as well as tangible" (1890, para. 1). However, this definition of privacy was not immediately supported.

In constitutional law, a right to privacy has been based on the Fourth Amendment:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (U.S. Const. amend. IV).

The Fourth Amendment was originally interpreted to protect a citizen's right against government intrusion of physical property. Over time, the Supreme Court's interpretation of this amendment has evolved to incorporate Warren and Brandeis' broader definition.

In the Supreme Court case *Olmstead v. United States* (1928), Justice Taft, writing the majority opinion, held that the wiretapping of a person's phone lines from outside of the home

was not considered a government intrusion under the Fourth Amendment. Taft reasoned that “there was no entry of the houses or offices of the defendants” and that “evidence was secured by the use of the sense of hearing,” 277 U. S. 465, (1928). According to the Taft majority, the Fourth Amendment only protects against physical trespass of the home and the seizure of tangible property, rather than intangible personal property such as a telephone conversation. However, Brandeis, dissenting, argued that the court must “meet modern conditions,” 277 U. S. 465, (1928). He believed that the interpretation of the Fourth Amendment must be expanded to include the capabilities of new technologies which could not have been predicted by the Founders when writing the constitution.

Following Brandeis’ suggestions, the majority’s strict interpretation of the Fourth Amendment as a protection against trespass was broadened in *Katz v. United States* (1967). The question at issue here was whether the recording of a telephone conversation in a public telephone booth by law enforcement constituted a violation of the Fourth Amendment. Justice Stewart, writing for the majority, argued that the Fourth Amendment protects *people*, not places, so that an intrusion of privacy is not defined solely as a physical trespass of the home. Stewart argued that the Fourth Amendment also protects against intrusion in a public setting if the individual takes steps to create a private space. “One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,” writes Stewart, 389 U.S. 352, (1967). Because the plaintiff, Katz, “shut the door” to the telephone booth, he was able to create a reasonable expectation of privacy in a public space. Justice Harlan, writing a concurring opinion, further refined the concept of a “reasonable expectation of privacy” in a two-part rule: “First that a person have exhibited an actual (subjective) expectation of

privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable,’” 389 U.S. 361, (1967). Thus, a reasonable expectation of privacy exists if two criteria are met. An individual must exhibit an expectation of privacy such as shutting a telephone booth door and society must acknowledge this expectation of privacy as reasonable.

However, the *Katz* rule does not protect one aspect of privacy- information revealed to a third party. In *United States v. Miller*, the Supreme Court held that “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities,” 425 U.S. 435 (1976). This rule, known as the Third Party Doctrine, disqualifies an expectation of privacy for information that has been knowingly revealed to a third party (Kerr, 2009). The Third Party Doctrine implies that if information on a social media site is shared with a third-party, such as Facebook staff or an Internet service provider, users would forfeit privacy rights (Semitsu, 2011). Justice Sotomayor in a recent Supreme Court decision, *United States v. Jones*, 565 U. S. ____ (2012), directly questions this aspect of the *Katz* ruling in a concurring opinion: “it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties,” she writes (p. 5). Sotomayor argues that this qualification is inappropriate in the digital age in which people reveal large amounts of private information to third parties, 565 U. S. ____ (2012).

The Sixth Court of Appeals in *Warshak v. United States*, 532 F.3d 521 (2008) found that in some circumstances there is a reasonable expectation of privacy even *after* information has been turned over to a third-party. In this case, the government requested a secret subpoena to access Warshak’s personal emails without his knowledge. The court found that the government had violated Warshak’s right to privacy under the Fourth Amendment because Warshak had a reasonable expectation of privacy in his emails. Even though Warshak turned his content over to

a third-party Internet service provider (ISP), there is no notice from the ISP that it will access email content. Thus, the court ruled, there remains a societal expectation that the email content is private. While this court ruling protects privacy online and could be applied to protect privacy on Facebook in the future, the Sixth Court of Appeals has limited jurisdiction and the Supreme Court could overturn this ruling if desired. However, Justice Sotomayor's statements hint that the Supreme Court may agree that the Third Party Doctrine no longer applies on the Internet.

The Stored Communications Act (1986), 18 U.S.C. §§ 2701, included in the Electronic Communications Privacy Act, was a legislative initiative to limit the Third Party Doctrine and the ability of third-party ISPs to reveal "information in their possession about their customers and subscribers" to the government and non-government entities. "The SCA was passed to bolster the weak Fourth Amendment privacy protections that applied to the Internet," according to legal scholar Orin Kern (Kern, 2004, p. 1234).

The SCA protects information stored on two types of service providers referred to as "electronic communication service" providers (ECS) and "remote computing service" providers (RCS):

- (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof.
- (B) any storage of such communication by an electronic communications service for the purposes of backup protection of such communication.

ECS providers are "prohibited from knowingly divulging the contents of a communication while in 'electronic storage' by that service" (Sidoti et al., 2010, p. 2). RCS providers are "are prohibited from divulging the content of any electronic communication carried or maintained on its service solely for the purpose of providing storage or computer processing services, if the provider is not authorized to access the communication for other purposes." (Sidoti et al., 2010, p. 3).

When Congress passed the SCA in 1986, the Internet was a nascent technology. Electronic communication has since exploded and new online communication technologies, such as social media sites, have emerged. However, Congress has not yet modified the SCA to protect the private information on these sites. Although Congress has not amended its policies, a recent court ruling has expanded the SCA to protect some aspects of Facebook.

District court Judge Morrow determined that Facebook and Myspace messages were subject to the SCA, since webmail and private messaging are “inherently private” communications that are “not readily accessible to the general public,” *Crispin v. Christian Audigier Inc*, 717 F. Supp. 2d 991 (2010). Facebook and Myspace wall posts were also considered to be protected by the SCA as long as “their access was limited to a few,” *Crispin v. Christian Audigier Inc*, 717 F. Supp. 2d 991 (2010). In other words, wall posts that were hidden behind privacy settings and were not available to the general public were also subject to the SCA (Sidoti et al., 2010). This is the first example of a judge allowing social media privacy settings to determine a privacy boundary online. However, since the case was only brought before a United States District Court, Judge Morrow’s ruling has limited jurisdiction. Also, even with the protections afforded by the SCA under Judge Morrow’s ruling, the SCA states that a warrant to notify the user that his or her electronic communications are being confiscated is only required to obtain content that is less than 181 days old. The government does not need a warrant to obtain electronic communications that have been in storage for more than 180 days.

While the SCA is the most recent piece of legislation passed by policy makers relevant to Facebook privacy, the Federal Trade Commission is currently working with Facebook to develop a privacy policy reminiscent of the *Crispin* holding. The F.T.C., on November 29, 2011, closed a deal with Facebook which “requires Facebook to obtain its users’ “affirmative express consent”

before it can override their own privacy settings” (Sengupta, 2011, para. 9). The F.T.C. has also recently worked with Google and Twitter to establish better privacy practices. It appears that both policy makers and courts are beginning to react to the technological innovations online in order to make long overdue reforms to the creation and interpretation of legislation relating to online privacy and in particular, social media.

Legal scholars have recommended reforms that the courts and policy makers should implement regarding Facebook privacy (Beckstrom, 2008-2009; Hodge, 2006; Semitsu, 2011). Semitsu (2011) compares conversations on Facebook to the telephone booth conversation recognized by the Supreme Court in *Katz* to warrant an expectation of privacy. He finds one main difference between the *Katz* telephone conversation and an equivalent conversation that might happen on Facebook today. On Facebook, *Katz*'s wall post or status would be broadcast to all of his Facebook friends. However, Semitsu argues that the “court never suggested that additional message recipients instantly defeat the expectation of privacy” (Semitsu, 2011, p. 369). In fact, Justice Stewart, in *Katz*, writes that “what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected,” *Katz v. United States*, 389 U.S., 351 (1967).

Semitsu then applies the *Katz* ruling to Facebook in order to suggest how courts today should interpret privacy intrusions on social media. He argues that the courts should view Facebook as the “twenty-first century equivalent of a phone booth” (Semitsu, 2011, p. 369). An individual who sets his Facebook content to private makes the equivalent action of shutting the telephone booth door. Conversely, an individual who keeps his content public cannot have a reasonable expectation of privacy. He adds that Facebook content that is permanently public, such as a profile picture, is “equivalent to one’s physical appearance or clothes while standing in

a glass phone booth” (Semitsu, 2011, p. 370). Semitsu (2011) also argues that policy makers should eliminate conflicting interpretations of the SCA by limiting the voluntary disclosure doctrine of third parties and adapt the SCA to explicitly protect all content on Facebook, such as photo-sharing and event-creating.

However, these recommendations are based solely on normative argument. While normative argument is important in developing the legal theory behind court decisions, “empirical and descriptive claims as to the current cultural understandings of privacy are very important in conceptualizing privacy. A conception of privacy must be responsive to social reality since privacy is an aspect of social practices” (Solove, 2002, p. 1142). Similarly, the social reality of privacy is deemed important by Justice Harlan in his concurring opinion in the *Katz* case. An individual must have an expectation of privacy “that society is prepared to recognize as ‘reasonable,’” *Katz v. United States*, 389 U.S. 361, (1967). Empirically measuring society’s expectation of privacy would greatly strengthen a court’s interpretation or a policy maker’s decision in determining the privacy boundary on social media.

Empirical Research Regarding Facebook Privacy

Since a definitive legal decision hasn’t been made by policy makers or the courts, the privacy boundary on social media sites has so far been determined by user norms and experiences. This boundary is asserted each time a social media user “venture[s] too far into public space with private details” resulting in negative consequences for the user (Lewis et al., 2009, p. 96). As news of these negative consequences spreads to other social media users, norms begin to develop regarding the extent to which private information is appropriate to share online. This determination of online appropriateness is referred to as “netiquette” (Benson 2009).

Benson conducted open interviews with ten Canadian individuals between the ages of 22 and 25 to compare their netiquette on Facebook to their etiquette offline. She hypothesized that personal information that is considered “offline-inappropriate” may be considered appropriate online, since individuals may assume that their online behavior is judged more leniently (Benson, 2009). Benson (2009) identified several categories of inappropriate Facebook content, including: 1) nudity, 2) excessive drinking, 3) drug use, 4) name-calling, 5) inappropriate photos with significant others, 5) racial slurs, and 6) political comments. Contrary to Benson’s hypothesis, the respondents considered these behaviors to be inappropriate online as well as offline. Benson further stated that appropriate online behaviors consisted of being “polite and courteous” and “the posting of embarrassing pictures of others is to be avoided, especially if one does not want embarrassing pictures posted of oneself” (Benson, 2009, p. 63). Benson’s (2009) respondents endorsed that a traditional sense of etiquette should be maintained in the online environment. However, Benson found that, at times, personal information deemed within “netiquette range” on Facebook would be seen as inappropriate by an employer. Thus, while Benson (2009) found that sharing personal information that was considered inappropriate offline was similarly considered inappropriate on Facebook, she also found that standards of appropriateness on Facebook are slightly more lenient.

This thesis will re-examine the claim that a traditional sense of offline etiquette is maintained online. While Benson’s studied focused on describing the similarities between the amount of private information individuals share offline and on Facebook, I will expand the scope of her research by using a larger and more diverse sample and comparing the manners in which individuals limit access to information about their private life both offline and on Facebook. In this study, self-revelation is the act of revealing private information. Privacy protection refers to

actions that limit access to this private information. By comparing self-revelation and privacy protection on Facebook and offline, I hope to provide an empirical confirmation of Semitu's application of *Katz* to Facebook. Most importantly with this approach, I hope to add some empirical clarity to the over-arching legal debate and question: do Facebook users have a "reasonable expectation of privacy" on Facebook?

First, I will revisit Benson's (2009) claims about self-revelation on Facebook. Benson found that standards of appropriateness did not vary greatly from offline to online. In other words, self-revelation on Facebook was mostly consistent with self-revelation offline. However, this conclusion was based on a study of college students in 2008. Older Facebook users may act differently on Facebook than younger users, and standards may have changed over the last four years as the site has grown.

The Net Generation and Self-Revelation on the Internet

Generational cohort is an important determining factor in an individual's attitudes towards and experience with online technologies (Tapscott, 2009). Tapscott (2009) defines the Net Generation as individuals who are currently aged 29 and younger and have grown up with the Internet. "Net Geners" have spent their formative years in a technological environment completely different from their parents and grandparents (Tapscott, 2009). Older generations may have different attitudes towards online privacy because they didn't grow up in this same environment. Tapscott (2009) claims that "Generation Xers," individuals currently in their 30s, most closely resemble the Net Generation in their Internet behaviors and attitudes. Based on Tapscott's analysis, I will conduct a comparison of self-revelation across these three generational cohorts: 1) The Net Generation, 2) Generation Xers, and 3) Baby Boomers.

Since the Net Generation has grown up in an environment where sharing private information online is the norm, members of this generation are more likely to reveal more information online than older generations (Palfry & Gasser, 2008). Palfry and Gasser discuss why young people may reveal more: “The digital age has brought about a new incentive to reveal information about oneself while reducing checks on imprudent behavior” (2008, p. 54).

Based on Tapscott’s and Palfry & Gasser’s findings, I predict that:

H1: The Net Generation will engage in greater self-revelation on Facebook than older generations.

Benson (2009) found that college students’ self-revelation did not differ significantly from offline to online. However, based on the differences between the Net Generation and the older generations, I do not think that this finding will be replicated for older generations. Since older generations are less comfortable revealing information online (Palfry & Gasser, 2008), it is likely their self-revelation will change from offline to online. I expect to find the following results in my research:

H2: The Net Generation will engage in more comparable offline and Facebook self-revelation than older generations.

Facebook Privacy Protection

Next, expanding upon Benson’s approach, I will compare privacy protection on Facebook to privacy protection offline. However, before I can compare offline and online privacy protection, I must first understand what type of privacy protection is used on Facebook. Facebook enables users to control the image that is presented on their profile or to limit who has access to this image via *privacy controls*, *image management*, and *friend selectivity*. *Privacy controls* allow a Facebook user to create “walls” around their content in order to limit access.

Privacy controls can be set so that only a select group of individuals, determined by the user is allowed to view content. *Image management* is comprised of decisions about which Facebook content is viewable on Facebook. For example, Facebook users engage in *image management* when they delete inappropriate content. *Friend selectivity* is comprised of the decisions about which Facebook users are considered acceptable “friends.” Debatin et al. (2009) found that “although many [users] restrict their profiles, they do not seem to fully understand that their level of privacy protection is relative to the number of friends, their criteria for accepting friends, and the amount and quality of personal data provided in their profiles” (p. 102). In other words, *image management* and *friend selectivity* serve as an extra safeguard for privacy.

Thus, my first research question:

RQ1: How often do Facebook users engage in privacy protection, as exhibited by the use of privacy controls, image management, and friend selectivity?

Variables that Predict Privacy Protection

The extent to which these three types of privacy protection are used on Facebook could be influenced by a variety of factors. Previous psychological research has found online privacy concerns to be influenced by generational cohort, gender, and personality variables. I also predict that the knowledge of Facebook privacy settings, network size, and role heterogeneity may influence privacy protection efforts. Next, I will review the theoretical inspiration behind each independent variable in detail.

The Net Generation

Generational cohorts have been found to be an important influence on the determination of online behavioral norms; however, this discussion has mostly focused on self-revelation (Tapscott, 2009; Palfry & Gasser, 2008). Although it has not yet been studied extensively, the

Net Generation may also use different online privacy protection strategies, compared to their older counterparts. Since the Net Generation is more likely than older generations to feel that sharing information online is the norm (Palfry & Gasser, 2008), it follows that the Net Generation may also feel less compelled to protect personal information. Expanding on Tapscott's and Palfry & Gasser's findings, I predict that:

H3: The Net Generation employs less stringent privacy controls, image management and friendship selectivity on Facebook than older generations.

Gender

In previous studies, females were found to employ more stringent privacy settings than males on Facebook (Lewis et al., 2009). However, females also post more photos on Facebook than males (Benson, 2009). While females may use more stringent privacy settings than males, they may also be more likely to have photos considered “inappropriate” on their Facebook wall than males. Users must balance the use of privacy controls with self-revelation. This is a theme I will revisit throughout the thesis.

H4: Females employ more stringent privacy controls, image management and friend selectivity on Facebook than males.

Privacy Controls Knowledge

A Facebook user's familiarity with privacy controls may also influence the stringency of his or her privacy protection. Users may want to have more stringent privacy settings but may not know how to change them or may think that they have more stringent privacy settings than they actually do. Facebook updates its privacy policies and privacy controls once or twice a year. If users are not up to date with the most recent privacy controls, their content may not be protected as intended. Butler et al. (2011) compared Facebook users' perceived privacy settings

to what their actual settings were and found that only 12.7% of respondents said they were up to date on Facebook's policy changes and correctly stated their settings. Interestingly enough, only 8% of respondents reported that they weren't confident in their knowledge and understanding of their privacy settings on Facebook (Butler et al., 2011).

Based on Butler et al.'s findings:

H5: Users with greater privacy controls knowledge will employ more stringent privacy controls on Facebook.

