JOURNAL OF COMPUTER-MEDIATED COMMUNICATION

Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences

Bernhard Debatin, Jennette P. Lovejoy

E.W. Scripps School of Journalism, Ohio University

Ann-Kathrin Horn, M.A.

Institut für Kommunikationswissenschaft, Leipzig University (Germany)

Brittany N. Hughes

Honors Tutorial College/E.W. Scripps School of Journalism, Ohio University

This article investigates Facebook users' awareness of privacy issues and perceived benefits and risks of utilizing Facebook. Research found that Facebook is deeply integrated in users' daily lives through specific routines and rituals. Users claimed to understand privacy issues, yet reported uploading large amounts of personal information. Risks to privacy invasion were ascribed more to others than to the self. However, users reporting privacy invasion were more likely to change privacy settings than those merely hearing about others' privacy invasions. Results suggest that this lax attitude may be based on a combination of high gratification, usage patterns, and a psychological mechanism similar to third-person effect. Safer use of social network services would thus require changes in user attitude.

doi:10.1111/j.1083-6101.2009.01494.x

Introduction

Student life without Facebook is almost unthinkable. Since its inception in 2004, this popular social network service has quickly become both a basic tool for and a mirror of social interaction, personal identity, and network building among students. Social network sites deeply penetrate their users' everyday life and, as pervasive technology, tend to become invisible once they are widely adopted, ubiquitous, and taken for granted (Luedtke, 2003, para 1). Pervasive technology often leads to unintended consequences, such as threats to privacy and changes in the relationship between public and private sphere. These issues have been studied with respect to a variety of Internet contexts and applications (Berkman & Shumway, 2003; Cocking & Matthews, 2000; Hamelink, 2000; Hinman, 2005; Iachello & Hong, 2007; McKenna & Bargh, 2000; Pankoke-Babatz & Jeffrey, 2002; Spinello, 2005; Tavani & Grodzinsky, 2002; Weinberger, 2005). Specific privacy concerns of online social networking

include inadvertent disclosure of personal information, damaged reputation due to rumors and gossip, unwanted contact and harassment or stalking, surveillance-like structures due to backtracking functions, use of personal data by third-parties, and hacking and identity theft (boyd & Ellison, 2008). Coupled with a rise in privacy concerns is the call to increase our understanding of the attitudes and behaviors toward "privacy-affecting systems" (Iachello & Hong, 2007, p. 100).

This paper investigates privacy violations on Facebook and how users understand the potential threat to their privacy. In particular, it explores Facebook users' awareness of privacy issues, their coping strategies, their experiences, and their meaning-making processes. To this end, we will first take a look at research on Facebook's privacy flaws and at existing studies of user behavior and privacy; thereafter, we will lay out our conceptual background and hypotheses, and present findings from our both quantitative and qualitative empirical research. Finally, we will draw some conclusions from our research.

Literature Review

Privacy and Facebook: The Visible and the Invisible

The privacy concerns delineated above are confirmed by several reports and studies on Facebook. In a report on 23 Internet service companies, the watchdog organization Privacy International charged Facebook with severe privacy flaws and put it in the second lowest category for "substantial and comprehensive privacy threats" ("A Race to the Bottom," 2007). Only Google scored worse; Facebook tied with six other companies. This rating was based on concerns about data matching, data mining, transfers to other companies, and in particular Facebook's curious policy that it "may also collect information about [its users] other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service" ("Facebook Principles," 2007, Information We Collect section, para. 8).

Already in 2005, Jones and Soltren identified serious flaws in Facebook's set-up that would facilitate privacy breaches and data mining. At the time, nearly 2 years after Facebook's inception, users' passwords were still being sent without encryption, and thus could be easily intercepted by a third party (Jones & Soltren, 2005). This has since been corrected. A simple algorithm could also be used to download all public profiles at a school, since Facebook used predictable URLs for profile pages (Jones & Soltren, 2005). The authors also noted that Facebook gathered information about its users from other sources unless the user specifically opted out. As of September 2007, the opt-out choice was no longer available but the data collection policy was still in force ("Facebook Principles," 2007).

Even the most lauded privacy feature of Facebook, the ability to restrict one's profile to be viewed by friends only, failed for the first 3 years of its existence: Information posted on restricted profiles showed up in searches unless a user chose to opt-out his or her profile from searches (Jones & Soltren, 2005). This glitch was fixed in late June 2007, but only after a technology blogger made the loophole

public and contacted Facebook (Singel, 2007). Recent attempts to make the profile restrictions more user-friendly and comprehensive seem mostly PR-driven and still include serious flaws (Soghoian, 2008a).

In September 2006, Facebook introduced the "News Feed," which tracks and displays the online activities of a user's friends, such as uploading pictures, befriending new people, writing on someone's wall, etc. Although none of the individual actions were private, their aggregated public display on the start pages of all friends outraged Facebook users, who felt exposed and deprived of their sense of control over their information (boyd, 2008). Protest groups formed on Facebook, among them the 700,000-member group "Students Against Facebook News Feed" (Romano, 2006, para. 1). Subsequently, Facebook introduced privacy controls that allowed users to determine what was shown on the news feed and to whom.

The implementation of a platform for programs created by third-party developers in summer 2007 and the ensuing flood of applications that track user behaviors and/or make information from personal profiles available for targeted advertising do not inspire trust in Facebook's privacy policy (Schonfeld, 2008; Soghoian, 2008b). Most notably, the Facebook Ads platform has raised serious questions. In an attempt to capitalize on social trust and taste, Facebook's "Beacon" online ad system tracks user behavior, such as online shopping. Initially information was broadcasted to users' friends. This led to angry protests in November 2007, and the formation of a Facebook group called "Petition: Facebook, Stop Invading My Privacy!" that gained over 70,000 members within its first two weeks. Facebook responded by introducing a feature that allowed users to opt out of the broadcasting, yet Beacon continues to collect data "on members' activities on third-party sites that participate in Beacon even if the users are logged off from Facebook and have declined having their activities broadcast to their Facebook friends" (Perez, 2007).

