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

Katherine Bies

Katherine Bies graduated from the University of Michigan (Ann Arbor) in 2012 with a Bachelor of Arts in Communication Studies. This policy research paper is an adaption from her senior honors thesis, which was awarded the Virginia L. Voss Memorial Award for excellence in writing. She is currently a Teach for America corps member at Brownsville Ascend Charter School in Brooklyn, New York.

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 privacy protection used offline; 3) the use of online privacy protection varies by generational cohort. These results suggest that action should be taken to legally afford social media users the same legal protections that are guaranteed offline.

Introduction

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 innovative technologies such as the telephone, recording devices, and cellphones come at a potential cost to personal privacy (Agre and Rotenberg 2007; Moore 1984; Caloyannides 2003; Ware 1986; Wolinksy and Sylvester 1992). The Fourth Amendment, which guards against unreasonable searches and seizures, has traditionally served as the constitutional safeguard of personal privacy. As technological innovations have made it easier to
obtain and share personal information, 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.

The Internet has facilitated the collection and sharing of personal information on an even greater scale (Caloyannides 2003). Social media sites, such as Facebook, LinkedIn, and Twitter, are communication platforms used by hundreds of millions of people to share personal information online. Many users limit access to personal information with privacy controls developed by these sites; however, the question remains: does this action guarantee an expectation of privacy on social media? This study explores this question by comparing privacy protection on social media sites with the offline expectation of privacy established by the Supreme Court.

Background

An Overview of Facebook

Facebook, launched in 2004, allows a registered user to create an online profile and to add other users as friends. Facebook invites users to disclose private information by posting information on their profile, sharing photos, exchanging “wall posts,” creating “status updates,” and sending “Facebook messages.”

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 (“Facebook Statistics” 2011). While 48 percent of its users are 18 to 34 year olds, the 35 and older cohort, currently 30 percent of the user base, is growing steadily (“Facebook Statistics” 2011). Also, Facebook provides both opportunities for sharing private information and privacy controls that are similar to other social media sites like Instagram, Twitter, and LinkedIn. The average Facebook user spends more than 55 minutes on Facebook per day (“Facebook Facts” 2010). Facebook’s ubiquity may have substantial implications for the current social privacy norms upon which developments in online privacy law will be based.

Privacy Risks on Social Media: The Facebook Case

Facebook has obvious social benefits, as well as risks, to personal privacy. The site has played an important role in developing and maintaining
relationships with friends by allowing users to interact with a large social network (Debatin et al. 2009; Ellison et al. 2007). The facilitation of friendship networks is positively correlated with the maintenance and creation of social capital (Ellison et al. 2007).

However, Facebook users do not always have control over, or even knowledge of, the many individuals with access to their personal information. Privacy breaches may bring unintended negative consequences. Facebook users have faced scrutiny from potential employers and law enforcement based on the material they post on social media— even when protected by privacy settings (Smith and Kidder 2010; Stone 2006; Kornblum and Marklein 2006). Employers admit using Facebook for recruiting and assessing applicants (Smith and Kidder 2010; Zeidner 2007). Police officers receive training about Facebook as a way to investigate and reduce crime (“The Fuzz” 2006). The FBI recently released an advertisement looking for companies with the capability to build a data-mining application for social media sites, including Facebook (Giles 2012). However, Facebook’s continued popularity proves that its benefits override the potential loss and even invasion of privacy (Debatin et al. 2009).

The Development of Privacy Law

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 Supreme Court’s interpretation of the Fourth Amendment has expanded from solely protecting a citizen’s right against government intrusion of physical property to encompass other aspects of personal privacy. The contemporary 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 future Supreme Court Justices Warren and Brandeis. Concerned that “modern” media technologies such as instant photographs and tabloid newspapers were intruding into the private lives of American citizens, Warren and Brandeis (1890) argued that individuals have a “right to be let alone” that extends beyond a person’s right to physical property to include his “thoughts, sentiments, and emotions.”
For the first half of the 20th century, privacy was limited to the physical space of the home. The 1928 case Olmstead v. United States, 277 U.S. 438, allowed law enforcement to wire-tap phone conversations if they did not physically enter the suspect’s house. Justice Brandeis, dissenting in the Olmstead case, argued that the court must “meet modern conditions” by expanding the interpretation of the Fourth Amendment to include the capabilities of new technologies that the Founders could not have predicted when writing the constitution, 277 U. S. 465, (1928).