Personality Variables

Junglas et al. (2008) studied the relationship between personality variables and a concern for online privacy. They defined a concern for privacy as "the anxious sense of interest that a person has because of various types of threats to the person's state of being free from intrusion" (p. 367). A concern for privacy was determined to be positively related to adaptive responses to threats, such as engaging in privacy protection (Junglas et al., 2008). The personality attributes studied were based on the Big Five framework: agreeableness, conscientiousness, emotional stability, extraversion, and openness to experience. Junglas et al. (2008) found only three of the five personality attributes to correlate significantly with a concern for privacy. Highly agreeable individuals, who strive for harmonious relationships and are more likely to trust their environment, had lower privacy concerns than non-agreeable individuals. Conscientious individuals, who are organized, meticulous, and deliberate, had a higher concern for privacy than non-conscientious individuals. Lastly, individuals open to experiencing new things also had a higher concern for privacy than non-open individuals.

Highly agreeable individuals on Facebook, since they are less suspicious of their environment, should be more likely to assume that their Facebook friends would approve of revealing private information.

H6: Highly agreeable individuals on Facebook will employ less stringent privacy controls, image management and friend selectivity than less agreeable individuals.

Highly conscientious individuals are logical, foresighted, organized, and disciplined, with a “tendency to adhere to standards and principles” (Junglas et al. 1991, p. 392). These individuals should be more concerned about what others may do with the personal information they have posted online (Junglas et al., 2008).

H7: Highly conscientious individuals on Facebook will employ more stringent privacy controls, image management and friend selectivity than less conscientious individuals.

Individuals open to new experiences will have had more variegated life experiences, both positive and negative (Junglas et al., 2008). Because of this, “open individuals have developed a broader and deeper sense of awareness” (Junglas et al., 2008, p. 393). Junglas et al. (2008) found that this broader awareness manifested itself in an increased concern for privacy online.

H8: Individuals open to experience will employ more stringent privacy controls, image management and friend selectivity than individuals less open to experience.

Although Junglas et al. (2008) did not find extraversion to correlate significantly with online privacy concerns, I predict that extraversion should influence privacy protection on Facebook. Extraverted individuals are more likely to take risks, to make efforts to provide information about themselves, and to obtain information about others (Junglas et al., 2008). Based on these tendencies, I predict that extraverted individuals will engage in less stringent privacy protection in order to share more information about themselves online.

H9: Extraverted individuals will employ less stringent privacy controls, image management and friend selectivity than individuals less open to experience.

Role Heterogeneity

According to Goffman's theatrical analogy, life is composed of a front stage and a backstage (1959). While on the front stage, the social actor makes a positive impression on his audience based on how well he conforms to the norms expected by that audience. For each audience, the social actor has the ability to choose his stage, props and costume. While back stage, the social actor is able to step out of character and present the "real" self. Role heterogeneity is the extent to which front stage and backstage audiences are present in your social network at the same. Greater role heterogeneity may mean greater conflict about which role, front stage or backstage, the social actor should utilize.

Benson (2009) uses Goffman's theory to analyze responses in her interviews. When considering Facebook in Goffman's terms, Benson hypothesized that users with more stringent settings would behave in a more "backstage" manner on Facebook than other users because they were able to limit the access of certain audiences such as prospective employers (2009). However, Benson found that users had stringent privacy controls regardless of their online behavior. The difference between front stage and backstage behavior on Facebook was found to have more to do with internal rather than external concerns for privacy. College students, concerned about other audiences such as family members, teachers and employers seeing various "backstage" behaviors on their Facebook, treated their profile as a permanently front stage environment, and expected other users to do the same (Benson, 2009). Students can also use custom privacy controls to exclude certain groups from content that they might consider

inappropriate and engage in image management to remove that content altogether from Facebook.

Based on Benson's findings, I predict role heterogeneity will play a factor in determining an individual's Facebook privacy protection. An individual with greater role heterogeneity will have more audiences to exclude from various aspects of his or her backstage self.

H10: Users with greater Facebook role heterogeneity will utilize more stringent privacy controls and engage in more extensive image management.

Cyberspace is also inherently different from the offline world in that a person is more likely to have front stage and backstage audiences present at the same time. For example, Facebook combines both backstage and front stage audiences (friends, parents, family members, teachers, and employers) on one social networking site. Offline, not only is it less likely that audiences with conflicting behavioral expectations will be present at the same, but also a person is able to physically keep track of which audiences are present and choose when to act in a front stage or backstage manner accordingly. Thus, I predict the effect of role heterogeneity to have a greater effect online than it does offline.

H11: Role heterogeneity will have a greater effect on the engagement in privacy protection on Facebook than offline.

Network Size

Network size could also influence a user's engagement in privacy protection both offline and online. Network size refers to the amount of friends a person has in their social network. Greater network sizes are inherently less private. Thus, I predict Facebook users with greater network sizes to engage in more stringent privacy protection.

H12: Users with a larger network size will employ more stringent Facebook privacy controls and engage in more extensive image management.

Network size is likely to have a greater effect on Facebook than offline because Facebook provides users an opportunity to correspond electronically with friends on a greater scale than physically possible in an offline setting. Therefore, I predict network size to have a greater influence on Facebook than it does offline.

H13: Network size will have a greater effect on the engagement in privacy protection on Facebook than offline.

A Comparison of Offline and Online Privacy Protection

This research centers on the question: do Facebook users have a reasonable expectation of privacy? The Supreme Court, in *Katz*, developed a two-step test to determine whether or not a reasonable expectation of privacy exists. First an individual must have exhibited an expectation of privacy and secondly, society must acknowledge this expectation of privacy as reasonable, *Katz v. United States*, 389 U.S. 361. Legal scholars have argued that the use of privacy controls affords users an expectation of privacy because it is the online legal equivalent to shutting the door to a public phone booth. (Semitsu, 2011). I will test this argument with empirical research. Do Facebook users take the same steps to protect their Facebook content as they do to protect private information offline? For example, does a Facebook user who refrains from talking about drinking in public also refrain from posting comments referencing drinking on Facebook? Thus, I answer this question by comparing offline and online privacy protection. If Facebook privacy protection is similar to offline privacy protection, then Facebook users also exhibit an expectation of privacy.

I predict that online privacy protection will be similar to offline privacy protection. Benson's findings (2009) regarding self-revelation suggest that, in general, online and offline behaviors do not differ as much as expected. Thus, it can be logically extended that an individual's privacy protection online and offline should also be relatively similar.

H14: Facebook users who engage in more stringent privacy protection offline will also engage in more stringent privacy controls, image management, and friend selectivity on Facebook.

Although it is predicted that Facebook users will exhibit an expectation of privacy, this expectation of privacy will not be recognized by the courts unless the second part of the *Katz* test is also confirmed. The second question to be asked is: will society recognize this expectation of privacy as reasonable? One way of predicting whether or not an individual will see something as reasonable is by the extent to which a person performs an action. Thus, people who are more likely to engage in Facebook privacy protection are also more likely to feel that these behaviors guarantee a reasonable expectation of privacy. However, people who engage in privacy protection on Facebook to a lesser extent may be less likely to feel that these behaviors guarantee a reasonable expectation of privacy. Therefore, to determine whether or not society feels that this expectation of privacy on Facebook is reasonable, I will identify which groups of Facebook users participate in less self-revelation and more privacy protection on Facebook.

Generational cohort has already been predicted to influence the extent to which a Facebook user engages in self-revelation and privacy protection on Facebook. Because of the differing amount of online experience that the Net Generation and older generations have had, I predict that these generational cohorts will have a different sense of what is a reasonable expectation of privacy on Facebook. Having grown up with the Internet and social media sites, the Net Generation has had the time to establish online behavioral norms and an expectation of

which behaviors on Facebook guarantee a sense of privacy (Palfry & Gasser, 2008; Benson, 2009) Older generations, growing up in a different technological environment, may be cautious to accept the norms that the Net Generation has already established on Facebook, especially if these behaviors are not entirely consistent with traditional privacy norms as predicted by Tapscott (2009) and Palfry & Gasser (2008). Instead, older generations may apply offline privacy norms as they navigate privacy boundaries in cyberspace.

Thus, I predict that:

H15: The Baby Boomers and Generation Xers will engage in more comparable offline and Facebook privacy protection than the Net Generation.

Method

Data Collection and Sample

The survey data is composed of two distinct samples. In both samples, all respondents signed an informed consent form prior to filling out the survey. Also, all respondents currently had a Facebook. Since the survey focuses on comparing behaviors on Facebook to offline behaviors, the survey was only directed towards and distributed to individuals who reported that they currently have a Facebook.

The first sample is composed of 381 respondents recruited using Amazon Mechanical Turk. The Amazon Mechanical Turk sample composed of three smaller age group samples, 18-25, 26-35, and 36 and older, loosely based on Tapscott's (2009) generational cohort definitions with 155 (41%) respondents in the 18-25 age group, 110 (29%) respondents in the 26-35 age group and 116 (30%) respondents in the 36 and older age group. The mean age of the sample was 32 years (Standard deviation = 11.55; Range = 18-77). By comparing 18-25 year old

Amazon Mechanical Turk users with other Mechanical Turk users of different age groups, I will better be able to distinguish the impact of age on privacy protection.

Of the Mechanical Turk respondents, 194 (51%) were male and 187 (49%) were female. Thirty percent of respondents had completed a four-year college degree, 17% were currently enrolled at a 4 year college, and 14% had completed high school but had not pursued higher education. Forty-nine percent of respondents were Caucasian, non-Hispanic, 25% were Asian, and 16% were Hispanic. Yearly household income self-reports ranged from less than \$10,000 to more than \$150,000 with 53% of respondents making less than \$40,000 per year and 16% making \$90,000 or more per year. All respondents currently had a Facebook. Thirty percent of the respondents had had a Facebook for more than 4 years and 64% of respondents had had a Facebook for 2 years or more. Forty-seven percent of respondents check their Facebook at least once per day, with 67% checking it at least once per week. Eight-five percent of respondents spend 30 minutes or on their Facebook at a time with 70% spending 15 minutes or less at a time on their Facebook (See Appendix A for demographic tables of this sample).

The second sample consisted of 60 college students at a large, public, Midwestern university who were recruited from an undergraduate participant pool and received course credit for participating. In the college sample, 40 (67%) were female and 20 (33%) were male. Fifty-two percent were freshmen and 23% were sophomores and 43% were 19 years old and 27% were 18. All respondents currently had a Facebook and 90% had had a Facebook for 4 or more years. 100% of respondents check their Facebook at least once a week and 90% check their Facebook daily. When checking their Facebook, 97% spend less than 30 minutes on Facebook at a time (See Appendix B for demographic tables of this sample).

The Amazon Mechanical Turk 18-25 age sample is an important and unique cohort because it includes the Net Generation and it also corresponds with the largest U.S. Facebook age demographic with over 50 million users (“Facebook Demographics”; Tapscott, 2009). The second sample of college students will be compared to this sample as a methodological and internal check. While respondents in these samples are similar in age, they may not be similar in other demographical variables. College students are traditionally more likely to be upper-class, educated, and more technologically savvy. Findings from the college sample will be compared with findings from the Amazon Mechanical Turk sample, predicted to be more diverse, as a way to compensate for unknown differences between the two samples and also to distinguish among possible groups of Facebook users in this cohort who may engage differently in self-revelation and privacy protection. Results were found to be very similar between these two groups (See Appendix C).

While survey responses can help to determine whether or not Facebook users act in a way that guarantees a reasonable expectation of privacy, these responses are not necessarily the best way to discover why Facebook users choose to act in these ways and whether or not Facebook users feel that they have an expectation of privacy on Facebook. Ten survey respondents of various ages and genders were asked to participate in an interview that would expand on their survey responses to address some of these ideas. All interview participants signed an informed consent form prior to participating in the interview and all participants who were part of the Communication Studies undergraduate participant pool received course credit.

Measures

The survey instrument consisted of 71 questions to measure the following central constructs developed in the hypotheses: (1) *Online self-revelation*, (2) *Offline self-revelation*, (3)

Online privacy protection, (4) *Offline privacy protection*, (5) *Online role heterogeneity*, (6) *Offline role heterogeneity*, (7) *Privacy controls knowledge* (8) *Offline network size*, and (9) *Online network size*. These measures were created and analyzed for the first time in this survey on both sample populations. Statistical analysis determining the reliability of these measures will be a helpful tool for the future creation of measures about self-revelation and privacy protection both online and offline in upcoming studies. Variables shown in previous studies to be related to privacy concerns and predicted to be related to privacy protection were also measured: (1) personality traits and (2) demographic variables such as gender and generational cohort. (See Appendix D for an overview of all indices used in this study, Appendix E for a complete list of survey questions used for the college sample, and Appendix F for a complete list of survey questions used for the Mechanical Turk sample.)

Online self-revelation measures the extent to which the respondent reveals private information on Facebook. The scale is based on behaviors deemed by interviewees in the Benson study as “Facebook inappropriate”. Interviewees named the following behaviors as inappropriate: nudity, excessive drinking, drug use, calling other people names, inappropriate photos with significant others, racial slurs, political comments, and swear words. A nine-item index was created to assess how often a Facebook user reveals inappropriate information on Facebook. Responses rated statements on a four-point scale with 1 as “never”, 2 as “sometimes”, 3 as “occasionally”, and 4 as “often.” Statements included: “I use swear words in a comment or status,” “I post or am tagged in photos wearing revealing clothing,” and “I reference excessive drinking in a comment or status.” Users who admitted to posting or being tagged in inappropriate photos also indicated the placement of these photos on Facebook. For instance, profile pictures are one of the only Facebook features that can be seen regardless of privacy setting. The

respondent was then asked “have you ever made one of these photos a profile picture?” If respondents indicated that they had posted or been tagged in photos concerning a specific behavior, the “yes” was given 1 point and a response of “no” was given 0. The *online self-revelation* index is composed of the score totals from both of these question types with a higher score signifying greater self-revelation. Thirteen items were aggregated for further analysis (Cronbach’s $\alpha = .84$ for the Mechanical Turk sample; Cronbach’s $\alpha = .75$ for the college sample).¹

Offline self-revelation was measured by analogizing interactions with Facebook friends to offline interactions with friends. Since Facebook users, in theory, share their content with their “friends,” a proper measurement of offline self-revelation should involve revealing private information to friends. To keep this measure consistent with the Facebook index, each Facebook item was converted into an offline item. For example, the following statement asked in the previous index “I use swear words in a comment or status” was changed to “I use swear words when I talk to my friends.” *Offline self-revelation* was measured with a seven-item index. Respondents assessed each statement with a four point scale from 1 as “never” to 4 as “often.” Other statements included: “I wear revealing clothing when I go out to a party or bar with my friends,” and “I talk about excessive drinking with my friends.” Raw scores were summed, with higher values indicating greater self-revelation (Cronbach’s $\alpha = .82$ for Mechanical Turk sample; Cronbach’s $\alpha = .74$ for college sample).

To measure *offline privacy protection*, respondents were asked about behaviors that limit to whom they reveal information about their private life or, in other words, behaviors that create privacy. The items were built in two parts. The first part, the private information that was being

¹ In college sample, one item (“Have you ever made a profile picture out of a photo of you using drugs”) was removed from the Facebook self-revelatory index because it had zero variance.

revealed, was based on the self-revelation indices. The second part, the limiting of who this information is being revealed too, was based on the *Katz* ruling that the act of shutting a telephone booth door constitutes the creation of a reasonable expectation of privacy. Behaviors that also limit the availability of private information to the public such as “refrain[ing] from talking about excessive drinking in public” were used in the measure. The index also included several statements which were reverse coded such as: “I talk on the phone about excessive drinking when I am in front of my parents,” and “I wear revealing clothing to work.” Respondents rated statements on a four-point scale from 1 as “never” to 4 as “often.” The eight-item index was moderately reliable in both the Mechanical Turk (Cronbach’s $\alpha = .71$) and college sample (Cronbach’s $\alpha = .69$).

Online privacy protection tapped behaviors that limit not only the audience who is able to see a user’s content online and but also what type of content is available online. *Online privacy protection* is composed of three separate indices: 1) *privacy controls*, 2) *image management*, and 3) *friend selectivity*. *Privacy controls* include Facebook created privacy settings that limit who is able to see a user’s content. *Image management* is composed of self-monitoring behaviors such as when users delete or refrain from posting content that they consider to be inappropriate. *Friend selectivity* involves the decisions about which Facebook users are considered to be acceptable friends.

The *privacy control* index is made up of three questions about privacy settings. Each question has three responses that are taken from the language that Facebook actually uses “public”, “friends only”, and “custom”. Responses are scored from 1 as “public” to 3 as “custom” with higher values representing more stringent privacy controls ($\alpha = .87$ for Mechanical Turk sample; $\alpha = .75$ for college sample). Respondent’s who used custom settings were then

asked about which groups they allow to see their content to get a better idea of which groups (close friends, parents, siblings, past or current employers, people under 18, past or current teachers) among their Facebook friends that they include or exclude. The *image management* index is composed of three questions which ask about self-monitoring and editing behaviors with answer choices rated from 1 as “never” to 4 as “often”. Two of these items were aggregated and summed with higher values signifying greater image management ($\alpha = .61$ for Mechanical Turk sample and college sample).² The *friend selectivity* index is measured by two questions which ask about a respondent’s tendency to accept friend requests. The first asks “who would you accept as a friend?” with responses from “only close friends” to “anybody.” The second asks “how well do you need to know someone before accepting a friend request on Facebook?” with answer choices ranging from 1 as “not well at all” to 5 as “extremely well.” The two items were aggregated with a higher score indicating greater selectivity when accepting friends (Cronbach’s $\alpha = .60$ for Mechanical Turk sample and Cronbach’s $\alpha = .43$ for college sample).