Additional concerns have been raised about links between Facebook and its use by government agencies such as the police or the Central Intelligence Agency. In a rather benign example, a police officer resorted to searching Facebook after witnessing a case of public urination outside a fraternity house at University of Illinois at Urbana-Champaign and the only other witness on the scene claimed not to know the lawbreaker. Once on Facebook, the officer searched the man's friend list and the lawbreaker he was looking for. The first man received a $145 ticket for public urination; the other received a $195 ticket for obstructing justice (Dawson, 2007). Additionally, the Patriot Act allows state agencies to bypass privacy settings on Facebook in order to look up potential employees (NACE Spotlight Online, 2006). An online presentation "Does what happens in the Facebook stay in the Facebook?" (2007) points out a number of connections between various Facebook investors and In-Q-Tel, the not-for-profit venture capital firm funded by the CIA to invest in technology companies for the CIA's information technology needs. The chief privacy officer of Facebook, Chris Kelly, accused the video of "strange interpretations of our policy" and "illogical connections" but did not substantially rebut the allegations (Kelly, 2007).

Further criticism is based on the fact that third parties can use Facebook for data mining, phishing, and other malicious purposes. Creating digital dossiers of college students containing detailed personal information would be a relatively simple task—and a clever data thief could even deduce social security numbers (which are often based on 5-digit ZIP codes, gender, and date of birth) from the information posted on almost half the users' profiles (Gross & Acquisti, 2005). Social networks are also ideal for mining information about relationships or common interests in groups, which can be exploited for phishing. For example, Jagatic, Johnson, Jakobsson, and Menczer (2005) launched a phishing experiment at Indiana University on selected college students, using social network sites to get information about students' friends. The experiment had an alarmingly high 72 percent success rate within the social network as opposed to 16 percent within the control group. The authors add that other phishing experiments by different researchers showed similar results, "We must conclude that the social context of the attack leads people to overlook important clues, lowering their guard and making themselves significantly more vulnerable" (Jagatic et al., 2005, p. 5). A high level of vulnerability is also engendered by the fact that many users post their address and class schedule, thus making it easy for potential stalkers to track them down (Acquisti & Gross 2006; Jones & Soltren 2005). Manipulating user pictures, setting up fake user profiles, and publicizing embarrassing private information to harass individuals are other frequently reported forms of malicious mischief on Facebook (Kessler, 2007; Maher, 2007; "Privacy Pilfered," 2007; Stehr, 2006).

While Facebook's privacy flaws are well documented and have made it into the news media, relatively little research is available on how exactly these problems play out in the social world of Facebook users and how much users know and care about these issues. In their small-sample study on Facebook users' awareness of privacy, Govani and Pashley (2005) found that more than 80 percent of participants knew about the privacy settings, yet only 40 percent actually made use of them. More than 60 percent of the users' profiles contained specific personal information such as date of birth, hometown, interests, relationship status, and a picture.

The study by Jones and Soltren (2005) showed that 74 percent of the users were aware of the privacy options in Facebook, yet only 62 percent actually used them. At the same time, users willingly post large amounts of personal information—Jones and Soltren found that over 70 percent posted demographic data, such as age, gender, location, and their interests—and demonstrate disregard for both the privacy settings and Facebook's privacy policy and terms of service. Eighty-nine percent admitted that they had never read the privacy policy and 91 percent were not familiar with the terms of service. This neglect to understand Facebook's privacy policies and terms of service is widespread (Acquisti & Gross, 2006; Govani & Pashley, 2005; Gross & Acquisti, 2005). In their before and after study, Govani and Pashley (2005) noticed that most students did not change their privacy settings on Facebook, even after they had been educated about the ways they can do so. Several studies found that there is little relationship between social network site users' disclosure of private

information and their stated privacy concerns (Dwyer, Hiltz, & Passerini, 2007; Livingstone, 2008; Tufekci, 2008). However, a recent study showed that actual risk perception significantly correlates with fear of online victimization (Higgins, Ricketts, & Vegh, 2008). Consequently, the authors recommend better privacy protection, higher transparency of who is visiting one's page, and more education about the risks of posting personal information to reduce risky behavior.

Tufekci (2008) also asserted that students may try "to restrict the visibility of their profile to desired audiences but are less aware of, concerned about, or willing to act on possible 'temporal' boundary intrusions posed by future audiences because of persistence of data" (p. 33). The most obvious and readily available mechanism to control the visibility of profile information is restricting it to friends. However, Ellison, Steinfield, & Lampe (2007) discovered that only 13 percent of the Facebook profiles at Michigan State University were restricted to "friends only." Also, the category "friend" is very broad and ambiguous in the online world; it may include anyone from an intimate friend to a casual acquaintance or a complete stranger of whom only their online identity is known. Though Jones and Soltren (2005) found that two-thirds of the surveyed users never befriend strangers, their finding also implies that one-third is willing to accept unknown people as friends.

This is confirmed by the experiment of Missouri University student Charlie Rosenbury, who wrote a computer program that enabled him to invite 250,000 people to be his friend, and 30 percent added him as their friend (Jump, 2005). Similarly, the IT security firm Sophos set up a fake profile to determine how easy it would be to data-mine Facebook for the purpose of identity theft. They found that out of 200 contacted people, 41 percent revealed personal information by either responding to the contact (and thus making their profile temporarily accessible) or immediately befriending the fake persona. The divulged information was enough "to create phishing e-mails or malware specifically targeted at individual users or businesses, to guess users' passwords, impersonate them, or even stalk them" ("Sophos Facebook ID," 2007)

These findings show that Facebook and other social network sites pose severe risks to their users' privacy. At the same time, they are extremely popular and seem to provide a high level of gratification to their users. Indeed, several studies found that users continually negotiate and manage the tension between perceived privacy risks and expected benefits (Ibrahim, 2008; Tufekci, 2008; Tyma, 2007). The most important benefit of online networks is probably, as Ellison, Steinfield, & Lampe (2007) showed, the social capital resulting from creating and maintaining interpersonal relationships and friendship. Since the creation and preservation of this social capital is systematically built upon the voluntary disclosure of private information to a virtually unlimited audience, Ibrahim (2008) characterized online networks as "complicit risk communities where personal information becomes social capital which is traded and exchanged" (p. 251). Consequently, social network site users are found to expose higher risk-taking attitudes than individuals who are not members of an online network (Fogel & Nehmad, 2008).