The Supreme Court expanded its interpretation again with the development of the public telephone booth. In Katz v. United States, the court ruled 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). Justice Stewart, writing for the majority, argued that the Fourth Amendment protects against intrusion in a public setting if the individual takes steps to create a private space such as “shut[ting] the door” to a telephone booth, 389 U.S. 352, (1967). Justice Harlan, writing a concurring opinion, further refined the concept of a “reasonable expectation of privacy” in a two-part rule: first, an individual must exhibit an expectation of privacy and secondly, society must acknowledge this expectation of privacy as reasonable.

Legal scholars have recommended that policy makers further expand the concept of personal privacy to safeguard against privacy intrusions on social media sites (Beckstrom 2008; Hodge 2006). Junichi Semitsu (2011) analogizes conversations on Facebook to the telephone booth conversation recognized by the Supreme Court in Katz to warrant an expectation of privacy. While he acknowledges that Facebook communications can be broadcast to a multitude of Facebook friends rather than one listener, Semitsu argues that the Supreme Court never suggested that additional message recipients necessarily defeats an expectation of privacy (Semitsu 2011). Applying the Katz decision to Facebook, Semitsu (2011) suggests that courts today should consider Facebook as the “twenty-first century equivalent of a phone booth.” An individual who uses Facebook privacy controls makes the equivalent action of shutting the telephone booth door and therefore has a reasonable expectation of privacy.

These recommendations are based solely on normative argument, however. While important in developing the legal theory behind court
decisions, empirical claims measuring the current cultural conception of privacy would add weight to any decision regarding a concept traditionally rooted in social practices (Solove 2002).

**Empirical Research Regarding Facebook Privacy**

Benson (2009) conducted open interviews with college students in order to determine the extent to which they share personal information both online and offline. Expanding upon Benson’s approach, I compare privacy practices on Facebook and offline. By comparing the offline and online behaviors of Facebook users, I hope to add empirical clarity to Semitsu’s application of Katz to Facebook, and most importantly, to the over-arching legal debate and question: do Facebook users have a reasonable expectation of privacy on Facebook?

**Hypotheses**

**Self-Revelation**

In Benson’s study, self-revelation is the act of disclosing private information. Benson identified several categories of Facebook content considered inappropriate to share in a public setting, including: excessive drug and alcohol use, name calling, and political comments (Benson 2009). Benson found that self-revelation did not vary significantly from online to offline for college students (Benson 2009). However, older users may behave differently than younger users.

Tapscott (2009) predicts that generational cohort is an important determining factor in an individual’s attitude towards and experience with online technologies. He defines the Net Generation as individuals who are currently aged 29 and younger and have grown up with the Internet (Tapscott 2009). Because of their online experiences, Palfry and Gasser (2008) suggest that these individuals relate information and experience friendship differently from their parents. To test these theories, I conduct a comparison of self-revelation across three generational cohorts, including the Net Generation, a middle cohort (26-35), and an older cohort (36 and older). Based on Benson’s findings, I predict that:

**H1:** The Net Generation will engage in more consistent self-revelation on Facebook and offline than older generations.
Correlates of Privacy Protection

Before I compare privacy practices on Facebook and offline, I first determine to what extent privacy protection is used on Facebook. Privacy protection refers to actions that limit access to private information. Facebook privacy controls allow a user to limit his or her content to specified groups of users. A variety of factors may influence the extent to which Facebook privacy controls are used.

The Net Generation. While generational cohort has an important influence on online behavioral norms, discussion on this topic has mostly focused on self-revelation (Tapscott 2009; Palfry and Gasser 2008). Early studies suggest the Net Generation may differ from older generations in its online privacy protection. Palfry and Gasser (2008) argue that the Net Generation is more likely than older generations to feel that sharing information online is the norm. The Net Generation may also feel less compelled to protect information. Expanding on Palfry & Gasser’s theory, I predict that:

H2: The Net Generation employs less stringent privacy controls on Facebook than older generations.