Offline and Facebook *network size* were measured by self-report. To measure *offline network size*, respondents were asked “about how many friends do you hang out with on a regular basis?” *Online network size* was measured with two questions: “about how many Facebook friends do you have?” and “how many Facebook friends would you consider to be close friends?”

Online role heterogeneity, measured with four items, assessed the diversity of Facebook networks. It is a count of the friends a user has from various groups not traditionally considered to be part of a peer group such as: “family members”, “past or current employers”, “people under 18”, and “past or current teachers or GSIs”. Respondents estimated the number of Facebook

² In both samples, one item (“refrain from posting a status or comment that you felt would be inappropriate”) was removed from the image management behavior index because it negatively correlated with the other two items.

friends they have in each group. These estimates were then divided by the total Facebook network size to create four different online role heterogeneity ratio variables which describe the extent to which their Facebook friends are family, employer, under 18, or teacher heterogeneous.

Offline role heterogeneity, analogous to role heterogeneity on Facebook, is defined as the extent to which a respondent finds himself or herself in a situation when both peers and non-peers are in attendance. For example, respondents were asked how often they invite friends over to their house while their parents are home or sign up for a class with a friend. These situations combine friends with parents and friends with teachers, respectively. *Offline role heterogeneity* was measured with four items, each describing a heterogeneous situation with the same four groups used in the online role heterogeneity variable: family, employer, under 18, and teacher. Responses rated from 4 as “often” to 1 as “never.”

The *privacy controls knowledge* index is comprised of five questions which ask respondents about their knowledge of and comfort with Facebook’s privacy controls. This index was based on a similar study by Butler et al. (2011). The first four questions, measured on a five-point Likert scale, with 5 as “strongly agree” and 1 as “strongly disagree.” Statements include “I feel comfortable using Facebook’s privacy settings” and “I was aware that Facebook updated its privacy controls in September of 2011.” Respondents were also asked the last time they adjusted their privacy controls, with available responses from 6 as “In the last month,” to 1 as “In the last three or more years.” Four of the five items were aggregated with higher scores meaning greater

knowledge of privacy controls (Cronbach's $\alpha = .68$ for Mechanical Turk; Cronbach's $\alpha = .70$ for college sample).³

Personality traits were measured by indexes developed in past research. The Big Five personality traits were assessed using a ten-item scale developed and validated by Gosling et al. (2003). Responses for each item were scored with a seven-point Likert scale, ranging from 1 as “strongly disagree” to 7 as “strongly agree.” This ten-item scale, more efficient time-wise than other personality measurements, has also been shown to be valid by both Gosling et al. and other researchers (Muck et al. 2007). See Table 1 for a comparison of Cronbach's Alphas calculated for each of the five personality indices. In the Mechanical Turk sample, two of the indices, agreeableness and openness, returned low reliability. In the college sample, conscientiousness returned low reliability. Demographic variables: gender, age, race, income, and current education level were also measured.

Table 1: Cronbach's Alpha for Big-Five Personality Trait Indices ($\alpha =$)

Personality Trait	Mechanical Turk Sample	College Sample
Agreeableness	.38	.64
Conscientiousness	.60	.28
Emotional Stability	.66	.69
Extraversion	.73	.78
Openness	.33	.65

³ In both samples, one item (“I was aware that Facebook update its privacy controls in September of 2011”) was deleted from the knowledge of privacy controls index because it wasn't as strongly correlated with the other items. After further reflection, the item is less about the knowledge of Facebook privacy controls and more about the knowledge of Facebook practices. For example, Facebook users could have realized Facebook's adjustment of privacy controls and adapted to this change in October but might not have known that this change actually occurred in September.

Results

A Comparison of Offline and Online Self-Revelation

Survey responses were analyzed to test each of the 15 hypotheses. Data analysis commenced with the extension of Benson's (2009) previous research on comparing self-revelation on Facebook and offline. Employing a larger and more diverse sample, I found that offline and online self-revelation indices are highly correlated ($r=.51$, $p<.01$). Individuals who are more self-revelatory online are also more self-revelatory offline. However, Facebook users were found to reveal more personal information offline (Median = .54) than online (Median = .34).⁴ This suggests that people are more concerned about revealing inappropriate information online than off.

Another difference between offline and online self-revelation was seen in the distribution of survey respondents. While offline self-revelation was normally distributed, online self-revelation was unexpectedly skewed to the left, which means that the graph has a long tail to the right (See Figures 1 and 2). This finding is unexpected because these two indices were created to be conceptually identical by analogizing self-revelation online and offline. As discussed above, the same self-revelatory behaviors were tapped for both indices. The only difference was whether the information was being revealed to friends in an offline setting or on Facebook. Because these indices were created to measure the same conceptual range of behavior, the difference in these distributions suggest that online and offline self-revelation are distinct phenomena. Again, it appears that Facebook users are more concerned about revealing personal information online than offline. This concern could stem from a fear that their Facebook content

⁴ Because the Facebook self-revelation distribution was so skewed, medians and not means were used for this comparison. As a result, a Paired Samples T-Test could not be used to determine whether or not this large distance between online and offline self-revelation is significant.

will not remain private. Sharing personal information online is not perceived as secure as sharing information face to face.

Figure 1:

Histogram of Offline Self-Revelation

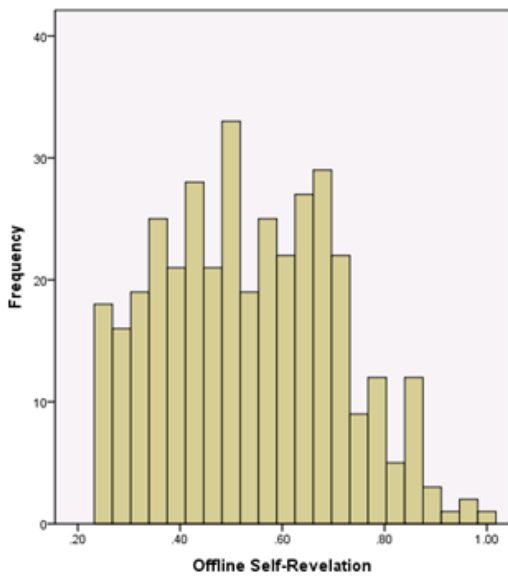
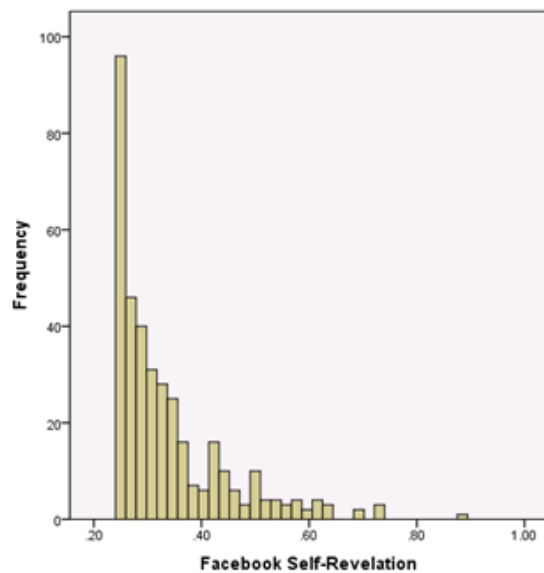


Figure 2:

Histogram of Online Self-Revelation



The online self-revelation distribution has outliers with very high self-revelatory scores that are pulling the distribution to the right. To find out which individuals were a part of this group, a regression was performed for both online and offline self-revelation to study the association of these indices with several variables discussed above to be predictors of online privacy protection: demographics, personality variables, generational cohorts, role heterogeneity, and network size.

The linear regression isolated the association of each one of the 18 independent variables with the online and offline self-revelation indices while controlling for the other 17 variables.

The two regressions were then compared to see whether similar factors predict self-revelation online and offline (See Table 2).

Table 2: A Regression Analysis of the Correlates of Online and Offline Self-Revelation

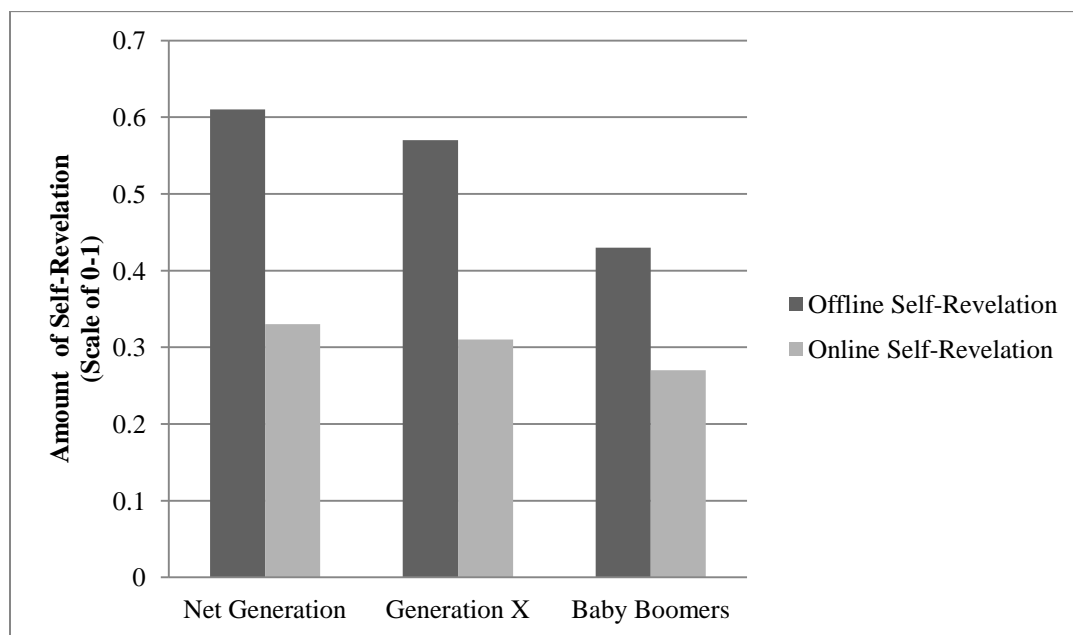
Predicting Variables	Facebook Self-revelation (B)	Offline Self-Revelation (B)
White	0.01	0.12**
Asian	-0.02	0.02
Black	-0.02	0.07
Female	-0.01	0.00
Income	-0.05**	-0.01
Current Education	-0.06 [^]	-0.03
Agreeableness	-0.08*	-0.22**
Conscientiousness	-0.08*	-0.12*
Emotional Stability	-0.02	-0.01
Extraversion	0.08**	-0.00
Openness	0.05	0.10 [^]
Generation Xers	0.01	-0.02
Baby Boomers	-0.04*	-0.11**
Role Heterogeneity Family	-0.02	-0.01
Role Heterogeneity Employers	-0.03	-0.02
Role Heterogeneity Under 18	-0.01	0.00
Role Heterogeneity Teacher	0.08	0.10**
Network Size	0.19**	0.05
N	361	357
R ²	.244	.245

*significant at $p < .05$, ** significant at $p < .01$, [^]significant at $p < .10$

H1 and H2 both predicted that generational cohorts would exhibit distinct patterns of online self-revelation. In H1, the Net Generation was expected to have greater self-revelation on Facebook. As seen in the comparison of self-revelation medians by generational cohort (See Figure 3), the Net Geners had the greatest self-revelation both on Facebook and offline. I was unable to perform a Paired Samples T-Test to determine if this modest difference between Net

Geners and Baby Boomers online self-revelation is significant since the online self-revelation distribution was skewed. However, the regression analysis confirmed H1. Baby Boomers were slightly, but significantly lower in Facebook self-revelation than the Net Generation. Therefore, as predicted, Baby Boomers share significantly less personal information online than younger generations.

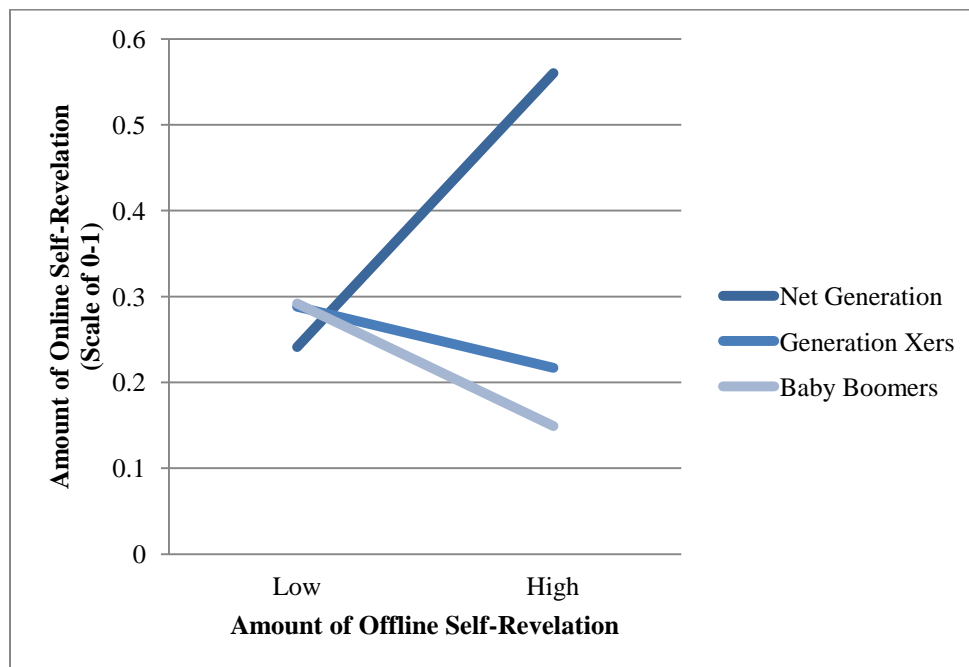
Figure 3: A Comparison of Offline and Online Self-Revelation Medians by Generational Cohort



H2 predicted that the Net Generation would have more comparable offline and online self-revelation than older generations. An interaction was calculated to determine the distinct relationship between online and offline self-revelation by generational cohort (See Figure 4). H2 was also confirmed. Net Geners exhibited a strong, positive, and significant correlation between offline and online privacy protection. Net Geners who are more self-revelatory offline are also more self-revelatory online. Baby Boomers exhibited a much smaller, and even slightly negative,

association between self-revelation offline and online. This means that Baby Boomers who share more information offline actually share *less* information online. The association for Generation Xers was, as predicted, in the middle of these two groups. Generation Xers are more similar than Baby Boomers to the online behavior of Net Geners.

Figure 4: The Relationship of Offline and Online Self-Revelation by Generational Cohort



Several demographic variables were differentially related to self-revelation online and offline. White respondents were higher in offline self-revelation than other groups, but racial groups were not distinct in terms of online self-revelation. Income and current education level were also negatively associated with online self-revelation, but unrelated to offline self-revelation. This means that individuals with low income levels and low current education levels are more likely to reveal personal information online.

Although specific predictions were not made regarding the influence of personality variables, personality was also found to influence self-revelation both online and offline. Agreeableness and conscientiousness were found to significantly predict self-revelation both online and offline. Agreeableness had a large, negative, and significant association with offline self-revelation and a small, negative, and significant association with Facebook self-revelation. Conscientiousness had a negative and significant correlation with both online and offline, but to a greater extent offline. In addition, extraversion had a small but positive and significant correlation with online but not offline self-revelation and openness had a moderate, positive correlation at marginal significance with offline self-revelation. In general, individuals, who are less agreeable, less conscientious, and more extraverted, exhibited greater self-revelation online.

Lastly, network size was differentially related to online and offline self-revelation. Facebook network size had a large, positive, significant correlation with Facebook self-revelation, but not with offline self-revelation. Individuals who have a larger network size on Facebook share more personal information than individuals with a smaller network size. It is possible that network size did not have a significant influence offline because offline networks are usually much smaller than those online.

While online and offline self-revelation were found to be similar, the same predicting variables, in general, did not significantly correlate with both online and offline self-revelation. The only predicting variables that these indices had in common were agreeableness, conscientiousness and generational cohort. Net Geners and individuals who are less agreeable and conscientious were found to have greater self-revelation both online and offline. However, individuals who engage in less self-revelation on Facebook than offline have higher incomes and current education levels, smaller network sizes, and are less extraverted. This suggests that while

online and offline self-revelation may be similar, not all users engage in online and offline self-revelation that is similar. While lower income and education level, larger network size and extraversion were not initially hypothesized to predict greater self-revelation, these findings help to create an image of the group of individuals who skew the distribution of Facebook self-revelation.