It can therefore be assumed that the expected gratification motivates the users to provide and frequently update very specific personal data that most of them would immediately refuse to reveal in other contexts, such as a telephone survey. Thus, social network sites provide an ideal, data-rich environment for microtargeted marketing and advertising, particularly when user profiles are combined with functions that track user behavior, such as Beacon. This commercial potential may explain why Facebook's valuation has reached astronomical levels, albeit on the basis of speculation. Since Microsoft's fall 2007 expression of interest in buying a 1.6 percent stake for $240 million, estimates of the company's value have ranged as high as $15 billion (Arrington, 2008; Sridharan, 2008; Stone, 2007).

For the average user, however, Facebook-based invasion of privacy and aggregation of data, as well as its potential commercial exploitation by third parties, tend to remain invisible. In this respect, the Beacon scandal was an accident, because it made the users aware of Facebook's vast data-gathering and behavior surveillance system. Facebook's owners quickly learned their lesson: The visible part of Facebook, innocent-looking user profiles and social interactions, must be neatly separated from the invisible parts. As in the case of an iceberg, the visible part makes up only a small amount of the whole (see figure 1).

The invisible part, on the other hand, is constantly fed by the data that trickle down from the interactions and self-descriptions of the users in the visible part. To maintain the separation (and the user's motivation to provide and constantly update his or her personal data), any marketing and advertising based on these data must be unobtrusive and subcutaneous, not in the user's face like the original version of Beacon.

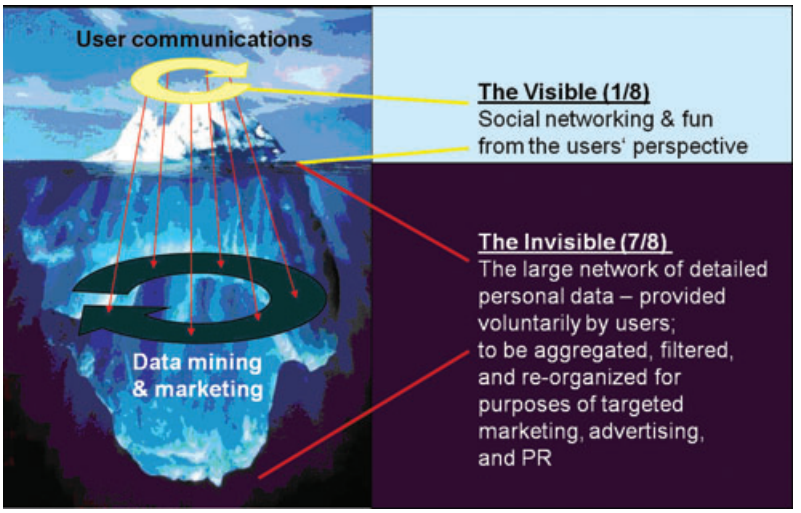

Figure 1 The Facebook Iceberg Model (Iceberg image © Ralph A. Clevenger/CORBIS)

Theoretical Approach

The conceptual framework of our research is a combination of three media theories: the "uses and gratifications" theory, the "third-person effect" approach, and the theory of "ritualized media use."

While this study does not test these three media theories, they are relevant as an analytical background and a framework from which to explain and contextualize our findings. The uses and gratifications approach looks at how people use media to fulfill their various needs, among them the three dimensions of (1) the need for diversion and entertainment, (2) the need for (para-social) relationships, and (3) the need for identity construction (Blumler & Katz, 1974; LaRose, Mastro, & Eastin 2001; Rosengren, Palmgreen, & Wenner, 1985). We assume that Facebook offers a strong promise of gratification in all three dimensions—strong enough to possibly override privacy concerns.

The third-person effect theory states that people expect mass media to have a greater effect on others than on themselves. This discrepancy between self-perception and assumptions about others is known as the perceptual hypothesis within the third-person effect approach (Brosius & Engel, 1996; Davison, 1983; Salwen & Dupagne, 2000). Though this approach has far-reaching implications with respect to people's support for censorship (known as the behavioral hypothesis), our interest is mostly focused on the *perceptual* side: How do Facebook users perceive effects on privacy caused by their use of Facebook and which consequences do they draw from this? Together with the uses and gratification theory, the third-person effect would explain a certain *economy of effect perception*, (i.e., negative side effects are ascribed to others, while the positive effects are ascribed to oneself).

The theory of ritualized media use states that media are not just consumed for informational or entertainment purposes, they are also habitually used as part of people's everyday life routines, as diversions and pastimes. Media rituals are often connected to temporary structures, such as favorite TV shows at a particular time, and to specific social rituals, such as ritualized meetings of friends to watch a favorite TV show, etc. (Couldry, 2002; Liebes & Curran, 1998; Pross, 1992; Rubin, 1984). It can be expected that the use of Facebook is at least to some degree ritualized and (subcutaneously) built into its users' daily life—a routinization (*Veralltäglichung*) in the sense of Max Weber (1972/1921). In conjunction with the two other approaches, this theory would further explain the enormous success of Facebook and users' lack of attention to privacy issues.