Privacy Controls Knowledge. A Facebook user’s familiarity with privacy controls may also influence the stringency of his or her privacy protection. In the last six months, Facebook has updated its privacy controls three times. If users are not current 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 23 percent correctly stated their settings. Based on Butler et al.’s findings, I predict that:

H3: Users with greater privacy controls knowledge will employ more stringent privacy protection on Facebook.

Demographic Factors. Previous psychological research has found gender and personality attributes to influence online privacy concerns. Lewis et al.(2009) discovered that females employ more stringent privacy settings than males on Facebook.

Junglas et al. (2008) examined the relationship between the Big Five personality variables and a concern for online privacy and found only three of the five attributes correlate significantly: agreeableness, conscientiousness,
and openness. Highly agreeable individuals had lower privacy concerns than non-agreeable individuals. Both conscientious individuals and individuals open to new experiences had a higher concern for privacy than non-conscientious or non-open people.

**A Comparison of Offline and Online Privacy Protection**

Legal scholars have argued that the use of privacy controls is the online equivalent to various forms of legally recognized offline privacy protection (Semitsu 2011; Beckstrom 2008; Hodge 2006). I test this argument by statistically comparing the offline and online privacy protection of Facebook users. Do Facebook users take similar steps to protect their Facebook content as they do to protect private information offline? If Facebook privacy protection and offline privacy protection are similar, legal scholars are more supported in their argument that Facebook users exhibit an expectation of privacy. Therefore, I predict:

\[
H4: \text{Facebook users who engage in more stringent privacy protection offline will also engage in more stringent privacy protection on Facebook.}
\]

The second part of the Katz test is whether or not society will recognize this expectation of privacy as reasonable. If only certain groups of Facebook users act in a way that affords an expectation of privacy online, then this expectation may not be reasonable by society’s standards.

**Moderating Effect of Generational Cohort.** Based on discussions above, I predict that generational cohort influences the relationship between online and offline privacy protection. Benson (2009) found that the Net Generation consistently reveals private information online and offline. Expanding on this finding, I predict that the Net Generation will also be consistent in its online and offline privacy protection. 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 (Tapscott 2009; Palfry and Gasser 2008). Therefore, I predict:

\[
H5: \text{The Net Generation will engage in more consistent privacy protection on Facebook and offline than older generations.}
\]
Data and Methods

Sample

I created and administered a survey to measure the five hypotheses. The non-representative sample was composed of 381 Facebook users recruited online using Amazon Mechanical Turk which allows registered “workers” to browse for and complete computer-based tasks for compensation. All respondents were required to be United States residents older than 17 years of age and to have a Facebook account in order to complete the survey.

Of the Mechanical Turk respondents, 194 (51 percent) were male and 187 (49 percent) were female. Forty-nine percent of participants were non-Hispanic Caucasian, 25 percent were Asian, and 16 percent were Hispanic. Fourteen percent of respondents had received a high school diploma as their highest level of education, 21 percent were currently enrolled in college, 38 percent had received a college degree and 26 percent were currently pursuing or had completed a higher degree. Sixty-four percent of respondents had a Facebook profile for two years or more. Half of the respondents check Facebook every day.

This sample is composed of three pre-determined age groups (18-25, 26-35, and 36 and older) based on Tapscott’s generational cohort definitions and Facebook’s demographic make up (Tapscott 2009; “Facebook Statistics” 2011). In order to best compare the three generational cohorts, each one needed a relatively equal percentage of survey respondents: the Net Generation cohort had 155 respondents (41 percent), the middle (26-35) cohort had 110 respondents (29 percent), and the oldest (36 and older) cohort had 116 respondents (30 percent). The mean age of the sample was 32 years (Standard deviation = 11.55; Range = 18-77).