Correlates of Privacy Protection

The first research question explored which types of Facebook privacy protection are implemented by Facebook users. The use of privacy controls, image management and friend selectivity were all studied. Using a comparison of means, it was found that while all types of privacy protection are implemented, privacy controls are the most commonly used privacy protection (Privacy Controls Mean= .68, Image Management Mean= .53, Friend Selectivity Mean= .56).⁵

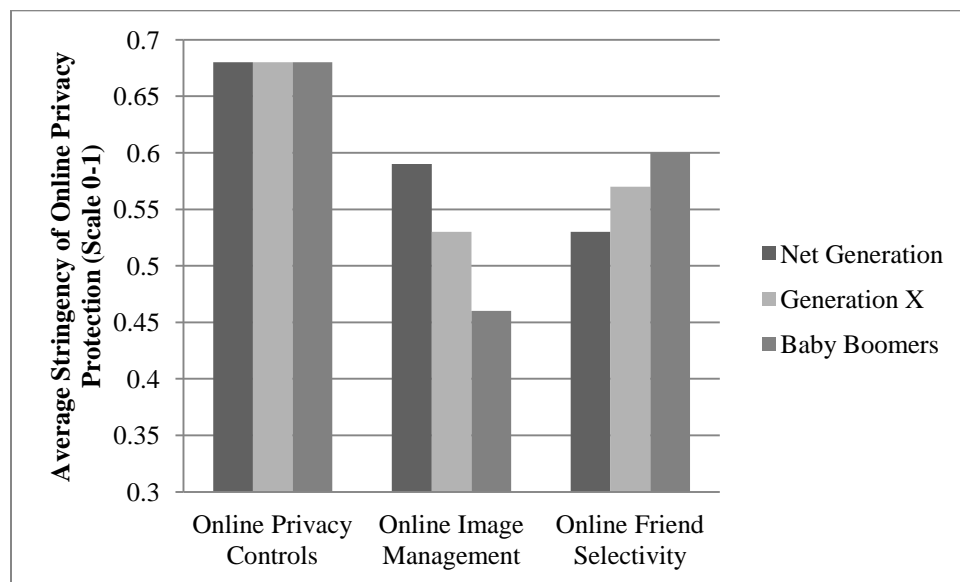
Next, I regressed these three online privacy protections, the demographic variables, personality variables, generational cohort, role heterogeneity, and network size measured in the previous model. A linear regression was performed on each of the three privacy protection indices: privacy controls, image management, and friend selectivity. A linear regression was also performed on the offline privacy protection index and compared with the three previous regressions in order see whether or not the same correlates affect offline and online privacy protection (See Table 3). The demographic, personality, and generational cohort variables were used in both the offline and online regressions. However, for role heterogeneity and network size, different but analogous variables (described in the Methods section) created to measure role heterogeneity and network size online and offline were used. Therefore in the online regressions, Facebook role heterogeneity and network size variables were used and in the offline regression,

⁵ These means were calculated on a scale of 0-1.

offline role heterogeneity and network size variables replaced the Facebook variables. The results from these regressions encompass the results for hypotheses 3 through 13.

H3 predicted that the Net Generation would engage in less stringent privacy protection than older generations. First, means were compared to determine whether Net Geners, on average, engage in less stringent privacy protection. Net Geners were found, on average, to have less stringent friend selectivity, but more stringent image management than older generations, and privacy controls consistent with older generations (See Figure 5).

Figure 5: A Comparison of Online Privacy Protection Means by Generational Cohort



An Independent Samples T-Test was used to determine that the difference between Net Geners and Baby Boomers was significant for both image management at friend selectivity at $p=.00$ (See Appendix G and Appendix H). The use of Facebook privacy controls did not differ significantly between generations (See Appendix I). Thus, it appears that all generations, on average, use a similar Facebook privacy setting- the restriction of content to only Facebook friends.

To determine if this finding was consistent for the generational distribution as a whole, the B values in the regression table were compared (See Table 3). Baby Boomers had a small, negative, and marginally significant association with privacy controls and a small, negative and significant association with image management. There was no significant generational difference for friend selectivity. Generation Xers also had negative associations with privacy controls and image management; however, these associations were not significant. This means that Net Geners, the excluded group in these models, actually exhibited the highest use of privacy controls and image management of any generation as a whole. Image Management was found by both the comparison of means and the regression to be more stringently used by the Net Generation than older generation. This finding also implies that Net Geners are more likely than older generations to use the “Custom” Facebook privacy control which goes a step further in privatizing content than the “Friends” control described above. The “Custom” setting not only limits content from the public view, but also from the view specific Facebook friends.

Females were predicted to engage in more stringent privacy protection than males (H4). As predicted, females had a small, positive, but marginally significant correlation with the use of privacy controls. Consistent with H4, females use more privacy controls than men. However, image management and friend selectivity did not vary significantly between men and women. While females have been shown in the past to have more stringent privacy settings (Lewis et al.,2009), gender does not appear to influence the use of image management and friend selectivity. The engagement in offline privacy protection also did not vary significantly between men and women. Current education level was another demographic variable with a moderate, positive, and marginally significantly correlation with the use of privacy controls. Thus, those

Table 3: A Regression Analysis of the Correlates of Online and Offline Privacy Protection

Predicting Variables	Facebook Privacy Protection			Offline
	Privacy controls (B)	Image Management (B)	Friend selectivity (B)	Privacy Protection (B)
White	0.04	0.02	0.02	-0.01
Asian	0.01	0.01	0.02	0.01
Black	-0.02	-0.12	-0.01	0.02
Female	0.04 [^]	-0.01	0.00	0.02
Income	0.04	-0.04	-0.01	0.02
Current Education Level	0.10 [^]	0.06	0.07	0.03
Agreeableness	0.04	-0.10	0.07	0.13**
Conscientiousness	0.14*	0.02	-0.01	0.13**
Emotional Stability	-0.11	0.01	0.05	0.03
Extraversion	-0.04	0.04	0.05	-0.05
Openness	0.09	-0.03	-0.04	-0.04
Generation Xers	-0.02	-0.03	0.01	0.00
Baby Boomers	-0.05 [^]	-0.06*	0.01	0.06**
Privacy Controls Knowledge	0.21**	0.17**	0.05	----- ⁶
Role Heterogeneity Family	0.03	0.08	.31**	0.02
Role Heterogeneity Employers	-0.13	0.07	0.08	-0.03
Role Heterogeneity Under 18	-0.02	0.15	0.00	-0.05
Role Heterogeneity Teachers	-0.09	0.38	-0.02	0.00
Network Size	-0.13	0.47**	-0.22**	-0.16*
N	348	371	368	357
R ²	.109	.144	.216	.224

*significant at $p < .05$, **significant at $p < .01$, [^]significant at $p < .10$

⁶ There was no analogous offline measure for knowledge of privacy settings, so this concept was not included in the offline privacy protection regression.

who had a higher education level used more stringent privacy controls. The other demographic variables were not found to be predictors of online or offline privacy protection.

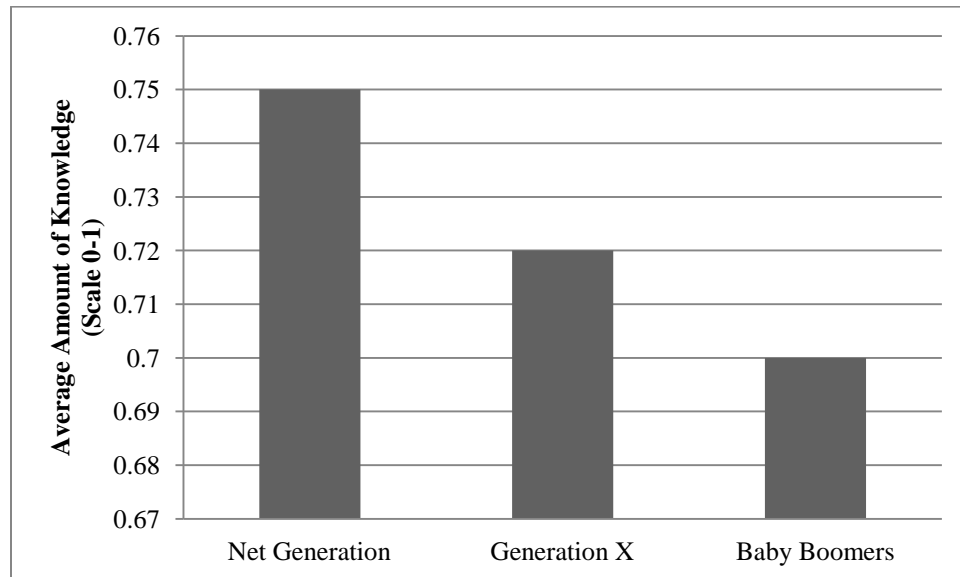
In H5, privacy controls knowledge was predicted to be positively correlated with the use of privacy controls on Facebook. The Net Generation was found to be most knowledgeable about privacy controls (See Figure 6).⁷ This difference between the privacy controls knowledge of Net Geners and Baby Boomers was found to be statistically significant at $p < .05$ after performing an Independent Samples T-Test (See Appendix J). Consistent with H5, the knowledge of Facebook privacy protection was positively and significantly correlated with the use of privacy controls. Since there is no analogous offline measure for privacy controls knowledge, there will be no online and offline comparison.

Personality variables were also expected to predict engagement in privacy protection on Facebook. Highly conscientious individuals (H7) and individuals more open to experience (H8) were expected to engage in more stringent privacy protection. Highly agreeable (H6) and extraverted (H9) individuals were expected to engage in less stringent privacy protection. As predicted in H7, conscientiousness had a moderate, positive, and significant association with Facebook privacy controls and offline privacy protection. Agreeableness also had a moderate, positive and significant correlation only with offline privacy protection. Contrary to hypotheses H6, H8 and H9, agreeableness, openness, and extraversion were not found to be predictors of online privacy protection.

According to H10, greater role heterogeneity was expected to predict greater engagement in Facebook privacy controls and image management. This relationship was also predicted to be greater online than offline (H11). Contrary to H10, the engagement in privacy protection did not

⁷ On a scale of 0-1.

Figure 6: A Comparison of Privacy Controls Knowledge Means by Generational Cohort



vary significantly by greater role heterogeneity of family, teachers, individuals under the age of 18 or employers either on Facebook or offline. However, greater family role heterogeneity did have a strong, positive and significant correlation with friend selectivity. This relationship is logical because those who are more stringent in their friend selectivity are more stringent because they only accept Facebook friends who are more close to them, such as family members and close friends. Contrary to H11, the association of role heterogeneity with privacy protection did not vary significantly from offline to online.

Lastly, network size was predicted by H12 to be associated with enhanced use of privacy controls and image management on Facebook. I expected the relationship to be greater on Facebook than offline (H13). H12 was partially supported. Network size was strongly, positively and significantly associated with image management, but not with the use of privacy controls. This could be because individuals use image management as an internal privacy protection strategy to keep other Facebook friends from seeing certain content, while they use privacy

controls to protect against external concerns. Surprisingly, and contrary to H13, offline network size had the opposite association. It was correlated negatively and significantly with privacy protection. Individuals with a greater network size were actually *less* likely to engage in stringent privacy protection offline.

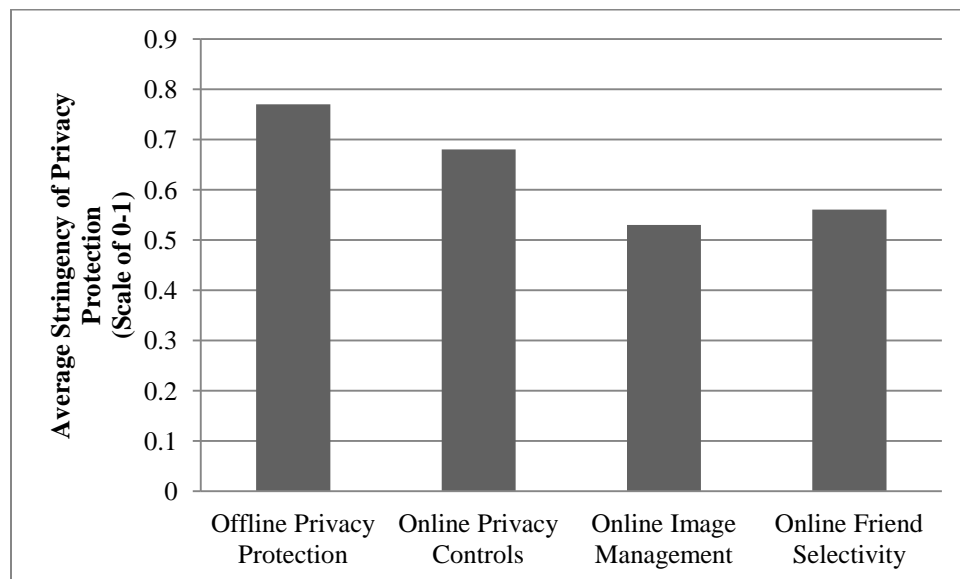
In all, there do not seem to be many significant predictors of Facebook privacy protection. The use of privacy controls is associated with Net Geners, females, and individuals who are more knowledgeable about privacy protection and more conscientious. Image management is correlated with Net Geners and individuals with a greater online network size. Friend selectivity is only related to greater family role heterogeneity.

Also, the relationships between correlates and privacy protection, when compared online and offline, were not consistent. However, the overall direction of these relationships was the most consistent for offline privacy protection and Facebook privacy controls, even though greater conscientiousness was the only significant correlate for both indices. For friend selectivity, the overall direction of these relationships was less consistent with offline privacy protection, but both were positively associated with network size. Image management shared no significant correlates with offline privacy protection and the overall direction of these associations was inconsistent across the two indices. This implies that out of the three types of Facebook privacy protection, privacy controls are most comparable to offline privacy protection. However, the fact that online and offline privacy protection have such different correlates could also mean that online and offline privacy protection may not be as similar as was expected. In order to offer more clarification on this issue, we must directly compare online and offline privacy protection.

A Comparison of Offline and Online Privacy Protection

The second research question asked how similar offline privacy protection is to online privacy protection in order to answer the overarching question: Do people have a reasonable expectation to privacy on Facebook? Means were compared across offline and online privacy protection indices. Greater privacy protection was engaged in offline (Mean = .77) than on Facebook (Privacy Controls Mean = .68, Image Management Mean = .53, Friend Selectivity = .56) (See Figure 7). A Paired Samples T-Test was performed and Facebook users were found to engage in significantly more stringent privacy protection offline than on Facebook at $p=.00$ (See Appendix K).

Figure 7: A Comparison of Offline and Online Privacy Protection Means



However, just because respondents engaged in greater offline privacy protection does not mean that offline and online privacy protection is different. To gauge the similarity of offline and online behaviors, the offline privacy protection index was correlated with each of the three

Facebook privacy protection indices: privacy controls, image management, friend selectivity
(See Table 4).

Table 4: Correlation between Offline Privacy Protection and Facebook Privacy Protection

<u>Facebook Privacy Protection Indices:</u>	<u>Offline Privacy Protection Index:</u>
Privacy Controls	.19**
Image Management	-.14**
Friend Selectivity	.16**

**correlation (r) is significant at $p < .01$.

H14 predicted that individuals who engage in stringent offline privacy protection will also engage in stringent online privacy protection. Privacy controls and friend selectivity have low but significant and positive correlations with offline privacy protection. However, image management is significantly, *negatively* correlated with offline privacy protection. This means that, as predicted, individuals who use more stringent privacy controls and friend selectivity on Facebook, also engage in more stringent privacy protection offline. Individuals who use more stringent image management actually engage in less privacy protection offline.

Next, a regression was performed to determine which variables moderate the relationship between the engagement in offline privacy protection and the use of privacy controls, image management, and friend selectivity. We can also see from these models if the correlations described in Table 4 still remain when controlling for a large number of predictors. The following variables were considered: demographic variables, personality variables, generational cohort. Role heterogeneity and network size were not incorporated. Since they were composed of a separate variable for online and offline, no one variable could be selected in an online/offline

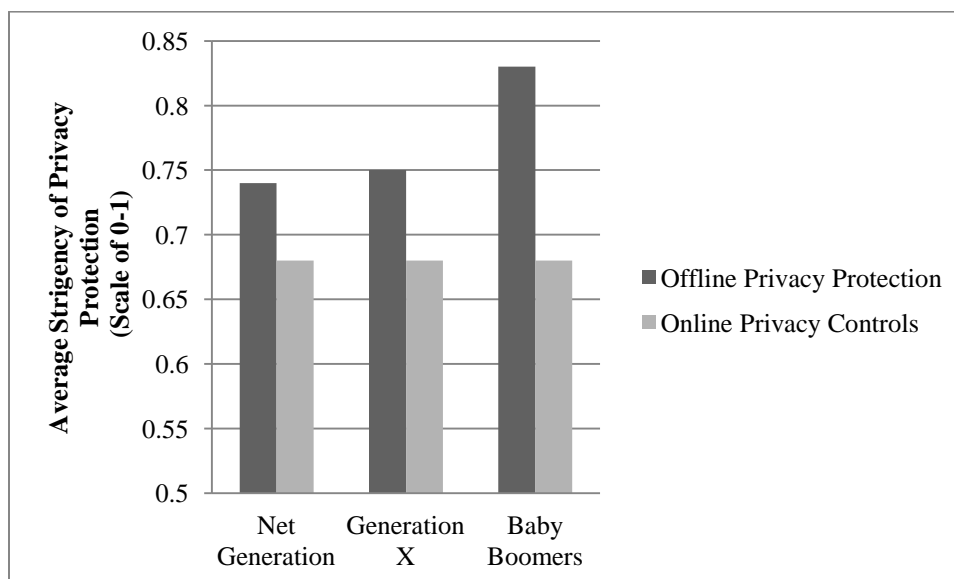
comparison. Only variables such as demographics and personality that were the same offline and online were used.