Based on the literature and theories examined above, the following four hypotheses for the survey and four open-ended research questions to guide the interviews were proposed:

H1: *Many if not most Facebook users have a limited understanding of privacy issues in social network services and therefore will make little use of their privacy settings.*

H2a: *For most Facebook users, the perceived benefits of online social networking will outweigh the observed risks of disclosing personal data.*

H2b: *At the same time, users will tend to be unaware of the importance of Facebook in their life due to its ritualized use.*

H3: *Facebook users are more likely to perceive risks to others' privacy rather than to their own privacy.*

H4: *If Facebook users report an invasion of personal privacy they are more likely to change their privacy settings than if they report an invasion of privacy happening to others.*

Research questions:

RQ1: *How important is Facebook to its users and which role does it play in their social life?*

RQ2: *To what extent is Facebook part of everyday rituals or has created its own rituals?*

RQ3: *Which role does Facebook play in creating and promoting gossip and rumors?*

RQ4: *Which negative effects, particularly with respect to privacy intrusions, does Facebook have?*

Method

An online survey, conducted in spring 2007, was administered to 119 college undergraduates at a large university in the Midwestern United States. A convenience sample was justified because this is a novel research field for which data are difficult to obtain and because online surveys rely on self-selection mechanisms and make randomized sampling difficult (Riffe, Lacy, & Fico, 1998). Additionally, eight participants (two male, six female) from the online survey respondent pool were selected for open-ended in-depth face-to-face interviews, which were conducted June 2007.

Survey Measures

The online questionnaire consisted of 36 multiple-choice questions. Survey respondents indicated basic information regarding Facebook habits, including the amount of time with an account (6 months, 1 year, 2 years, 3 years, greater than 3 years), how often the account was checked (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), and the average amount of time spent on Facebook *each* use (up to 5 minutes, 15 minutes, 30 minutes, 1 hour, or more than an hour). Furthermore, respondents specified what types of personal information they revealed in their profile, such as basic descriptors (e.g., gender, relationship status, if interested in men/women, birthday, hometown, political views, religious views), contact information (e.g., e-mail, phone number, address, number or dorm room or house, Web site), personal interests (e.g., favorite TV shows, movies, books, quotes, music), education information (e.g., field of study, degree, high school), work information (e.g., employer, position), and break information (e.g., activity, place). They also indicated what name they signed up under (i.e., if they used their real name, first name only, nickname, or made-up

name) as well as if they had uploaded a profile picture of themselves or additional pictures of friends, pets, etc.

In order to understand users' practices with regard to privacy, they were asked 1) if they were familiar with Facebook privacy settings (yes/no), 2) if they protected their profile (yes/no), and 3) how they protected their profile (survey options mirrored actual Facebook options: "I'm not sure," "All of my networks and all of my friends can see it," "some of my networks and some of my friends can see it," "only my friends can see it," and "I have different settings for different parts of my profile."). Respondents further indicated when they adjusted their privacy settings ("Right at the beginning," "After I figured out how to adjust the privacy settings," and "After having a profile for awhile") and, if so, why ("I am generally a cautious person," "I heard some concerning stories," and "Don't remember.") In all of these questions, respondents could only select one answer.

In order to assess the role of friends in Facebook use, respondents indicated how many friends they had and what kind of "friends" they accept ("Only people I know personally," "People I have heard of through others," or "Anybody who requests to be my friend"). In order to assess some of the perceived benefits of Facebook, respondents were asked three separate questions, "Do you feel that Facebook helps you interact with friends and people?" (yes/no) "Do you think that you would have less contact with your friends if you didn't have your Facebook account?" (yes/no), and "What role does Facebook play in your everyday life?" (very important/not important). Furthermore, to assess the perceived benefits of using Facebook, for each of these last three questions respondents' answers were given a score of 1 for a "yes" answer and 0 for a "no" answer. These three questions were then summed and averaged in order to create a perceived "benefits" score.

In order to examine the potential risks of Facebook, respondents answered whether they had encountered any or all of these three problems on Facebook: 1) unwanted advances, stalking, or harassment, 2) damaging gossip or rumors, or 3) personal data stolen/abused by others. Respondents could check yes or no to these three questions. Respondents' answers were given a "1" for a "yes" answer and a "0" for a "no" answer. Although the question did not differentiate between actual and perceived negative incidents, it is reasonable to assume that the subjective nature of these categories allows treating them as perceived risks. Additionally, respondents indicated how they reacted to those negative incidents ("I didn't change anything," "I restricted my profile and privacy settings," or "I cancelled my Facebook account").

Respondents further indicated whether *each* of these three negative incidents may have happened to *other* people (again, with yes/no options) and, if so, how respondents presumably reacted: "Did hearing about such incidences make you change your account settings?" (same answer options for when a negative incident had happened to the self—see above). Respondents were further asked, "*If* you were to hear about such incidents, would you change your account settings?" (same answer options for when a negative incident actually *had* happened—see above).

In order to examine the difference between perceived negative incidents to oneself and those perceived about others, ''self'' scores were aggregated and averaged and ''other'' scores were aggregated and averaged; thus, a third-person differential score was created by subtracting the ''self'' score from the ''other.'' In other words, this differential score reflected the difference between the negative effects respondents perceived about others and the perceived negative effects to themselves. To reiterate, the range for the perceived ''benefits'' score, the perceived negative incidents to *oneself*, and the perceived negative incidents to *others* were all 1 to 0 because each response that made up the score was assigned a ''1'' for a ''yes'' response and a ''0'' for a ''no'' response. Thus, the summed and averaged score remained on that scale.

Lastly, the demographic variables gender, age, and nationality were recorded.