Variables

The survey instrument consisted of 66 questions to measure the central constructs developed in the hypotheses. The research focuses on two comparisons: (1) online self-revelation to offline self-revelation and (2) online privacy protection to offline privacy protection. Variables shown in previous studies to be related to privacy concerns were also measured as controls: privacy controls knowledge, personality traits, and demographic variables such as gender and generational cohort.
Online and Offline Comparisons. Online self-revelation measures the extent to which the respondent reveals private information on Facebook. A thirteen-item index was created based on Benson’s findings about information that Facebook users found socially inappropriate (Benson 2009). Respondents rated statements on a four-point scale with 1 as “never,” 2 as “sometimes,” 3 as “occasionally,” and 4 as “often.” A higher score signifies greater self-revelation (Cronbach’s α = .84).

Offline self-revelation was measured by analogizing interactions with Facebook friends to offline interactions with friends. To keep this measure consistent with the online self-revelation index, selected online items were converted into a six-item offline self-revelation index. Raw scores were summed, with higher values indicating greater self-revelation (Cronbach’s α = .82).

Online privacy protection measures the extent to which a Facebook user applies privacy settings to limit the audience who is able to see a user’s content online. This index is made up of three questions about the use of Facebook’s privacy settings: “public,” “friends only,” and “custom.” The “custom” privacy control goes a step further in privatizing content because it not only limits content from the public view, but also from the view of specific Facebook friends. Responses are scored from 1 as “public” to 3 as “custom” with higher values representing more stringent privacy controls (Cronbach’s α = .87).

Offline privacy protection measures behaviors that limit to whom a respondent reveals personal information. The items were built in two parts: (1) private information revealed, based on the self-revelation index, and (2) limiting who this information is being revealed to, based on the Katz analogy. Respondents rated statements on a four-point scale from 1 as “never” to 4 as “often.” The eight-item index was moderately reliable (Cronbach’s α = .71). The internal consistency of this measure is not as high as the previous measures, but it shows acceptable reliability. The reliability was not improved by removing any of the items.

Control Variables. Privacy controls knowledge is a five-item index comprised of questions about respondents’ knowledge of and comfort with Facebook’s privacy controls based on a similar study by Butler et al. (2011). Four of the five items were aggregated with higher scores demonstrating
greater knowledge of privacy controls (Cronbach’s $\alpha = .68$). One item was removed in order to improve internal consistency.

The Big Five personality traits were assessed using a ten-item scale developed by Gosling et al. (2003) and validated by Muck et al. (2007). Responses for each item were scored with a seven-point Likert scale, ranging from 1 as “strongly disagree” to 7 as “strongly agree.” Demographic variables of gender, age, race, income, and current education level were also measured.

**Results**

**Self-Revelation**

H1 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 1). The Net Generation exhibited a strong, positive, and significant correlation between offline and online privacy protection. I fail to reject H1. Facebook users in the Net Generation who are more self-revelatory offline are also more self-revelatory online. Older generations exhibited a much smaller, and even slightly negative, association between self-revelation offline and online, which means that older generations who share more information offline actually share less information online.

**Correlates of Privacy Protection**

The average Facebook user was found to use privacy settings to limit content to Facebook friends. To determine if this finding was consistent for the generational distribution as a whole, a regression was performed to control for demographic characteristics associated with predicting privacy protection (see Table 1). The Net Generation and high privacy controls knowledge were found to have a significant, positive association with privacy protection. Individuals with greater conscientiousness, a higher education level, and females were also found to use more stringent privacy settings. The other measured variables were not found to be significant predictors of privacy protection.
Generational Cohort. H2 predicted the Net Generation to have less stringent privacy controls than older generations. However, the older cohorts both had small, negative associations with privacy protection (see Table 1; the oldest cohorts association is marginally significant at $p < .10$). This demonstrates that the Net Generation, the excluded group in this regression, exhibited the most stringent use of privacy controls of any generation as a whole. I reject H2. The Net Generation was more likely than older generations to use the more stringent “custom” Facebook privacy control. Possible explanations of this phenomenon will be explained in the Discussion.