After controlling for alternative predicting variables, offline privacy protection only had a strong, positive, and significant correlation with Facebook privacy controls (See Table 5). Offline privacy protection had a moderate, positive correlation with friend selectivity but this was marginally significant. The relationship between image management and offline privacy protection was not significant. Therefore, those who engage in more stringent offline privacy protection also engage in more stringent online privacy protection for two out of the three types of online privacy protection studied. These regression findings are mostly consistent with the initial correlation findings except for the fact that the negative correlation between offline and privacy protection and image management is not significant. The possible differences between image management and the other two online privacy protections that might account for this inconsistency will be discussed later.

Table 5 also shows generational cohort to be a moderating variable for each of the three online and offline privacy protection comparisons even when controlled for alternative predicting variables. A comparison of offline and online privacy protection means shows Baby Boomers to have the greatest difference and Net Geners to have the smallest between online and offline mean privacy protection; however, both of these differences were modest in size (See Figure 8). With an Independent Samples T-Test, Baby Boomers were found to engage in significantly more stringent privacy protection offline than Net Geners at $p=.00$ (See Appendix L). As discussed previously, the use of Facebook privacy controls did not differ significantly between generations (See Appendix I). Although Baby Boomers, on average, engage in more stringent offline privacy protection than Net Geners, this distinction is not present in cyberspace.

This suggests that Net Geners are *more* concerned about their online privacy than older generations. This may be because they reveal more personal information online than older generations.

Figure 8: A Comparison of Offline Privacy Protection and Online Privacy Controls Means by Generational Cohort



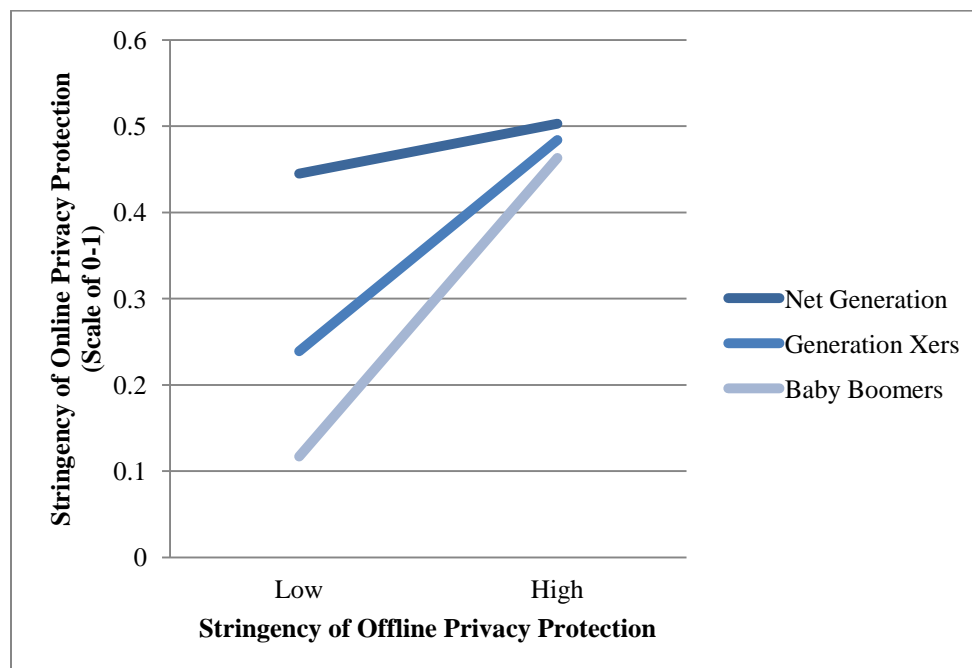
H15 predicted that older generations would engage in more comparable offline and online privacy protection than the Net Generation. An interaction was calculated to determine the distinct relationship between privacy protection and generational cohort (See Figure 9). Baby Boomers and Generation Xers were found to have a high, positive and significant interaction on the relationship between offline privacy protection and Facebook privacy controls. H15 was confirmed. Baby Boomers have the largest positive correlation between offline and online privacy protection. Generation Xers have a slightly smaller correlation. Net Geners do not have

Table 5: A Regression Analysis of the Relationship between Online and Offline Privacy Protection

Moderating Variables	Facebook Privacy Protection		
	Privacy Controls (B)	Image Management (B)	Friend Selectivity (B)
Offline Privacy Protection	0.23**	-0.09	0.13 [^]
White	0.06	0.01	0.02
Asian	0.02	0.01	0.02
Black	-0.02	-0.05	-0.04
Female	0.04*	-0.01	0.01
Agreeableness	-0.01	-0.10	0.06
Conscientiousness	0.14*	0.05	0.01
Emotional Stability	-0.10	-0.01	0.03
Extraversion	-0.04	0.07	0.07
Openness	0.13 [^]	-0.04	-0.07
Income	0.03	-0.04	-0.03
Current Education	0.06	0.06	0.04
Generation Xers	-0.02	-0.05*	0.05*
Baby Boomers	-0.06*	-0.09**	0.07**
N	339	363	360
R ²	.118	.123	.086

*significant at $p < .05$, **significant at $p < .01$, [^]significant at $p < .10$

Figure 9: The Relationship of Offline and Online Privacy Protection by Generational Cohort



a significant correlation. Again, Generation Xers are found to be more similar than Baby Boomers to the online behavior of Net Geners. As predicted, offline and online privacy protection is more comparable for older generations than they are for younger generations. These generations are aligning their online privacy protection with their offline privacy protection. They may even be basing their online privacy protection off of their offline privacy protection. It should also be noted that Net Geners engage in more stringent privacy protection online regardless of the stringency of their offline privacy protections. This further confirms that Net Geners are *more* concerned about online privacy. For image management and friend selectivity, Baby Boomers and Generation Xers were also found to have interactions in the same direction, but with no significance.

My thesis has a causal hypothesis that offline behavioral norms influence the creation of online behaviors, but I cannot prove the direction of this relationship with survey research. There

may be another causal story. Online norms may actually influence offline norms. However, it makes the most logical sense to describe offline behavior as influencing online behavior. Since offline behaviors are learned before online behaviors, offline behavioral norms most likely developed before online norms- especially for the older generations who did not grow up with the Internet. This finding, regardless of the relationship's direction, has significant implications for the central question of the research: Do Facebook users have a reasonable expectation of privacy?

Table 6: A Summary Hypotheses and Findings

H1	Confirmed	Net Geners engage in greater self-revelation online than older generations.
H2	Confirmed	Net Geners have more comparable offline and online self-revelation than older generations.
H3	Rejected	Net Geners engage in more stringent privacy protection online (privacy controls and image management) than older generations.
H4	Partially confirmed	Females use more stringent privacy controls but do not engage in more stringent image management or friend selectivity.
H5	Confirmed	Privacy controls knowledge is associated with a more stringent use of privacy controls.
H6	Rejected	Agreeableness is not a predictor of Facebook privacy protection.
H7	Partially confirmed	Higher conscientiousness is associated with more stringent privacy controls but not image management and friend selectivity.
H8	Rejected	Openness is not a predictor of Facebook privacy protection.
H9	Rejected	Extraversion is not a predictor of Facebook privacy protection.
H10	Rejected	Role heterogeneity is not a predictor of Facebook privacy controls or image management.
H11	Rejected	Role heterogeneity is not a predictor of online or offline privacy protection.
H12	Partially confirmed	Greater network size is associated with more stringent image management but not privacy controls.
H13	Rejected	Network size has a positive association with online privacy protection, but a negative association with offline privacy protection.
H14	Partially confirmed	Privacy controls and friend selectivity are positively correlated with offline privacy protection. Image management is negatively correlated with offline privacy protection.
H15	Confirmed	Offline and online privacy protection is more comparable for older generations than they are for younger generations.

Discussion

Do Facebook users exhibit an expectation to privacy?

The data were analyzed to ultimately determine the answer to the question: Do social media users have a reasonable expectation of privacy? Based on *Katz v. United States* (1967), the legal definition of privacy involves two criteria. First, an individual must exhibit an actual expectation of privacy. Secondly, society must acknowledge this expectation as reasonable, 389 U.S. 361. My study focused on Facebook as one example of online social media, but I believe the insights I draw from this particular site can be applied to other social media sites that involve the sharing of personal information.

In order for Facebook users to meet the first criterion- that individuals expect their self-revelation to be private- they must behave in a way that displays this expectation. One way of determining this is by comparing offline privacy protection based on the Supreme Court example in *Katz* of shutting the door to a public telephone booth with privacy protection used on Facebook. I believe that the overall pattern of results from my survey of 381 adults around the country suggest that the first criterion has been met. In this section, I will also discuss commentary provided by 10 Facebook users with whom I conducted in-depth interviews. The names of these individuals were changed to protect their identity. Although these comments are not representative of Facebook users as a whole, the insights of actual Facebook users, in addition to my already established hypotheses, play an important role in interpreting and explaining the Facebook behavioral tendencies found in my data analysis.

Results show that Facebook users act in ways that are consistent with the notion that they consider their online communication to be private. First, Facebook users engage in online privacy protection that is similar to offline privacy protection. Out of the three types of online privacy protection, Facebook privacy controls were found to be the most highly correlated with

offline privacy protection such as refraining from talking about excessive drinking or sexual experiences in public, even after the relationship was controlled for other possible predicting variables. Not only is the use of Facebook privacy controls most strongly correlated with online privacy protection, these two behaviors were also the most similar in terms of the overall direction and size of the correlates. However, the only correlate with a significant effect was the personality variable conscientiousness.

The use of privacy controls on Facebook is very similar to the *Katz* example of “shutting the telephone booth door,” *Katz v. United States*, 389 U.S. 352, (1967). By using privacy controls, Facebook users are drawing a privacy boundary on Facebook. Information that is limited to only Facebook friends is more private than information that is viewable to all Internet users. Facebook users, regardless of generational cohort, were found on average to use the “Friend” privacy control to restrict their content from public view. Hiding Facebook content behind a protective cyberwall is analogous to concealing a private telephone conversation behind a telephone booth wall. As legal scholar, Semitsu had argued, the courts should imagine the use of Facebook privacy settings as the “twenty-first century equivalent of a phone booth” (Semitsu, 2011, p. 369). My results suggest this is exactly how users apply and even think of these features on the social media sites.

In open-ended conversations, Facebook users discussed their expectation that privacy controls on Facebook should be respected. “My content is more private than a person’s who has their settings set to public,” said Lucy, age 19. When asked how he would react if someone were to find a way to get past his privacy settings without his knowledge or consent, George, age 22 said, “I would feel violated. You are creating a barrier between the people you want to see your

content and the people you don't want. If [others] don't respect that barrier, then it's a privacy invasion."

Friend selectivity is, to a lesser extent, correlated with the use of offline privacy protection such as refraining from criticizing a professor or employer in public. This effect remained even after controlling for other variables that might be responsible for the relationship. An individual who is more selective about Facebook friends will have a more private audience for his or her online content. Preventing unwanted audiences from viewing content on Facebook is also similar to shutting a telephone booth door in order to prevent unwanted audiences from overhearing a private telephone conversation. Like privacy controls, friend selectivity can be seen as a second online equivalent to shutting the telephone booth door. Privacy controls and friend selectivity are actually very similar behaviors- they both allow a user to control who views their content.

However, friend selectivity was correlated to a lesser extent than privacy controls with offline privacy protection. This finding, while not predicted, is not unexpected. It was found that privacy controls are the most commonly used privacy protection across generations. Privacy controls are the only privacy protection that is actually created, explained, and promoted by Facebook. Friend selectivity is a user-initiated behavior which serves as an additional privacy safeguard. Another explanation is that the friend selectivity index was the least reliable index and was only marginally reliable.⁸ In conclusion, both of the variables do appear to guarantee an expectation of privacy on Facebook. This suggests that people may rely on offline expectations of privacy to determine their online behaviors. This is a clear indication that social media users exhibit an expectation of privacy online.

⁸ Cronbach's Alpha (α) = .60

It was also found that individuals who engage in more stringent image management actually employ *less stringent* privacy protection offline. This negative relationship was not significant when other predictors were controlled. While this finding was unexpected, there are a few reasons why image management is distinguishable from privacy controls and friend selectivity. One difference is that privacy controls and friend selectivity are behaviors that block audiences from content while image management limits available content to those who already have access. Offline privacy protection was created to include both limiting content and blocking audiences.

Upon later reflection, image management may not actually be a privacy protection, but a limit on self-revelation. Deleting and refraining from posting certain content is more about limiting the private information you share rather than limiting who is able to see that private information. One explanation of why image management is negatively related to offline privacy protection is that individuals who use greater image management might share less inappropriate content on Facebook in the first place because they are more private individuals. This was found not to be the case, because image management is positively and significantly correlated with Facebook self-revelation.⁹ Facebook users who are more likely to delete inappropriate pictures or postings are also more likely to post inappropriate content on Facebook. This finding further supports the fact that image management may be more related to self-revelation than privacy protection.

Do Facebook users have a reasonable expectation to privacy?

Although engaging in privacy controls and friend selectivity does exhibit a privacy expectation on Facebook, it has still not been determined yet whether or not this expectation is *reasonable*. This criterion is determined by the prevailing standards in society. However, the

⁹ Correlation is $r = .20$ with $p < .01$.

answer to this question is complicated because the *Katz* test assumes that privacy expectations are well-developed and stable, and new technologies can put these expectations in flux, *United States v. Jones*, 565 U.S. _____, (2012). One way of measuring society's standard is to discover whether certain groups of Facebook users are less likely to reveal information and to use privacy protection online. These groups are more likely to see a difference between cyberspace and offline and less likely to feel that Facebook behaviors afford the same protections as offline behaviors. Thus, these groups are less likely to acknowledge this expectation of privacy on Facebook as reasonable. My results suggest that certain groups of Facebook users do differ in their behavior on Facebook. A deeper analysis can determine why these groups of Facebook users are more or less likely to agree that social media users have a reasonable expectation of privacy.

Self-Revelation

In general, Facebook users were found to reveal less information online than offline. This finding suggests that Facebook users are concerned that Facebook conversations are less private than an offline conversation, and thus, are more cautious with what they reveal. While all generations revealed less personal information on Facebook than offline, Baby Boomers revealed the least amount of inappropriate information on Facebook. Some Baby Boomers are more cautious. "I'm not 100% confident that my privacy settings can keep out unwanted onlookers-people can always figure out how to work a system. It makes me more cautious about what information I share," said Joyce, a 42-year-old participant. Others don't understand why some people enjoy sharing personal information online: "I find it odd when people share information about what they are doing. First of all, why would anyone else care, and second, who would want to publicize that to the world?" asked Bruce, aged 50. In addition, older generations simply

lack experience with the site. “I don’t really put anything on Facebook. I use Facebook more to look at other peoples’ stuff,” Bruce added.

On the other hand, younger generations identify more benefits in sharing private information online (Debatin et al., 2009; Ellison et al., 2007). Beth, age 18, sees Facebook as an opportunity to connect with friends she no longer sees as often: “I want to give off a good impression of my college experience to friends back home.” Facebook can also help promote a certain image which some users feel pressured to maintain. “You don’t want to seem like a bore on Facebook,” George, age 22, explained about why he sometimes posts inappropriate information. However, it seems that even for the Net Generation there are limits to what is appropriate to post on Facebook because of concerns about the consequences of revealing too much personal information online (Benson, 2009). “I personally don’t post pictures suggesting alcohol use or drug use or any sexual innuendo. To a lesser extent, bad language is also not appropriate,” said George. Christina, age 20, also warned about taking pictures holding a red cup- a symbol of drinking among the Net Generation. “The red cup- that’s like a classic nono. Even if it’s just water, don’t have a red cup,” she advised.

Younger generation, lower income and education, greater network size, and extraversion were all positively associated with greater self-revelation only on Facebook. These characteristics appear to fall into two groups: extraversion and generational cohort. Extraverted individuals are more likely to take risks and share information (Junglas et al., 2008) and will logically have a larger social network on Facebook. The second category, generational cohort, encompasses both income and education because respondents in the youngest generational cohort had the lowest income and current education levels. Two characteristics of Net Geners, maturity and vulnerability, explain why younger generations reveal more information online. Net

Geners may reveal more because they are younger and more immature. These individuals may think less about the consequences of revealing personal information online than older generations. Net Geners, having lower income and education levels, are also less likely to have a professional image to maintain and therefore are less vulnerable.