In-depth Interviews

Eight participants (two male, six female) from the online survey respondent pool were selected for open-ended narrative face-to-face interviews, which were conducted in June 2007. At the end of the online survey, participants were asked if they would like to participate in a face-to-face interview about their Facebook use and experience. Interviewees were selected systematically by looking at their survey answers and comments (such as personal experience with privacy invasion), and pragmatically by their availability. In qualitative research, criteria for selecting subjects are often derived from the research questions, such as the expectation of topically relevant and rich narratives; hence, a randomized, statistically representative sample for the interviews is neither desirable nor necessary (Wrigley, 2002). The names of the interviewees are anonymous to protect their privacy. The participants received a written explanation of the research objectives and ethics before signing a consent form. Interviews followed the general interview guide approach and lasted between 45 and 90 minutes.

The interviews were recorded, transcribed, and then analyzed through a combination of qualitative content analysis, typological reduction analysis, and hermeneutical/rhetorical interpretation (Fisher, 1987; Kvale, 1996; Mayring, 1990; Weber, 1990). This type of qualitative analysis is particularly fruitful when dealing with a novel field that is not yet structured and requires preliminary understanding (Patton, 1990). It is mostly based on the summarizing reduction of the material and the inductive development of analytical categories from it and, in a second step, the deductive application of categories to interpret the data. Our main categories used to identify and interpret relevant statements were (1) invasion of privacy, (2) breach of trust, (3) violation of boundaries, (4) gossip and rumors, (5) habitual or ritualized use of Facebook. Additionally, statements containing the following specific figures of speech were identified for interpretation: (A) Salience—interesting or unusual expressions that indicate significance and/or emotional involvement; (B) metaphors, analogies, and similes—particularly with respect to how interviewees conceptualize facebook and their use of it; (C) ellipses and allusions—particularly implicit or indirect reference to connotations and background knowledge; (D) moral judgments

and value statements. Statements were checked for semantic intensity, frequency, and valence to reconstruct the interviewees' understanding of their experiences and their emotional involvement.

The qualitative analysis supplements the survey findings with additional evidence by providing access to Facebook users' meaning-making processes. They give deeper insight into attitudes and behaviors with respect to Facebook use and privacy issues, narratives related to the relevance, attraction, and usage of Facebook, and experiences about invasion of privacy on Facebook.

Findings

Quantitative Surveys

The survey respondents (n = 119) were predominantly female (68%), U.S. American (95%), and the largest age group ranged from 22–24 years old (27%). Half of the respondents had their Facebook account for 2 years and 37% checked this account daily, with 25% checking it three times/day and 23% checking it five times/day. On average, half of the respondents were spending up to 15 minutes each time they use Facebook, while 20% spent up to 30 minutes and 20% spent up to 5 minutes. Over a quarter (29%) reported that their Facebook account is always open or active when they are online. Almost 18% reported personally experiencing negative effects of Facebook, such as unwanted advances, stalking, and harassment, damaging gossip or rumor, or data theft. Forty-seven percent said they restricted access to their profile because they are generally cautious, and 38% because they had heard "some concerning stories." Most respondents (83%) reported that Facebook helps them interact with friends and other people.

Hypothesis tests

H1 predicted that Facebook users have a limited understanding of privacy settings in social network services and, therefore, will likely make little use of their privacy settings. This hypothesis was partially supported. Contrary to H1, a chi-square analysis revealed that there was a significant association between being "familiar" with Facebook privacy settings and utilizing privacy settings—in fact, the vast *majority* of Facebook users (91%) claimed indeed to be familiar with Facebook privacy issues and were also likely to restrict their profiles (77%) through privacy settings, $\chi^2(1) = 16.3, p < .001$. However, the same chi-square analysis revealed that those who were not familiar with privacy settings (9%) were also more likely to *not* protect their profiles. In other words, while the majority of users report to be familiar with privacy settings and protect their profiles, the minority—unfamiliar users—are also not protecting their profiles.

Furthermore, only 69% of the respondents indicated that they had actually changed the default privacy settings and about half reported that they restricted their profile so that "only friends can see it." Importantly, the definition of "friends" may

be different in this case, as the relative majority of users (38%), have over 300 friends, followed by 24% with 200–300 friends and 18% with 100–200 friends. Additionally, 10% reported that they accept "anybody" as a friend, 37% accept people "heard of through others," and 52% only accept people they personally know. Furthermore, over 90% of the respondents signed up under their full real name and included their gender, date of birth, and hometown. This same percentage of respondents also uploaded a picture of themselves as well as additional pictures of friends, family, pets, etc. Four-fifths of the participants specified interests, favorite TV shows, music, and movies, field of study, schools attended, and e-mail address on their online profile. About one-third provided specific contact information, such as phone number, address, and number of their house/dorm and room.

The above descriptives tell a different side to H1, showing that although the vast majority of users claim to be familiar with Facebook's privacy settings and report protecting their profile, they are allowing large groups of "friends" access to detailed, personal information. Therefore, H1, is partially supported because while the majority of respondents claim to understand Facebook's privacy settings and restrict their profiles, the minority who report being unfamiliar with the privacy settings are not restricting their profile. Additionally, the descriptives of respondents' actions speak differently: Extensive personal information is being uploaded and protected with suboptimal access restrictions, in effect making it accessible to large groups of people that the respondent may not personally know—which further illuminates the fact that participants may indeed have a limited understanding of privacy issues in social network services.

H2a, which predicted that perceived benefits of Facebook would appear to outweigh the observed risks of disclosing personal data, was supported. A paired-samples t-test was used to assess the difference between the perceived benefits and risks of using Facebook. Recall that respondents answered three yes/no questions that composed the perceived benefits score and three yes/no questions that composed the risks score. Results demonstrated that respondents did indeed see the benefits (mean = .75) outweighing the risks (mean = .28), $t(118) = 13.10, p < .001$.

H2b, which predicted that users tended to be unaware of the importance of Facebook in their life due to its routinized use, was not supported. A chi-square test of association showed that there was a significant relationship between frequency of Facebook use and perceived importance, $\chi^2(1) = 9.07,\ p < .01$. Specifically, more respondents than expected reported using Facebook *at least* "daily" and also reported that it was "very important" or "important" in everyday life. Similarly, more respondents than expected reported using Facebook fewer than once a day reported that it was not important in their everyday life. Significantly, those making Facebook part of an everyday habit seemed to recognize its importance—a shift contrary to H2b.