Privacy Controls Knowledge. Privacy controls knowledge was predicted to positively influence the use of Facebook privacy controls in H3. The Net Generation was found to not only use the most stringent privacy settings, but also to be most knowledgeable about privacy controls (see Table 1 and Figure 2). This difference between the privacy controls

---

1 Scale of 0-1, with 1 being highest amount of self-revelation. High self-revelation respondents fall in the top third and low self-revelation respondents fall in the bottom third.
### Table 1: A Regression Analysis of the Correlates of Online Privacy Protection

<table>
<thead>
<tr>
<th>Predicting Variables</th>
<th>Online Privacy Protection (B)</th>
<th>Standard Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>White</td>
<td>0.04</td>
<td>0.04</td>
</tr>
<tr>
<td>Asian</td>
<td>0.01</td>
<td>0.04</td>
</tr>
<tr>
<td>Black</td>
<td>-0.02</td>
<td>0.07</td>
</tr>
<tr>
<td>Female</td>
<td>0.04^</td>
<td>0.02</td>
</tr>
<tr>
<td>Income</td>
<td>0.04</td>
<td>0.04</td>
</tr>
<tr>
<td>Education</td>
<td>0.10^</td>
<td>0.06</td>
</tr>
<tr>
<td>Agreeableness</td>
<td>0.04</td>
<td>0.07</td>
</tr>
<tr>
<td>Conscientiousness</td>
<td>0.14*</td>
<td>0.07</td>
</tr>
<tr>
<td>Emotional Stability</td>
<td>-0.11</td>
<td>0.06</td>
</tr>
<tr>
<td>Extraversion</td>
<td>-0.04</td>
<td>0.05</td>
</tr>
<tr>
<td>Openness</td>
<td>0.09</td>
<td>0.07</td>
</tr>
<tr>
<td>26-35 cohort</td>
<td>-0.02</td>
<td>0.03</td>
</tr>
<tr>
<td>36 and older cohort</td>
<td>-0.05^</td>
<td>0.03</td>
</tr>
<tr>
<td>Privacy Controls Knowledge</td>
<td>0.21**</td>
<td>0.08</td>
</tr>
</tbody>
</table>

N = 348, R² = 0.109

*significant at p < .05, **significant at p < .01, ^significant at p < .10

### Figure 2: A Comparison of Privacy Controls Knowledge Means by Generational Cohort

![Bar chart showing privacy controls knowledge means by generational cohort](chart.png)

Average Amount of Knowledge (Scale 0-1)
knowledge of the Net Generation and the oldest generation was found to be statistically significant at p<.05 after performing an Independent Samples T-Test. I fail to reject H3.

**A Comparison of Offline and Online Privacy Protection**

To gauge the similarity of offline and online behaviors, a regression was performed to determine if a relationship still exists after controlling for a large number of demographic predictors. Offline privacy protection had a strong, positive, and significant correlation (.23 at p<.01) with Facebook privacy protection (see Table 3). I fail to reject H4. These results suggest that the use of Facebook controls is similar to steps taken to protect privacy offline.

**Moderating Effect of Generational Cohort.** H5 predicted the Net Generation to engage in more consistent privacy protection online and offline than older generations. Table 3 shows generational cohort is a moderating variable for the online and offline privacy protection comparisons even when controlled for alternative predicting variables. An interaction was calculated to determine the distinct relationship between privacy protection and generational cohort (see Figure 2). The oldest cohort had a large, significant, and positive correlation (at p < .05) between offline and online privacy protection. The Net Generation did not have a significant correlation. I reject H5.

The Net Generation engages in more stringent privacy protection online regardless of its offline privacy protection. Offline and online privacy protection is actually more consistent for older generations. This suggests that the Net Generation is more concerned about online privacy than older generations. Possible explanations will be discussed later.