While role heterogeneity was predicted to influence privacy protection, it actually appears to play a greater role in self-revelation. For instance, it was found that individuals with more family members on Facebook are less likely to reveal personal information on Facebook. Individuals with a higher current education were found to have a greater number of employers and teachers as Facebook friends. These individuals, more likely to be part of an older generation, may feel that their Facebook friends would judge them more harshly for revealing inappropriate information and may be more worried about potential negative consequences in their professional life. “When I was a freshman in college, I didn’t have to worry about applying to jobs or school. Due to a combination of both immaturity and also being in less professional situations, I was less guarded than I am now on Facebook and Twitter,” explains George, age 22. This is also supported by the fact that those with a higher current education level use more stringent privacy controls. However, role heterogeneity could also be an effect of self-revelation rather than a cause. Users who reveal less on Facebook may be more comfortable with having a more heterogeneous network on Facebook. The association of greater self-revelation with lower income and education level could also be the result of a cultural difference, based on socio-economic status, rather than one based on maturity and vulnerability. A future study could attempt to explain this difference in self-revelation online.

One unexpected finding was that highly conscientious individuals have high self-revelation both online and offline, even though they are more likely to be concerned about what

others may do with this information (Junglas et al., 2008). However, sharing information is only half of the process. Facebook users can also limit unwanted access to private information by engaging in privacy protection. It may be that while conscientious individuals share more, they also more carefully control who has access to that information. Indeed, in this study, conscientiousness was found to predict the use of privacy controls.

Not only do Net Geners reveal more online, but they are also more consistent with what they share online and offline compared to older generations, confirming Benson's findings (2009). Net Geners do not seem to distinguish between cyberspace and offline when it comes to sharing information. "Some of my friends treat Facebook as a diary," said Jeremy aged 19. In fact, it is possible that Net Geners view social media as an online reflection of their offline world. Beth, age 18, feels pressure to keep her Facebook image consistent with her offline image. "I feel like I have to have up-to-date profile pictures. I can't use a picture from last year because then it will be like something's wrong with me now and I don't want to be seen," she said.

For Baby Boomers, online and offline self-revelation is not similar. Baby Boomers who are more self-revelatory offline are actually less self-revelatory online. Cyberspace is not a reflection of offline life. Baby Boomers treat cyberspace differently- they see self-revelation offline and online as distinct phenomena. This further implies why they are more cautious than the Net Generation in revealing information online.

Privacy Protection

While it was predicted that Net Geners would engage in less privacy protection on Facebook, it was actually found that older generations, as a whole, use less stringent privacy controls and image management. Since older generations reveal less personal information online,

these individuals may engage in less stringent privacy protection because they have less information to hide. “I’m not concerned about who can see my profile because I put very little information out there- only things that I would be comfortable showing anybody,” explained Bruce aged 50. Because they have less to hide, their concern for protecting their Facebook content is also lessened. “Newspaper reporters, my mothers, and nosy neighbors are more of a concern to me than a privacy invasion on Facebook” said Hilary aged 50.

While Net Geners use more stringent privacy controls in general, the average Facebook user, regardless of generational cohort, was found to use the “Friend” privacy control. The “Friend” setting allows only Facebook friends to access Facebook content. Thus, on average, Facebook users privatize their content. Net Geners are more likely to use the “Custom” setting which is a more stringent control because it limits content to specific Facebook friends. Why are Net Geners more likely to take this extra step to protect their privacy?

One explanation is that Net Geners are more concerned about their online privacy than older generations. Indeed, this was found to be this case. Net Geners, who reveal more personal information online, have a reason to be more concerned about their privacy. Net Geners also use more stringent image management on Facebook than older generations. Older generations do not have the same need to manage their online image because they don’t reveal personal information that would be considered inappropriate in the first place. Since Net Geners have decided to reveal more inappropriate information online, they have a greater need to manage their image.

Another explanation is that Net Geners are more knowledgeable about privacy settings and are therefore savvier users of “Custom” controls than older generations. I also found evidence for this in the current study. Further supporting this claim, I found that out of the three Baby Boomers interviewed, not one could describe their Facebook privacy controls when asked.

Joyce, age 42 explained, “I don’t take the time to learn about privacy controls because I don’t share information that I’m that concerned about protecting.” On the other hand, all Net Geners interviewed could name their privacy settings when asked and could even describe a specific reason for choosing this privacy setting. Younger Facebook users are more knowledgeable about and take greater advantage of Facebook’s most stringent privacy settings. Christina, age 20, explained, “I use the custom privacy setting a lot because some of my Facebook friends are family members or [University] faculty. If I’m using profanity or something I don’t want my daddy to see, I make sure to customize him out.” While an older user may simply decide not to use profanity, the Net Generation privatizes it using Facebook privacy controls.

Personality variables were not found to have a significant effect on the use of Facebook privacy protection. Jungals et al. (2008) did find more conscientious individuals and individuals more open to experience to have more online privacy concerns; however, only conscientiousness was found to predict more stringent use of privacy controls. Junglas et al. (2008) also found that less agreeable and more open individuals have more online privacy concerns (Junglas et al., 2008), but I found no evidence for these relationships in the current study. It could be that for agreeable and open individuals, concern for online privacy does not actually influence privacy protection. Or, these individuals could find ways other than altering their online behavior to minimize their privacy concerns and risks. For instance, individuals low on agreeableness and high on openness were found in this study to engage in less self-revelation on Facebook.¹⁰ Instead of using privacy controls to minimize who has access to their content, they might instead refrain from posting inappropriate content in the first place. However, both the agreeableness and

¹⁰ The effect of openness on online self-revelation was not significant.

openness to experience indices had a low Cronbach's Alpha. Even though a well tested measure was used, these findings are less reliable.¹¹

Role heterogeneity also had barely any significant influence on the use of online and offline privacy protection. Based on Goffman's theory on front stage and backstage (1959), this finding was also unexpected. This may be due to an invalid measure of network heterogeneity. I compared a ratio of Facebook friends in each "front stage" group with a report on how often an individual finds himself or herself in an offline situation where both front stage and backstage audiences are present. However, one explanation is that role heterogeneity is more related to self-revelation than privacy protection. Individuals with greater role heterogeneity shared less personal information on Facebook because they were more concerned with the negative consequences on their professional life. But, it cannot be determined from this research if greater role heterogeneity causes less self-revelation or if it is an effect. It may be that individuals who reveal less on Facebook may be more comfortable with accepting Facebook friends that are family members, teachers or employers.

Network size unexpectedly had an opposite effect online than it did offline. Online, greater network size predicted more stringent privacy protection. This may occur because Facebook users with a larger social network feel a greater need to protect their content. Or, the reverse could be true. Those who engage in more stringent privacy protection may feel more comfortable engaging in greater self-revelation regardless of network size. Like role heterogeneity, network size may actually be a consequence rather than a cause of privacy protection. Offline, an individual with greater network size engaged in less stringent privacy protection. It is possible that, offline, individuals who value privacy more highly will have fewer friends and reveal less information will not need to engage in privacy protection. In contrast,

¹¹ Agreeableness: Cronbach's Alpha (α) = .38, Openness: Cronbach's Alpha (α) = .33

individuals who have more friends may be less private and may feel comfortable revealing personal information to more people. Rather than network size influencing privacy protection, it could actually be a personality trait such as extraversion or openness which influences both behaviors. However, neither extraversion nor openness was found to have a significant influence.¹²

In conclusion, it appears that a privacy boundary has been established on Facebook across all generational cohorts. However, older generations, in general, have different behaviors on Facebook than Net Geners. Baby Boomers, as a whole, are less self-revelatory and engage in less stringent privacy protection online. Their remedy to privacy risk is not the use of privacy controls, but the decision to not post inappropriate content. Is this because Baby Boomers are not as familiar with social media technology, in particular, privacy settings? Or, because they believe that there is no expectation of privacy online?

Baby Boomers have less experience on social media and are therefore less knowledgeable about sharing and privatizing content. Since Baby Boomers reveal less information online, they may have less of a concern about online privacy and may spend less time learning about privacy settings. Baby Boomers are much less likely than younger generations to use the "Custom" privacy control which is more difficult to manage and also more time consuming to use than the "Friend" privacy setting. Net Geners, who are more likely to use the "Custom" control, have more of an incentive to master the use of this control because they reveal more inappropriate information online.

Another explanation is that Baby Boomers are hesitant to conform to the behavioral norms that have been established by Net Geners online. Net Geners, who use more stringent

¹² It should be noted that the openness to experience index received a low Cronbach's Alpha and has low reliability as a measure. Openness: Cronbach's Alpha (α) = .33.

privacy controls regardless of their offline behavior, have adapted a behavioral standard online for privacy protection. However, older generations, having less experience online, have not adopted this same standard. Rather, their offline privacy protection is strongly correlated with their online privacy protection. Older generations are applying offline privacy norms as they navigate privacy boundaries in cyberspace rather than taking cues from the Net Geners. Net Geners also engage in greater self-revelation online and are more consistent in their self-revelation from online to offline than Baby Boomers. Again, this implies that Baby Boomers are hesitant to adopt the online behavioral norms of Net Geners when it comes to sharing and privatizing information online. If this is true, Baby Boomers may be less likely to see these behaviors as guaranteeing a reasonable expectation of privacy.

While online behaviors do differ across generations and attitudes about online privacy concern are currently in flux, it can be predicted that the online behavior of Net Geners will eventually become the norm. Generation X is a generation in transition. This generation's self-revelation and privacy protection fall in between that of Net Geners and Baby Boomers. Generation Xers were found to use slightly more privacy controls than Baby Boomers and to be slightly more self-revelatory than Baby Boomers. As Tapscott (2009) predicted, Generation Xers are most similar to the Net Generation when it comes to online behavior. This is evidence that although the behaviors of Net Geners are currently seen as normatively different from older generations, as the cohorts continue to age, the Internet behaviors of Net Geners may become the norm.

Since generational cohort has proven to have such an important influence on both the use of self-revelation and privacy protection, it is difficult to say that all generations will currently agree on a reasonable expectation of privacy on social media. Baby Boomers may be less willing

to recognize a reasonable expectation of privacy because these individuals use Facebook so differently than younger generations. “Facebook is free. Facebook is a business. I use Facebook, but I keep these two things in mind always,” said Hilary, age 50. However, not all Baby Boomers are as skeptical about an expectation of privacy on Facebook. Bruce, age 50, feels that “if its password protected and if you’ve got the right security controls, then it should be considered private regardless of the media used.”

It appears that a privacy boundary has been negotiated online. The “Friend” privacy control, used by all generations, restricts Facebook content from the public view. Although society may have not reached a definitive consensus on whether or not this affords a reasonable expectation of privacy, an agreement is in progress as demonstrated by the Generation X’s role as a transitional generation. Thus, the question remains, is the difference in behavior due to older generations’ lack of experience with and comfort with social media? Or is it due to a belief that cyberspace does not afford the same expectations of privacy as offline? Once older generations have had more experience with social media, and the Net Generation ages and becomes a larger part of the citizenry, we will have a better sense of whether or not *Katz* should be expanded to include social media sites and the Internet.

The Role of Legislative Bodies

“The *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations...dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes,” writes Justice Alito, *United States v. Jones*, 565 U.S. _____, (2012), (p. 10). According to Alito, the *Katz* test should be applied to a society that has a “well-developed and stable set of privacy expectations.” Social media sites have encouraged greater

self-revelation on the Internet and changed expectations of privacy online. It will take time for these privacy expectations to develop and stabilize. Since the development of these social media is so recent, older generational cohorts, having less experience with the technology, may not have been able to develop a consistent popular attitude towards Facebook privacy boundaries.

Until it is determined why older generations engage in less stringent privacy protection, it may not be the place for the courts to draw this online privacy boundary using the *Katz* test. Prematurely interpreting a societal attitude in a major court ruling about online privacy would most likely be viewed as judicial activism which occurs when judges allow their personal views about public policy, among other factors, to guide their decisions. However, the courts are not the only possible actor in this scenario. Opponents of this judicial philosophy encourage the courts to wait for policy makers to draft legislation that best targets society's concerns. "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way," writes Justice Alito in his opinion, *United States v. Jones*, 565 U.S. _____, (2012), (p. 13).

While it is important to determine a Facebook users' expectation of privacy, it is also important to acknowledge the groups on Facebook, such as older generational cohorts, who may disagree with this determination. Because there are significant differences in Facebook behavior across Facebook user generations, it is difficult to currently label this reasonable expectation of privacy as "well-developed and stable" until it is better understood why these groups differ. However, based on these findings, it can be assumed that the "Friend" privacy control setting is a standard for all Facebook users regardless of generation. Therefore, as Justice Alito recently

suggested, legislators may need to step in and define privacy boundaries online along this already established privacy boundary for those who need and expect it most.

Summary of Limitations and Further Research

While these results suggest that a general consensus about privacy expectations online has yet to coalesce, several limitations in the current study would need to be addressed before recommending legal or legislative policy action. A large sample was used, but it was not a representative one. The results found in this study can hint at the general behavior Facebook users, but it cannot be assumed that these results will apply to all Americans. Another limit of survey research is that while a causal direction was implied, we cannot be certain about the causal antecedents of online privacy protection. It is a logical assumption to make that since offline behaviors are learned before online behaviors, a user may simply apply their offline privacy standards to their behavior in cyberspace. However, the direction of this relationship may actually be reversed for many citizens, especially those in younger generations who are learning norms of social interaction online before adulthood. Further research on this question could attempt to definitively determine the directionality of this relationship. But, for legal purposes, it is enough to say that these offline and online privacy protections are similar in order to afford the same protection offline and online.

Another limitation is that new measures were used. Although for the most part reliable,¹³ these measures may not be valid. I attempted to analogize interactions and behaviors on cyberspace with offline interactions and behaviors. Since the development of the Internet, Supreme Court justices and legal scholars have attempted to create these analogies in order to determine how law should apply to cyberspace. However, there are inherent differences between

¹³ As discussed, the friend acceptance, agreeableness and openness indices all had low Cronbach's Alpha scores, making these indices less reliable.

cyberspace and offline that make it very difficult to develop these analogies. As discussed in the methods section, I attempted to make logical analogies between online and offline behaviors, but, these are not the only online and offline analogies possible. Further research could be conducted using different analogies in an attempt to find the most valid measure of behaviors both offline and on Facebook. It must also be asked whether or not these online analogies apply to other social media sites such as Twitter, Linked In, and Myspace. Privacy controls are common to each of these social media technologies, but further research could show if friend selectivity and image management are also used, and if privacy controls are used to the same extent across all social media sites.

This research also mostly dealt with the Fourth Amendment and possible online privacy invasions by law enforcement, employers, and school officials. These privacy risks were based on revealing information that these groups deem inappropriate or illegal. However, there are also other types of privacy risks on Facebook. For example, publishing personal information such as an address, phone number, credit card, or social security number online can have its own risks related to safety and identity theft. Lucy, age 19, uses privacy settings because “there are a lot of crazy people out there. I want to feel safe.” Other groups can also be seen as invasive. Commercial organizations use data mining of Facebook and other social media sites to provide information about consumer interests and preferences. Previous research has already dealt with some of these questions, but it is important to better understand the attitudes and behaviors of Facebook users regarding these types of privacy risks in order to determine whether or not more protective legislation needs to be passed.

Conclusion

The development of social media, which encourages the sharing of personal information, has created serious privacy risks for Internet users. While social media usage is inherently social, many users still consider their shared content to be private. In other words, social media users have negotiated a privacy boundary on the Internet. The “Friend” privacy control on Facebook, which limits content from public view, is the most consistently applied privacy setting across generations. Information that is protected by privacy settings developed by social media sites is considered to be more private than information that is not. However, this sense of privacy, if not legally recognized, may not be realized. Even though social media users take similar steps online and offline to protect their privacy, current privacy law does not afford these individuals with an expectation of privacy in cyberspace. I hope that this research will contribute to the development of a new “Katz” standard that protects privacy both online and offline.

The courts, using the current *Katz* test, may be hesitant to rule that social media users have a reasonable expectation of privacy online based on the fact that generational cohorts differ so significantly in their behaviors on social media sites. Further research can determine if these behaviors differ because of a lack of knowledge or experience with the site, or if older generations simply believe that there is no reasonable expectation of privacy online. However, it is unrealistic that social media users must wait for their established privacy boundary to be legally confirmed by Supreme Court until an indefinite point in the future. Not only must a case about social media privacy invasion reach the Supreme Court, but society’s consensus regarding a reasonable expectation of privacy on social media must also be better understood. Until then, social media users, 50% of all Americans according to study by the Pew Research Center, will have a false sense of security online (Sengupta, 2011). The percentage of Americans with their

online privacy at risk is unacceptable. Thus, legislators must take action in order to protect this established online privacy boundary, and quickly.

Legislation should be passed to afford social media users the same legal protections that are guaranteed offline. While private information may be confiscated offline via a court-ordered warrant or subpoena, an individual must have notice and knowledge of this access. Privacy law should also limit the unauthorized access of social media content without a social media user's knowledge or consent. The Federal Trade Commission recently worked with Facebook to update its privacy policy to limit Facebook's ability to override its users' privacy settings (Sengupta, 2011). Legislators should expand this policy to restrict any individual from overriding a user's privacy settings without a court-issued warrant or subpoena. Facebook has recently released statements warning employers against accessing a job applicant's private content because it violates a user's privacy (Duncan, 2012). Policy makers should take a similar stance and also restrict employers, law enforcement, and other individuals from violating a social media user's expectation of privacy by accessing private content without his or her knowledge or consent.