H3, which predicted that Facebook users are more likely to perceive risks to others' privacy rather than to their own privacy, was supported. A paired-samples t-test was utilized to examine the difference between perceived risks to the self and

perceived risks to others. Recall that risks to the self were summed (i.e., respondents' answers received a "1" if they indicated a risk and a "0" if they reported no risk) and averaged, as well as risks to others were summed and averaged. There was a significant difference between the perceived risks to the self (mean = .07) and risks about others (mean = .38), $t(118) = -10.60, p < .001$. Simply, respondents perceived more risks to others than to themselves. This finding further illustrates a *possible* third-person effect taking place.

H4, which predicted that Facebook users were more likely to change privacy settings if they reported a *personal* invasion of privacy than if they reported an invasion of privacy to *others*, was supported. A chi-square test of association showed that there was a significant relationship between the likelihood of changing Facebook privacy settings and the type of reported invasion (happened personally or happened to someone else), $\chi^2(1) = 6.23$, $p < .05$. For this analysis, only individuals who reported personally experiencing invasion of privacy (n = 23) or hearing about it through others (n = 41) were included. Specifically, 80% (n = 17) of those who *personally* experienced invasion of privacy made setting changes, while only 42% (n = 17) of those who heard about *others* experiencing invasion of privacy reported making changes. Thus, more than expected were making changes after personal experience and fewer than expected were making changes after hearing of "others" experience.

Qualitative Interviews

The qualitative analysis yielded four main topical areas that will be presented in the following sections: (A) routinization—the function of Facebook in users' daily life, (B) ritualization—the communicative and media rituals typical for Facebook usage, (C) the rumor mill—the function of Facebook as an accelerator and intensifier of gossip and rumor, and (D) privacy invasion—actual negative effects of Facebook on users.

Routinization—Just to keep in touch?

The main reason students say they use Facebook is to stay in contact with friends. Anne claims that it is "just to keep in touch, just to see what people are up to." For Emily, Facebook is important because of its convenience. Through Facebook, she can find phone numbers and e-mail addresses or send messages. Answers like this confirm that students use Facebook to easily access contact information, to communicate, and to find out what's going on in each others' lives. But it is more than that. Shannon described it as "kind of like you're hanging out with all your friends, but you don't have to be in the same room." It is like socializing without being social.

Interviewees usually spend up to an hour a day on Facebook, and the prevailing pattern seems to be that they check their account multiple times a day for a few minutes at a time, as opposed to one or two longer sessions. Most interviewees admit to Facebook being important in their lives because it helps them staying in

touch with ''friends back home.'' Jessica initially claimed that Facebook was not too important in her daily life, but later she acknowledged that she habitually looked at other peoples' pictures on Facebook and that the pictures are essential conversation subjects. Similarly, Meghan first maintained that Facebook was not important in her life but then she also admitted that it had become an integral part of her life. Given the fact that she has over 500 Facebook friends, one can reasonably assume that this may be an attempt to downplay and rationalize the significance Facebook has for her.

All in all, the statements from the interviews showed that Facebook had become an important part of student life, deeply ingrained in their daily routines, as is typical for pervasive technology. The gratifications drawn from using Facebook were mostly about the convenience and ease of being socially connected to a large number of people.

Ritualization—Rites with a safety net

Closely related to the routinization of Facebook is its ritualistic function. Students reported joining Facebook in a ritualized way, as a *rite of passage*. As long as Facebook limited its membership to college students, they signed up around the time they started college, upon hearing about it from peers and under pressure from them. Brian had the most interesting Facebook joining story: ''Everyone else had one and I was like one of the five people left on campus who didn't have one,'' he joked. While he described himself as initially ''very anti-Facebook,'' he ended up joining because his girlfriend forced him by setting up a profile for him. He then changed the password and has been using Facebook ever since.

User behavior on Facebook is in itself highly ritualized. The most striking example is Jessica's story about her habit to look at their friends' pictures:

Yeah, like, I mean, cause on Friday and Saturday people go out, well, Thursday I guess, like Thursday, Friday and Saturday people will go out. Sunday people will upload pictures. So Sunday, Monday people will up[date] profiles and that's when you look at everyone's pictures. At least that's what most people, most of my friends on Facebook do.

Jessica was, in fact, taking part in a well established weekly ritual of rehashing the weekend's social events with her friends—not too dissimilar to other media rituals such as group watching and rehashing of favorite TV shows. Interestingly, she was also well aware of the fact that she was not reciprocating the ritual because she did not upload her own pictures, although she liked to take a lot of them. The peer pressure did not seem to be strong enough to make her share her own pictures, yet she wanted to participate in the ritual of looking at the lives of others, which seemed to confirm to the above mentioned sentiment of socializing without being social, an intimate yet distanced voyeuristic position without actual involvement.

Facebook also seemed to have its own unwritten rules governing the ritual of accepting friend requests. Emily explained that on MySpace people are friends with strangers, ''but on Facebook, it's only people that you know that you're friends with . . . I think that's an unwritten rule for Facebook and an unwritten rule for

MySpace.'' The predictable environment of people she knew made Emily ''feel safer'' and she was therefore much more inclined to use Facebook than MySpace. Yet Facebook friends are not necessarily real friends. Rather, it seemed that the status of a Facebook friend could be used to maintain a ritualized distance from people, while at the same time affirming some sort of social relationship to them. This delicate balance was well described by Anne, who stated that there was a decisive distinction between real friends she hung out with and mere Facebook friends, with whom she had limited contact.