**Discussion**

**Do Facebook users exhibit an expectation to privacy?**

The overall pattern of results from my survey of 381 adults around the country suggests that the first Katz criterion has been met: Facebook users exhibit an expectation of privacy. First, the median Facebook user implements the “Friend” privacy control to restrict his or her content from public view. Secondly, Facebook users, regardless of generational cohort,
Table 2: A Regression Analysis of the Relationship between Online and Offline Privacy Protection

<table>
<thead>
<tr>
<th>Moderating Variables</th>
<th>Privacy Controls (B)</th>
<th>Standard Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline Privacy Protection</td>
<td>0.23**</td>
<td>0.08</td>
</tr>
<tr>
<td>White</td>
<td>0.06</td>
<td>0.04</td>
</tr>
<tr>
<td>Asian</td>
<td>0.02</td>
<td>0.04</td>
</tr>
<tr>
<td>Black</td>
<td>-0.02</td>
<td>0.07</td>
</tr>
<tr>
<td>Female</td>
<td>0.04*</td>
<td>0.02</td>
</tr>
<tr>
<td>Agreeableness</td>
<td>-0.01</td>
<td>0.07</td>
</tr>
<tr>
<td>Conscientiousness</td>
<td>0.14*</td>
<td>0.07</td>
</tr>
<tr>
<td>Emotional Stability</td>
<td>-0.1</td>
<td>0.06</td>
</tr>
<tr>
<td>Extraversion</td>
<td>-0.04</td>
<td>0.05</td>
</tr>
<tr>
<td>Openness</td>
<td>0.13^</td>
<td>0.07</td>
</tr>
<tr>
<td>Income</td>
<td>0.03</td>
<td>0.04</td>
</tr>
<tr>
<td>Current Education</td>
<td>0.06</td>
<td>0.06</td>
</tr>
<tr>
<td>26-35 cohort</td>
<td>-0.02</td>
<td>0.02</td>
</tr>
<tr>
<td>36+ cohort</td>
<td>-0.06*</td>
<td>0.03</td>
</tr>
<tr>
<td>N</td>
<td>339</td>
<td></td>
</tr>
<tr>
<td>R²</td>
<td>0.118</td>
<td></td>
</tr>
</tbody>
</table>

*significant at p<.05, **significant at p<.01, ^significant at p<.10

Figure 3: The Relationship of Offline and Online Privacy Protection by Generational Cohort²

² Scale of 0-1, with 1 being highest stringency of privacy protection. High stringency respondents are in the top third and low stringency respondents are in the bottom third.
were found to engage in online privacy protection that is similar to offline privacy protection. These results support Semitsu’s suggestion that hiding Facebook content behind a protective cyberwall is analogous to the Katz example of concealing a private telephone conversation behind a telephone booth wall (Semitsu 2011).

In follow-up interviews with a sub-sample of survey respondents, 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.” By using privacy controls, it appears Facebook users are defining a privacy boundary on Facebook.

Is this expectation reasonable?

Results suggest that generational cohort has an important influence on both the use of self-revelation and privacy protection on Facebook. The Net Generation is more likely than older generations to use the “Custom” setting. Survey results and follow-up interviews reveal why the Net Generation is more likely than older generations to take this extra step to protect their privacy.

Since the Net Generation shares more private information on Facebook, these individuals may have a greater desire to protect their content. Survey data found that the Net Generation reveals more personal information and is more knowledgeable about Facebook privacy settings than older generations. The Net Generation’s greater concern with privacy may be the reason these individuals are savvier users of “Custom” controls. For example, Christina, age 20, explained, “I use the custom privacy setting a lot because some of my Facebook friends are family members… If I’m using profanity or something I don’t want my daddy to see, I make sure to customize him out.” On the other hand, older generations may not take the time to use more stringent settings, because they do not need to. Joyce, age 42 explained, “I don’t take the time to learn about privacy controls because I don’t share information that I’m concerned about protecting.” While this study limited its research to whether or not Facebook users implement “Custom” privacy settings, further research could focus on why “Custom”
settings are used and which Facebook friends are customized in or out by Facebook users.

Another explanation is that the Net Generation, having grown up with the Internet and social media sites, has established online behavioral norms and an expectation of which behaviors on Facebook guarantee a sense of privacy (Tapscott 2009; Palfry and Gasser 2008). 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 (Tapscott 2009; Palfry and Gasser 2008). Since results show the online and offline privacy protection of older generations to be similar, older generations may be applying offline privacy norms as they navigate privacy boundaries in cyberspace rather than taking cues from the Net Generation.