Legislators can also update the Stored Communications Act, 18 U.S.C. §§ 2701, a legislative initiative that was passed to limit the ability of third-party Internet service providers to reveal information to the government and non-government entities, in order to better protect privacy on social media sites. District court Judge Morrow ruled that social media messages and privatized wall posts were subject to the SCA in *Crispin v. Christian Audigier Inc*, 717 F. Supp. 2d 991 (2010). In line with this ruling, legislators can expand the SCA to protect wall posts, messages and other content on social media such as photo-sharing and event-creating that are privatized (Semitsu, 2011). Limiting the voluntary disclosure abilities of third parties would also correspond with a recent Supreme Court ruling, *Warshak v. United States*, 532 F.3d 521 (2008),

which limited the ability of Internet service providers to turn over the content of a user's emails without his or her knowledge. While the SCA only currently protects electronic communications that have been in storage for less than 180 days, the SCA could also be expanded to require that all private online communication, regardless of how old it is, must require user-notice before it is accessed. It is not likely that Facebook users feel that their older content on Facebook is less private than newer posts.

These changes would not make it impossible to access information that has been privatized on social media sites, but would instead limit the access of private information in cyberspace to the rules of offline privacy law. While some may argue that social media users should simply reveal less information online, this argument does not take into account changing behavioral norms. Online behavioral norms are currently in transition. As the Net Generation ages, its online behaviors will become the norm. Instead of attempting to change behavioral norms on the Internet, legislators should work to protect and more concretely define the already established privacy boundary online.

References

- (2011). "Statistics." *Facebook*. Retrieved from <http://www.facebook.com/press/info.php?statistics>.
- (2011, January 18). "Facebook Statistics, Stats & Facts for 2011." *DigitalBuzz*. Retrieved from <http://www.digitalbuzzblog.com/facebook-statistics-stats-facts-2011/>.
- (2011, March 7) "Facebook Demographics Revisited- 2011 Statistics." *Social Media Today*. Retrieved from: <http://socialmediatoday.com/kenburbary/276356/facebook-demographics-revisited-2011-statistics>.
- (2011, September 22). "Facebook F8: Redesigning and hitting 800 million users." *The L.A. Times*. Retrieved from <http://latimesblogs.latimes.com/technology/2011/09/facebook-f8-media-features.html>.
- (2011, November 29). "Facebook." *The New York Times*. Retrieved from http://topics.nytimes.com/top/news/business/companies/facebook_inc/index.html
- (2006, August 15). "The Fuzz wants to add you as a friend." *ZDNet*. Retrieved from <http://www.zdnet.com/blog/education/the-fuzz-wants-to-add-you-as-a-friend/411>.
- Agre, Philip E. & Marc Rotenberg, Eds. (1997). *Technology and Privacy: The New Landscape*. Cambridge, MIT Press.
- Arthur, C. (2009, June 29). "Average Twitter user has 126 followers and only 20% of users go via web." *The Guardian*. Retrieved from <http://www.guardian.co.uk/technology/blog/2009/jun/29/twitter-users-average-api-traffic>.
- Beckstrom, D.C. (2008-2009). Who's Looking at Your Facebook Profile- The Use of Student Codes to Censor College Students' Online Speech. *Willamette Law Review*, 45, 261-312.
- Benson, J. (2009). Saving Face: The Offline Implications of Behavior on Facebook. (Unpublished doctoral dissertation). Dalhousie University: Nova Scotia, Canada.
- Biddle, B. J. (1986). Recent Developments in Role Theory. *Annual Review of Sociology*, 12(1), 67-92.
- Bosker, B. (2011, August 23). Facebook's New Privacy Settings: 7 Things You Need To Know. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/2011/08/23/facebooks-new-privacy-settings_n_934413.html#s337268&title=Tag_People_Youre/.
- Brandenburg, C. (2008). The newest way to screen job applicants: A social networker's nightmare. *Federal Communications Law Journal*, 60(3), 597-626.
- Bratman, B. (2001-2002). Brandeis and Warren's The Right to Privacy and the Birth of the Right to Privacy. *Tennessee Law Review*, 69, 623-653.
- Burbary, K. (March 7, 2011). "Facebook Demographics Revisited – 2011 Statistics." *Web Business*. Retrieved from <http://www.kenburbary.com/2011/03/facebook-demographics-revisited-2011-statistics-2/>.
- Butler, E., McCann, E. & Thomas, J. (2011). Privacy Setting Awareness on Facebook and Its Effect on User-Posted Content. *Human Communication*, 14(1), 39–55.
- Costa, P.T., McCrae, R.R., & Dye, D.A. (1991). Facet scales for agreeableness and conscientiousness: a revision of the neo personality inventory. *Personal Individual Differences*, 12(9), 887–898.
- Crispin v. Christian Audigier, Inc. 717 F. Supp. 2d 965 (C.D. Cal. 2010)
- Caloyannides, M. (2003). Privacy vs. Information Technology. *IEEE Security & Privacy Magazine*, 1(1),100-103.

- Davis, W. (2010, August 3). Study: Dramatic Rise In College Students Tweaking Facebook Privacy Settings. *Online Media Daily*. Retrieved From <http://www.mediapost.com/publications/article/133070/>.
- Debatin, B., Lovejoy, J.P., Horn, A.K., & Hughes, B.N. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer Mediated Communication*, 15, 83-108.
- Duncan, G. (2012, March 23). Facebook warns employers: don't ask for passwords. *Yahoo! News*. Retrieved from <http://news.yahoo.com/facebook-warns-employers-dont-ask-passwords-163806953.html>.
- Gabbert, E. (2011, October 17). Facebook Wall of Shame: Facebook's Failures, Criticisms and Missteps. *WordStream*. Retrieved from <http://www.wordstream.com/blog/ws/2011/10/17/facebook-wall-of-shame-infographic>.
- Giles, J. (2012, January 25). FBI releases plans to monitor social networks. *NewScientist*. Retrieved from <http://www.newscientist.com/blogs/onepercent/2012/01/fbi-releases-plans-to-monitor.html>.
- Goffman, E. (1959) *The Presentation of Self in Everyday Life*. New York: Anchor Books.
- Gosling, S.D., Rentfrow, P.J. and William, B.S. (2003). A very brief measure of the big-five personality domains. *Journal of Research in Personality* 37, 504–528.
- Hill, K. (2011, October 3). What Prospective Employers Hope To See In Your Facebook Account: Creativity, Well-Roundedness, & 'Chastity'. *Forbes*. Retrieved from <http://www.forbes.com/sites/kashmirhill/2011/10/03/what-prospective-employers-hope-to-see-in-your-facebook-account-creativity-well-roundedness-chastity/>
- Hodge, M.J. (2006). Fourth Amendment and Privacy Issues on the New Internet: Facebook.com and Myspace.com. *Southern Illinois University Law Journal*, 31(1), 95-122.
- Hough, M. (2009). Keeping it to Ourselves: Technology, Privacy, and the Loss of Reserve. *Technology in Society*, 31(4), 406-413.
- Junglas, I.A., Johnson, N.A., & Spitzmuller, C. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. *European Journal of Information Systems*, 17, 387-402.
- Katz v. United States*, 389 U.S. 347 (1967).
- Kerr, O.S. (2004). A User's Guide to the Stored Communications Act and a Legislator's Guide to Amending It. *George Washington Law Review*, 72, 1208-1243.
- Kerr, O.S. (2009). The Case for the Third-Party Doctrine. *Michigan Law Review*, 107, 561-602.
- Kornblum, J. & Marklein M.B. (2006, March 9). What you say online could haunt you; Schools, employers scrutinize social websites such as MySpace and Facebook. *USA Today*. Retrieved from <http://www.usatoday.com/educate/college/firstyear/articles/20060319.html>.
- Lewis, K., Kaufman, J., & Christakis, N. (2008). The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network. *Journal of Computer Mediated Communication*, 14, 79-100.
- Lipka, S. (2008). The Digital Limits of In Loco Parentis. *Chronicle of Higher Education*, 54(26) pA1.
- Moore, Jr., Barrington (1984). *Privacy: Studies in Social Cultural History*. Armonk, NY, M. E. Sharpe.

- Moschis, George P., Roy L. Moore, and Ruth B. Smith. (1984). The Impact of Family Communication on Adolescent Consumer Socialization. *Advances in Consumer Research*, 11, 314–319.
- Muck, P.M., Hell, B. and Gosling, S.D. (2007). Construct validation of a short five-factor model instrument: a self-peer study on german adaptation of the ten-item personality inventory (tipi-g). *European Journal of Psychological Assessment*, 23(3), 166–175.
- Olmstead vs. United States, 277 U.S. 438 (1928).
- Popkin, H. (2010, January 13). Privacy is dead on Facebook. Get over it. *MSNBC*. Retrieved from http://www.msnbc.msn.com/id/34825225/ns/technology_and_science-tech_and_gadgets/t/privacy-dead-facebook-get-over-it/#.TsR7qXKwW3c.
- Rothke, B. (2010, June 14). The Facebook privacy paradox. *CSOOnline*. Retrieved from <http://www.csoonline.com/article/596685/the-facebook-privacy-paradox?page=1>.
- Semitsu, J. (2011). From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance. *Pace Law Review*, 31, 291-381.
- Sengupta, S. (2011, November 29). F.T.C. Settles Privacy Issue at Facebook. *The New York Times*. Retrieved from <http://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html>.
- Sengupta, S. (2011, August 26). Half of America Is Using Social Networks. *The New York Times*. Retrieved from <http://bits.blogs.nytimes.com/2011/08/26/half-of-america-is-using-social-networks/>.
- Sidoti, M.S., Duffy, P.J., & Asfendis, P.E. (2010, October 4). How Private is Facebook Under SCA? *Gibbons Law*. Retrieved from <http://www.gibbonslaw.com/files/1297115450.pdf>.
- Smith, W. & Kidder, D. (2010). You've been tagged! (Then again, maybe not): Employers and Facebook. *Business Horizons* 53, 491-499.
- Snell, R. (2011, April 25). Fed Mine Facebook for info. *The Detroit News*, pp. 3A
- Solove, D.J. (2002). Conceptualizing Privacy. *California Law Review*, 90, 1087-1156.
- Stone, B. (2006). Web of risks: Students adore social-networking sites like Facebook, but indiscreet postings can mean really big trouble. *Newsweek*, 148(7), 76.
- Tapscott, D. (2009). *Grown Up Digital: How the Net Generation is Changing Your World*. New York: McGraw-Hill.
- The Stored Communications Act 18 U.S.C. §§ 2701 to 2712 (1986).
- United States v. Jones*, 565 U. S. ____ (2012), No. 10–1259, slip op. (U.S. January 23, 2012), <http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf>.
- United States v. Miller*. 425 U.S. 435 (1976).
- United States v. Warshak*. 532 F.3d 521 (2010).
- Ware, W. (1986). Emerging Privacy Issues. *Computers & Security*, 5(2), 101-113.
- Warren S. & Brandeis L. (1890) The Right to Privacy. *Harvard Law Review* 4(5).
- Welsh, T. (2008, May 6). Police Watch Your News Feeds, Too. *The Badger Herald*. Retrieved from http://badgerherald.com/news/2008/05/06/police_watch_your_ne.php.
- Wolinsky, C. & Sylvester, J. (1992). Privacy in the Telecommunications Age. *Communications of the ACM*, 35(2), 23-25.
- Youn, S. (2008). Parental Influence and Teens' Attitude toward Online Privacy Protection. *The Journal of Consumer Affairs*, 42(3), 362-388.
- Zeidner, R. (2007). How deep can you probe? *HRMagazine*, 52(10), 57-60.

Appendix A: Demographics of Mechanical Turk Sample

Current/Highest Level of Education Received	
Completed High School	14%
Currently Enrolled at a 2 year college	4%
Currently enrolled at a 4 year college	17%
Completed a 2 or 4 year college degree	38%
Currently pursuing/Completed a higher degree	26%

If currently enrolled in a 4 year college, what grade?	
Freshmen	16%
Sophomore	19%
Junior	24%
Senior	40%

Race	
White, Hispanic origin	16%
White, Non-Hispanic origin	49%
American Indian or Alaska Native	3%
Asian or Pacific Islander	25%
Black or African American	3%

Income	
Less than \$19,999	30%
\$20,000-\$49,999	33%
\$50,000-\$99,999	20%
More than \$100,000	16%

Appendix B: Demographics of College Sample

Age	
18	27%
19	43%
20	7%
21	12%
22	12%

Grade Level	
Freshmen	53%
Sophomore	23%
Junior	7%
Senior	17%

Race	
White, Hispanic origin	15%
White, Non-Hispanic origin	65%
American Indian or Alaska Native	10%
Asian or Pacific Islander	8%
Black or African American	2%

Appendix C: Comparison between Mechanical Turk and College Sample

Correlation between Offline and Online Self-Revelation

Mechanical Turk Net Generation Sample

Offline Self-Revelation:

Facebook Self-Revelation:

.48**

**correlation (r) is significant at $p < .01$.

College Sample

Offline Self-Revelation:

Facebook Self-Revelation:

.59**

**correlation (r) is significant at $p < .01$.

Correlation between Offline and Online Privacy Protection

Mechanical Turk Net Generation Sample

Offline Privacy Protection:

Facebook Privacy Protection Indices:

Privacy Controls .07

Image Management -.13

Friend Selectivity .06

**correlation (r) is significant at $p < .01$.

College Sample

Offline Privacy Protection:

Facebook Privacy Protection Indices:

Privacy Controls -.00

Image Management -.12

Friend Selectivity .03

**correlation (r) is significant at $p < .01$.

Appendix D: Index Measures

Offline Self-Revelation Index (6 items, 4 answer choices for each)

How often do you engage in each of the following activities?

For each action, chose one of the following:

(Often, occasionally, sometimes, never)

1. I talk about drug use with my friends.
2. I talk about excessive drinking with my friends.
3. I talk about sexual experiences with my friends.
4. I wear revealing clothing when I go out to a party or bar with my friends.
5. I talk negatively about class or a teacher with my friends.
6. I use swear words when I talk to my friends.

Facebook Self-Revelation Index (9 questions, 4 answer choices for each)

How often do you engage in each of the following activities on Facebook?

For each action, chose one of the following:

(Often, occasionally, sometimes, never)

1. Use swear words in a comment or status.
2. Talk about sexual experiences in a comment or status.
3. Post or am tagged in photos wearing revealing clothing.
 - a. Have you ever made one of these photos a profile picture? (yes/no)
4. Post or am tagged in photos holding red cups or bottles of beer, wine, or alcohol.
 - a. Have you ever made one of these photos a profile picture? (yes/no)
5. Criticize a class, professor or a GSI in a comment or status.
6. Criticize an employer or workplace in a negative way in a comment or status.
7. Talk about excessive drinking in a comment or status.
8. Post or am tagged in photos where I am making out with a friend or significant other.
 - a. Have you ever made one of these photos a profile picture? (yes/no)
9. Post or am tagged in photos using drugs.
 - a. Have you ever made one of these photos a profile picture? (yes/no)

Facebook Privacy Protection Indices

Privacy Control Index (3 items)

1. What is your default privacy setting?
Public
Friends only
Custom
2. What is your typical privacy setting for photos?
Public
Friends only
Custom
3. What is your typical privacy setting for statuses?
Public
Friends only
Custom

Image Management Index (3 items)

How often do you engage in each of the following behaviors?

For each behavior, chose one of the following answer choices:

(Often, occasionally, sometimes, never)

1. Untag photos of yourself that you feel are inappropriate?
2. Refrain from posing a status or comment that you felt would be inappropriate?
3. Delete comments a friend made on your wall because you thought it was inappropriate?

Friend Selectivity Index (2 items)

1. Who would you accept as a friend?
Anybody
Anybody who attends my school
Friends of friends
People I have met before
Only very close friends and family
Only family
Only close friends
2. How well do you need to know someone before accepting a friend request on Facebook?
Extremely well
Very well
Somewhat well

Not too well
Not well at all

Offline Privacy Protection Index (8 items)

How often do you engage in each of the following activities?

For each behavior, chose one of the following answer choices:

(Often, occasionally, sometimes, never)

1. Refrain from talking about excessive drinking on the phone, unless I am in a private space such as my room, my house, or my car.
2. Use swear words in a public setting where others could possibly overhear. (R)
3. Wear somewhat revealing clothing to work or a job interview. (R)
4. Refrain from talking about sexual experiences on the phone, unless I am in a private space such as my room, my house, or my car.
5. Kiss someone in public. (R)
6. Talk on the phone about excessive drinking when I am in front of my parents. (R)
7. Refrain from talking about drug use, unless I am in a private space such as my room, my house, or my car.
8. Criticize a class or a teacher in a public setting where others could possibly overhear. (R)

Privacy Controls Knowledge (5 items)

How much do you agree or disagree with the following statements?

(Strongly agree, agree, don't know, disagree, strongly disagree)

1. I am unfamiliar with Facebook's privacy settings. (R)
2. I feel comfortable using Facebook's privacy settings.
3. I am unsure of how protective my current privacy settings are. (R)
4. I was aware when Facebook updated its privacy controls in September of 2011.
5. When do you last adjust your privacy settings?
In the last month
In the last 3 months
In the last 6 months
In the last year
In the last two years
In the last three or more years

Big Five Personality Ten-Item Index

How much do you agree or disagree with the following statements?