As much as it has its own (above described) rite of initiation, Facebook also seemed to support the *rite of separation* young college students go through when they move away from their home town. As Ellison, Steinfield, & Lampe (2007) have shown, this can be regarded as a form of ''maintained social capital'' that helps in keeping potentially useful contacts alive and in dealing with the distress caused by the loss of old friends. In our interview, Anne remarked ''nobody is going home anymore.'' She had 700 Facebook friends, and she added that Facebook friends are those with whom ''we're slowly becoming not friends.''

These three instances of ritualized Facebook use are very instructive. Not only did they confirm how much Facebook has grown into the daily life of college students, they also revealed important social and emotional functions of Facebook in their lives. Facebook provides ritualized ways of joining and opportunities for ritualized consumption of its content, but it also redefines the notion of friendship and provides a peculiar safety net for falling out of touch with friends.

The rumor mill—Feeding gossip and rumors

All interviewees agreed that Facebook fueled gossip and rumors, but they seemed to see this as mere side-effects of their Facebook usage and not as a main component. Students tended to see Facebook primarily as a tool to enhance social connectedness—only when specifically asked about the subject did they all acknowledge having first-hand experience with gossip and rumors generated through Facebook, particularly through the news feed. The participants expressed mixed feelings about this feature. Most of them disliked it and the overall consensus was that it increased gossip and rumor.

Anne said she ''hated'' the news feed from its debut, but despite her dislike she still looked at the news feed out of curiosity. Brian, who has experienced the most extreme form of privacy invasion through Facebook (see below), expressed strong dislike for the news feed, since it helped fuel the rumor mill when he was dealing with a hacker. He made it clear that rumors (as opposed to mere gossip) cross the line of what is tolerable. Both Anne and Brian agreed that relationship status is an important part of Facebook gossip. Any change in the relationship status will get the rumor started, Brian said. This indicates that inhibitions to gossip and rumor are lowered due to the news feed feature—a mechanical gossip machine—but it also highlights the interconnectedness of the Facebook world and the real world.

Emily downplayed the importance of Facebook gossip by saying that although Facebook might increase the speed rumors fly, gossip will exist regardless. She liked the news feed and thought that relationship stories were the only "interesting" news feed postings. Yet, she and her boyfriend did not immediately post their relationship on Facebook because she saw the relationship status as an important tool to create and maintain a positive image. She thought it should only be used if one is in a serious relationship. Though she believed herself to be unaffected by Facebook gossip, it turned out that she was actually heavily engaged in image management, which is just the flip side of the gossip mill.

Meghan explained that some rumors about people's relationships would not exist, or at least not spread as fast, without Facebook. Similarly, some of the gossip Jessica engaged in would not exist without Facebook. She and a friend from home "keep in touch kind of like through an enemy" by discussing another girl's pictures and making comments about her weight. Without Facebook, "it [the other girl's weight] wouldn't be a topic at all," she admitted. Students agreed that pictures were important gossip starters. Pictures will get taken out of context, as both Meghan and Jessica noted, and become the center of gossip and rumors. Participants are well aware of the risks that pictures of inappropriate, frowned upon, or illegal behavior pose. Some pictures should just "not be public knowledge," Shannon said. Everybody knew someone who got in trouble for underage drinking pictures, and there was widespread interest in damage control. Several students also mentioned that future employers may look at their profiles and that they did not want to possibly ruin their career.

Overall, gossip and rumors played a central role on Facebook. Not only are they fueled by the way the news feed system works, but in some ways they also provide the social glue that keeps the community alive and interesting. Facebook's creators may have been aware of the social desire for gossip and its function in a social network when they introduced the news feed. Indeed, gossip and rumor-mongering make up a key element of why students use Facebook—even if they don't want to admit it or seem not quite aware of it.

Privacy invasion—Crossing the line

Interviewees presented a wide range of experiences with privacy invasion on Facebook with a varying degree of actual changes in their behavior. Brian encountered the most extreme form of Facebook privacy invasion by having his profile hacked into multiple times, which twice led him to delete his profile, and (after the second occurrence) to institute strict privacy settings. The first time, the hacker changed some of Brian's groups and altered his "interested in" to insinuate (incorrectly) that Brian was gay. He brushed the incident off as a joke, changed his password, and "went on with everyday life." At that time, he was not aware of privacy options. Then, the hacker again entered his profile, changed his password back, and altered some things. Brian changed them back again and wrote on his status, "ok, you know, enough is enough . . . the joke's over, this isn't funny anymore." On the third day, his profile was

completely changed, including groups and interests, and his profile picture showed a combination of his head and a porn star's body. The hacker had also put in a relationship request with Brian's freshman-year roommate and changed his status to "I was just kidding. I'm having a hard time coming out of the closet right now."

To Brian's dismay, all these changes were made public through the news feed. This incident prompted Brian to delete his profile and stay away from Facebook for 3 months. But because he felt that Facebook is "a really easy way to keep in contact with people," Brian rejoined Facebook with a new e-mail address, assuming the hackers had finished their game. Yet six months later, his profile was attacked again, this time with a shot at his girlfriend. The hackers used the same manipulated profile picture, but added the character Donkey from the movie *Shrek* and tagged Donkey as Brian's girlfriend. Brian deleted the profile again, and set up another profile with a nonschool e-mail and strict privacy settings. The whole incident left him guessing who did it and why. He also said that he was very upset about the incident, particularly because his girlfriend became the target too. It is remarkable that Brian stayed with Facebook and kept coming back to it again and again. This case illustrates that the benefits and gratifications from using Facebook as a social tool can override the effects of even extremely negative experiences.

Peter also had an invasion of privacy experience with Facebook that prompted him to delete his profile. He got into an argument with another man in a Facebook group after criticizing the group's disapproval of men wearing a certain item of clothing. After the two of them argued back and forth through e-mail and Wall postings, the opponent posted the entire conversation on his group profile so it was public and Peter was unable to delete or change it. To have the comments removed, Peter had had to delete his account and set up a new one. He then restricted his new profile so that only his friends could see it, and reduced his friends from 500 friends to about 26 people he actually knew. His reasoning was that he wanted to be able to express himself without getting judged by people who did not know him.