Because the Net Generation varies significantly from older generations in its online behavior, it is difficult to say that all generations will currently agree on a reasonable expectation of privacy on social media. While it appears that a privacy boundary has been negotiated online, society may not have reached a definitive consensus on whether or not this affords a reasonable expectation of privacy.

Summary of Limitations

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 action. A large sample was used, but it was not a representative one. Since survey respondents were recruited online, these individuals are more tech-savvy than the average user. The high correlation between knowledge of privacy controls and the use of stringent controls may not actually be reflective of the larger public. The fact that respondents self-selected to complete the survey for payment could also bias results.

Another limitation is that a causal direction between online and offline privacy protection cannot be determined from the results. Further research on this question with an experimental design could attempt to definitively determine the directionality of this relationship. It should be noted, however, that in some Supreme Court cases, such as *Katz*, it has been enough for legal argument to analogize between two actions in order...
to guarantee an expectation of privacy; for example, a traditional behavior and a behavior made possible by a new technology. Therefore, it may be sufficient to say that these offline and online privacy protections are similar in order to determine that an expectation of privacy exists on Facebook.

Another limitation is that new measures were used. Although reliable, these measures may not be valid. I attempt to analogize interactions and behaviors on cyberspace with offline interactions and behaviors. Since the development of the Internet, 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 cyberspace and offline that make it very difficult to develop these analogies.

Policy Considerations and Further Research

This study suggests that social media users have negotiated a privacy boundary on Facebook by using privacy controls. However, this sense of privacy, if not legally recognized, may not be realized. Even though results suggest that Facebook users take similar steps to protect their online and offline privacy, regardless of generational cohort, 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 style standard that protects privacy both online and offline.

Justice Alito, in a case concerning the use of GPS tracking devices to monitor vehicles, wrote that the Katz test should be applied to a society that has a “well-developed and stable set of privacy expectations” United States v. Jones, 565 U.S., (2012:10). 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 online behaviors across 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.

There are many other questions that should be considered before policy is enacted. Further research could better determine why and in what situations “Custom” controls are used on Facebook. Also, privacy expectations may differ between Facebook and other social media sites such as Twitter and Instagram. Lastly, an important consideration in this
discussion is the fact that social media sites create privacy policies to which users must agree and adhere. Does agreeing to a privacy policy inherently alter a user’s expectation of privacy?

Recent developments in privacy policy regarding social media sites offer clues to the direction which privacy law is headed. 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). Facebook has also recently released statements warning employers against accessing a job applicant’s private content as a privacy violation (Duncan 2012). 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 Stored Communications Act (SCA), Crispin v. Christian Audigier Inc, 717 F. Supp. 2d 991 (2010). The SCA, 18 U.S.C. §§ 2701, is a legislative initiative that was passed to limit the ability of third-party Internet service providers to reveal information to government and non-government entities. This ruling follows a recent Supreme Court decision, 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 the user’s knowledge. In general, these policy changes have favored greater privacy protections on social media sites.

With these policy changes, social media sites are increasingly being guaranteed the same legal protections offered on other communication platforms. While some may argue that social media users should simply reveal less information online, this argument does not take into account changing behavioral norms. The Net Generation varies significantly from older generations in both self-revelation and privacy practices on social media sites. Instead of attempting to change these established behavioral norms on the Internet, policymakers should continue to protect and more concretely define the already established privacy boundary on social media sites.

References Cited


Brad Stone, “Web of Risks: Students adore social-networking sites like Facebook, but indiscreet postings can mean really big trouble,” Newsweek, August 21, 2006, 76.


Janet Kornblum and Mary Beth Marklein, “What you say online could haunt you; Schools, employers scrutinize social websites such as MySpace and Facebook,” *USA Today*, March 9, 2006, http://www.usatoday.com/educate/college/firstyear/articles/20060319.html.


Olmstead vs. United States, 277 U.S. 438 (1928).