(strongly disagree, disagree, somewhat disagree, don't know, somewhat agree, agree, strongly agree)

Agreeableness

1. I see myself as sympathetic/warm
2. I see myself as critical/quarrelsome(R)

Conscientiousness

1. I see myself as dependable/self-disciplined
2. I see myself as disorganized/careless (R)

Emotional stability

1. I see myself as calm/emotionally stable
2. I see myself as anxious/easily upset (R)

Extraversion

1. I see myself as extraverted/enthusiastic
2. I see myself as reserved/quiet (R)

Openness to new experience

1. I see myself as open to new experiences/complex
2. I see myself as conventional/uncreative (R)

Appendix E: Complete Survey for College Sample

1. Please select your sex:
 - Male
 - Female

2. What is your grade level?
 - Freshman
 - Sophomore
 - Junior
 - Senior

3. What is your age?
 - 18
 - 19
 - 20
 - 21
 - 22
 - 23
 - 24

4. What is your race?
 - White, Hispanic origin
 - White, Non-Hispanic origin
 - American Indian or Alaska Native
 - Asian or Pacific Islander
 - Black or African American
 - Other

5. Do you have a Facebook account?
 - Yes
 - No

6. How long have you had your Facebook account?
 - 6 months
 - 1 year
 - 2 years
 - 3 years
 - 4 years

- More than 4 years
7. How often do you check your account?
- Less than a few times per month,
 - A few times per month
 - A few times per week
 - Daily
 - More than 3 times per day
 - More than 5 times per day
8. On average, how much time do you spend on Facebook each time you check your account?
- Up to 5 minutes
 - 15 minutes
 - 30 minutes
 - 1 hour
 - More than 1 hour
9. About how many Facebook friends do you have? _____
10. How many of your Facebook friends would you consider to be close friends? _____
11. About how many friends do you hang out with or see on a regular basis? _____
12. Who would you accept as a friend?
- Anybody
 - Anybody in the University of Michigan network
 - Friends of friends
 - People you I have met
 - Only very close friends and family
 - Only family
13. How well do you have to know someone before you will accept them as a friend on Facebook?
- Extremely well
 - Very well
 - Somewhat well
 - Not too well
 - Not well at all

How much do you agree or disagree with the following statements?

(Strongly agree, agree, don't know, disagree, strongly disagree)

13. I am unfamiliar with Facebook's privacy settings.
14. I feel comfortable using Facebook's privacy settings.
15. I am unsure of how protective my current privacy settings are.
16. I was aware when Facebook updated its privacy controls in September of 2011.

17. When do you last adjust your privacy settings?

In the last month

In the last 3 months

In the last 6 months

In the last year

In the last two years

In the last three or more years

About how many of your Facebook friends fall into each one of these groups?

18. Family members _____

19. Past or current employers _____

20. People under 18 _____

21. Past or current teachers or GSIs _____

22. What is your default privacy setting?

- Public
- Friends only
- Custom
- Don't know

a. If Custom setting: Which of the following groups do you show your content.

Check all that apply.

- Close friends
- Parents
- Siblings

- Past or current employers
- People under 18
- Past or current teachers or GSIs

23. What is your typical privacy setting for photos?

- Public
 - Friends only
 - Custom
 - Don't know
- a. If Custom setting: Which of the following groups do you show your content.
Check all that apply.

- Close friends
- Parents
- Siblings
- Past or current employers
- People under 18
- Past or current teachers or GSIs

24. What is your typical privacy setting for statuses?

- Public
 - Friends only
 - Custom
 - Don't know
- a. If Custom setting: Which of the following groups do you show your content.
Check all that apply.

- Close friends
- Parents
- Siblings
- Past or current employers
- People under 18
- Past or current teachers or GSIs

How often do you engage in each of the following behaviors?

For each behavior, chose one of the following answer choices:

- Often
- Occasionally
- Sometimes
- Never

25. Untag photos of yourself that you feel are inappropriate?

26. Refrain from positing a status or comment that you felt would be inappropriate?

27. Delete comments a friend made on your wall because you thought it was inappropriate?

How much do you agree or disagree with the following statements?

For each statement, chose one of the following answer choices:

- Strongly disagree
- Disagree
- Somewhat disagree
- Don't know
- Somewhat agree
- Agree
- Strongly agree

28. I see myself as sympathetic/warm

29. I see myself as critical/quarrelsome

30. I see myself as dependable/self-disciplined

31. I see myself as disorganized/careless

32. I see myself as calm/emotionally stable

33. I see myself as anxious/easily upset

34. I see myself as extraverted/enthusiastic

35. I see myself as reserved/quiet

36. I see myself as open to new experiences/complex

37. I see myself as conventional/uncreative

How often do you do each of the following activities?

For each statement, choose one of the following:

- Often
- Occasionally
- Sometimes
- Never

38. Invite friends over to your house while your parents are home.

39. Invite a past or current employer to a party.

40. Invite a close friend, sibling, or other family member that is under 18 to a party.

41. Sign up for the same discussion section with a close friend.

How often do you engage in each of the following activities?

For each action, chose one of the following:

- Often
- Occasionally
- Sometimes
- Never

42. Talk about drug use with my friends.

43. Talk about excessive drinking with my friends.

44. Talk about sexual experiences with my friends

45. Wear somewhat revealing clothing when I go out to a party or bar with my friends.

46. Criticize class or a teacher with my friends.

47. Use swear words when I talk to my friends.

How often do you engage in each of the following activities?

For each behavior, chose one of the following answer choices:

- Often

- Occasionally
- Sometimes
- Never

48. Refrain from talking about excessive drinking in public.

49. Use swear words in a public.

50. Wear somewhat revealing clothing to work or a job interview.

51. Refrain from talking about sexual experiences in public.

52. Kiss someone in public.

53. Talk to a friend about excessive drinking when I am in front of my parents.

54. Refrain from talking about drug use in public.

55. Refrain from criticizing a class or a teacher in public.

How often do you engage in each of the following activities on Facebook?

For each action, chose one of the following:

- Often
- Occasionally
- Sometimes
- Never

56. Use swear words in a comment or status.

57. Talk about sexual experiences in a comment or status.

58. Post or am tagged in photos wearing revealing clothing.

a. If so, have you ever made one of these photos a profile picture?

- Yes
- No

59. Post or am tagged in photos holding red cups or bottles of beer, wine, or alcohol.

a. If so, have you ever made one of these photos a profile picture?

- Yes
- No

60. Criticize a class, professor or a GSI in a comment or status.

61. Criticize an employer or workplace in a negative way in a comment or status.

62. Talk about excessive drinking in a comment or status.

63. Post or am tagged in photos where I am making out with a friend or significant other.

- a. If so, have you ever made one of these photos a profile picture?
 - Yes
 - No
64. Post or am tagged in photos using drugs.
- a. If so, have you ever made one of these photos a profile picture?
 - Yes
 - No

Appendix F: Complete Survey for Mechanical Turk Sample

1. Please select your sex:
 - Male
 - Female
2. How old are you? _____
3. What is your level of education?
 - Currently in high school
 - Completed high school / GED
 - Currently enrolled at a 2 year college (Associates degree)
 - Currently enrolled at a 4 year college (BA,BS degree)
 - If so, what year are you?
 - Freshman
 - Sophomore
 - Junior
 - Senior
 - Completed a 2 year college degree (Associates)
 - Completed a 4 year college degree (BA,BS)
 - Currently pursuing Masters degree
 - Completed Masters degree
 - Currently pursuing Doctoral degree
 - Completed Doctoral degree
 - Currently pursuing Professional degree (JD, MD)
 - Completed Professional degree (JD, MD)
4. What is your race:
 - American Indian or Alaska Native
 - Asian
 - African American
 - White
 - Other
5. What is your total household income?
 - Less than \$10,000
 - \$10,000-\$19,999
 - \$20,000-\$29,999
 - \$30,000-\$39,999
 - \$40,000-\$49,999
 - \$50,000-\$59,999
 - \$60,000-\$69,999

- \$70,000-\$79,999
 - \$80,000-\$89,999
 - \$90,000-\$99,999
 - \$100,000-\$149,000
 - More than \$150,000
6. Do you have a Facebook account?
- Yes
 - No
7. How long have you had your Facebook account?
- 6 months
 - 1 year
 - 2 years
 - 3 years
 - 4 years
 - More than 4 years
8. How often do you check your account?
- Less than a few times per month,
 - A few times per month
 - A few times per week
 - Daily
 - More than 3 times per day
 - More than 5 times per day
9. On average, how much time do you spend on Facebook each time you check your account?
- Up to 5 minutes
 - 15 minutes
 - 30 minutes
 - 1 hour
 - More than 1 hour
10. About how many Facebook friends do you have? _____
11. How many of your Facebook friends would you consider to be close friends? _____
12. About how many friends do you hang out with or see on a regular basis? _____
13. Who would you accept as a friend?
- Anybody
 - Anybody in the University of Michigan network

- Friends of friends
- People you I have met
- Only very close friends and family
- Only family

14. How well do you have to know someone before you will accept them as a friend on Facebook?

- Extremely well
- Very well
- Somewhat well
- Not too well
- Not well at all

How much do you agree or disagree with the following statements?

(Strongly agree, agree, don't know, disagree, strongly disagree)

14. I am unfamiliar with Facebook's privacy settings.
15. I feel comfortable using Facebook's privacy settings.
16. I am unsure of how protective my current privacy settings are.
17. I was aware when Facebook updated its privacy controls in September of 2011.
18. When do you last adjust your privacy settings?
- In the last month
- In the last 3 months
- In the last 6 months
- In the last year
- In the last two years
- In the last three or more years

About how many of your Facebook friends fall into each one of these groups?

19. Family members _____
20. Past or current employers _____
21. People under 18 _____
22. Past or current teachers _____
23. What is your default privacy setting?
- Public
 - Friends only

- Custom
 - Don't know
- a. If Custom setting: Which of the following groups do you show your content.

Check all that apply.

- Close friends
- Parents
- Siblings
- Past or current employers
- People under 18
- Past or current teachers

24. What is your typical privacy setting for photos?

- Public
- Friends only
- Custom
- Don't know

- a. If Custom setting: Which of the following groups do you show your content.

Check all that apply.

- Close friends
- Parents
- Siblings
- Past or current employers
- People under 18
- Past or current teachers

25. What is your typical privacy setting for statuses?

- Public
- Friends only
- Custom
- Don't know

- a. If Custom setting: Which of the following groups do you show your content.

Check all that apply.

- Close friends
- Parents
- Siblings
- Past or current employers
- People under 18
- Past or current teachers

How often do you engage in each of the following behaviors?

For each behavior, chose one of the following answer choices:

- Often
- Occasionally
- Sometimes
- Never

26. Untag photos of yourself that you feel are inappropriate?

27. Refrain from positing a status or comment that you felt would be inappropriate?

28. Delete comments a friend made on your wall because you thought it was inappropriate?

How much do you agree or disagree with the following statements?

For each statement, chose one of the following answer choices:

- Strongly disagree
- Disagree
- Somewhat disagree
- Don't know
- Somewhat agree
- Agree
- Strongly agree

29. I see myself as sympathetic/warm

30. I see myself as critical/quarrelsome

31. I see myself as dependable/self-disciplined

32. I see myself as disorganized/careless

33. I see myself as calm/emotionally stable

34. I see myself as anxious/easily upset

35. I see myself as extraverted/enthusiastic

36. I see myself as reserved/quiet

37. I see myself as open to new experiences/complex

38. I see myself as conventional/uncreative

How often do you do each of the following activities?

For each statement, choose one of the following:

- Often
- Occasionally
- Sometimes
- Never
- N/A

39. Invite friends over while your kids (if you have children) or your parents are home.

40. Invite a past or current employer to a party or bar.

41. Invite someone who is under 18 to a party with your friends

42. Sign up for a class or seminar with a close friend.

How often do you engage in each of the following activities?

For each action, chose one of the following:

- Often
- Occasionally
- Sometimes
- Never

43. Talk about drug use with my friends.

44. Talk about excessive drinking with my friends.

45. Talk about sexual experiences with my friends

46. Wear somewhat revealing clothing when I go out to a party or bar with my friends.

47. Criticize class or a teacher with my friends.

48. Use swear words when I talk to my friends.

How often do you engage in each of the following activities?

For each behavior, chose one of the following answer choices:

- Often
- Occasionally
- Sometimes
- Never

49. Refrain from talking about excessive drinking in public.

50. Use swear words in a public. (R)

51. Wear somewhat revealing clothing to work or a job interview. (R)
52. Refrain from talking about sexual experiences in public.
53. Kiss someone in public. (R)
54. Talk on the phone about excessive drinking when I am in front of my parents. (R)
55. Refrain from criticizing an employer or workplace in public.
56. Refrain from talking about drug use in public.
57. Refrain from criticizing a teacher or class in public.

How often do you engage in each of the following activities on Facebook?

For each action, chose one of the following:

- Often
- Occasionally
- Sometimes
- Never
- N/A

58. Use swear words in a comment or status.
59. Talk about sexual experiences in a comment or status.
60. Post or am tagged in photos wearing revealing clothing.
 - a. If so, have you ever made one of these photos a profile picture?
 - Yes
 - No
61. Post or am tagged in photos holding red cups or bottles of beer, wine, or alcohol.
 - a. If so, have you ever made one of these photos a profile picture?
 - Yes
 - No
62. Criticize a class or teacher in a comment or status.
63. Criticize an employer or workplace in a comment or status.
64. Talk about excessive drinking in a comment or status.
65. Post or am tagged in photos where I am kissing someone.
 - a. If so, have you ever made one of these photos a profile picture?
 - Yes
 - No
66. Post or am tagged in photos using drugs.
 - a. If so, have you ever made one of these photos a profile picture?

- Yes
- No

Appendix G: An Independent Samples T-Test Comparing the Image Management of Net Geners and Baby Boomers

Group Statistics

Age	N	Mean	Std. Deviation	Std. Error Mean
ImageManagement1 NetGeners	155	.5871	.19911	.01599
BabyBoomers	116	.4623	.20471	.01901

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
ImageManagement1	Equal variances assumed	.082	.775	5.045	269	.000	.12481	.02474	.07610	.17352
	Equal variances not assumed			5.025	244.110	.000	.12481	.02484	.07588	.17374

Appendix H: An Independent Samples T-Test Comparing the Friend Selectivity of Net Geners and Baby Boomers

Group Statistics

Age	N	Mean	Std. Deviation	Std. Error Mean
FriendSelectivity1 Net Geners	154	.5252	.14941	.01204
Baby Boomers	115	.6001	.18264	.01703

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
FriendAcceptance1	Equal variances assumed	3.088	.080	-3.696	267	.000	-.07489	.02026	-.11479	-.03500
	Equal variances not assumed			-3.591	216.184	.000	-.07489	.02086	-.11600	-.03378

Appendix I: An Independent Samples T-Test Comparing the Privacy Controls of Net Geners and Baby Boomers

Group Statistics

Age	N	Mean	Std. Deviation	Std. Error Mean
PrivacyControl1 NetGeners	149	.6801	.19067	.01562
BabyBoomers	104	.6795	.19786	.01940

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
PrivacyControl1	Equal variances assumed	.043	.836	.024	251	.981	.00060	.02474	-.04813	.04934
	Equal variances not assumed			.024	216.498	.981	.00060	.02491	-.04849	.04970

Appendix J: An Independent Samples T-Test Comparing the Privacy Controls Knowledge of Net Geners and Baby Boomers

Group Statistics

Age		N	Mean	Std. Deviation	Std. Error Mean
PrivacyKnowledge	NetGeners	155	.7520	.16613	.01334
	Baby	116	.6998	.19072	.01771
	Boomers				

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
PrivacyKnowledge	Equal variances assumed	1.161	.282	2.402	269	.017	.05220	.02174	.00941	.09500
	Equal variances not assumed			2.354	227.824	.019	.05220	.02217	.00851	.09589

Appendix K: A Paired Samples T-Test Comparing Offline Privacy Protection and Facebook Privacy Controls

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	OfflinePrivacy1	.7728	345	.13165	.00709
	PrivacyControl1	.6831	345	.18576	.01000

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	OfflinePrivacy1 & PrivacyControl1	345	.188	.000

Paired Samples Test

		Paired Differences				t	df	Sig. (2-tailed)	
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference				
					Lower				Upper
Pair 1	OfflinePrivacy1 - PrivacyControl1	.08969	.20647	.01112	.06783	.11156	8.069	344	.000

Appendix L: An Independent Samples T-Test Comparing the Offline Privacy Protection of Net Geners and Baby Boomers

Group Statistics

Age	N	Mean	Std. Deviation	Std. Error Mean
OfflinePrivacy1 NetGeners	151	.7437	.12185	.00992
BabyBoomers	110	.8343	.12564	.01198

Independent Samples Test

		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
OfflinePrivacy1	Equal variances assumed	.088	.767	-5.854	259	.000	-.09060	.01548	-.12107	-.06012
	Equal variances not assumed			-5.826	230.806	.000	-.09060	.01555	-.12124	-.05996