Two additional interviewees experienced unwanted contact through Facebook. Anne removed her screen name from her Facebook profile after she received "random" instant messages from people who got her information through Facebook. She also removed her cell phone number after getting Facebook messages referencing her cell phone number. Anne has restricted her profile to be viewed by her friends only, but with her 700 Facebook friends, this restriction seems rather meaningless. Shannon recounted being tracked down by a man that she had borrowed a scarf from at a party. About a month or two later, he e-mailed her and called her home phone number, asking for the return of his scarf. He told her that he had found her through Facebook and then got her home phone number from the university directory. This seemingly benign incident made her uncomfortable and she subsequently tightened her security settings.

These stories show that privacy invasion is part of the Facebook reality and not just a hypothetical possibility. The intrusions into the users' personal lives create feelings of anger, lack of control, and fear. At the same time, users seem to adopt

two complementary types of coping strategies. The technical strategy is to tighten the privacy settings; the psychological strategy is to integrate and transform the incidents into a meaningful and ultimately unthreatening context. Knowing or at least believing to know who the perpetrator is creates a feeling of control and reassurance. The perpetrators are branded immature individuals or creeps, and the incidents tend to be minimized as pranks, exceptions, or events from a different world: "In the end," said Brian, reflecting on the hacking incident, "it's just Facebook. . . There was a time before Facebook. You can do without it. It's ok."

Discussion

This study examined the relationship of Facebook privacy issues, privacy settings, perceived benefits and risks, routinization and ritualization, and invasion of privacy to the self and others among a college population.

Survey findings indicated that while the majority of Facebook users report having an understanding of privacy settings and make use of their privacy settings, it is also apparent, however, that they may have a skewed sense of what that exactly entails. Additionally, as hypothesized, perceived benefits of online social networking outweighed risks of disclosing personal information. Risks to privacy were ascribed more to others than to the self. If Facebook users reported an invasion of *personal* privacy, users are more likely to change privacy settings than if they reported hearing of an invasion of privacy happening to *others*.

In general, the findings from the qualitative interviews corroborate the survey findings. Most strikingly, the interviews exemplified how deeply Facebook is integrated into daily routines and rituals, and how much it has produced its own routines and rites. The habitual use of Facebook and its integration into daily life indicates that it has become an indispensable tool of social capital and connectedness with large numbers of people. The benefits of Facebook outweigh privacy concerns, even when concrete privacy invasion was experienced.

All in all, the findings of our study confirm the results of previous studies on social networking, particularly with respect to routinization, privacy awareness, privacy settings, and trust (boyd & Ellison, 2008; Ellison, Steinfield, & Lampe, 2007; Jones & Soltren, 2005; Tufekci, 2008). Previous studies on social networking have also found a discrepancy between users reporting understanding and caution in regards to privacy and actually implementing the necessary steps to safeguard detailed personal data (Dwyer, Hiltz, & Passerini, 2007; Livingstone, 2008; Tufekci, 2008). While the Facebook users in our study report familiarity and use of privacy settings, they are still accepting people as "friends" that they have only heard of through others or do not know at all and, therefore, most have very large groups of "friends" that have access to widely uploaded information such as full names, birthdates, hometowns, and many pictures.

Additionally, many users are not changing default privacy settings, making them rely on lax, initial startup settings. Thus, conceptually, individuals may understand

the dangers of posting personal content on Facebook, but the desire to include personal information (this is after all what social networking sites do—allow others to get to know the individual behind the name) and the facade of only allowing "friends" access, eases users into believing that they have done an adequate job in protection. Therefore, it seems likely that the risks pale in comparison to the perceived benefits, even though many users report having observed the risks of using a Facebook account. Perhaps the evolving obsession with developing a persona and maintaining communication through technology (Twitter, texting, instant messaging, posting to social networking account, Second Life, etc.) is so embedded in the typical college students' ecology that to not engage in this form of communication would be social death.

Contrary to the survey findings, interviewees tended to underestimate Facebook's actual importance to them. This can be seen as an expression of the level of Facebook's integration into students' lives: A truly pervasive technology with a high level of gratification, Facebook has become an almost invisible part of students' everyday life. Part of this gratification is also the ability to participate in intimate yet distanced voyeuristic practices and to watch the gossip and rumor mill through the news feed and friends' pictures. The aggregated visibility of user activity through the news feed turned out to be a driving force in the production and proliferation of gossip and rumors.

Facebook allows users to maintain superficial social relationships with large numbers of people. In network theory, this phenomenon is discussed as "weak ties in the flow of information" (Gross & Acquisti, 2005, p. 2f), but this does not capture the sociopsychological function of the ritual, which became apparent in the interviews—to keep people at a ritualized distance. Possible consequences and negative side effects are also often seen as something that only happens to others: As long as they don't have direct personal experience with invasion of privacy, at least some users seem to think of privacy risks in terms of a third-person effect. Moreover, the conveniences and gratifications of Facebook as a social tool seem to override privacy concerns even in those cases where actual invasions of privacy were experienced. This was particularly well amplified in the story of the interviewee whose profile was hacked multiple times and who kept coming back to Facebook regardless. The coping strategies that the victims of privacy invasions tend to employ, however, demonstrate the affected users' urge to regain control. Restricting not only one's profile but also the number of one's friends is a reasonable strategy, and so are the meaning-making strategies that help to minimize feelings of fear and powerlessness. Though appropriate, these strategies are circumstantial and opportunistic, rather than expressions of stringent rational behavior—otherwise the risks Facebook poses to privacy would not be taken lightly in the first place.

Although this data suggests a third-person effect (perceived risk to the privacy of others is greater than the perceived risk to personal privacy) this may be misleading because in reality users potentially hear about problems or bad stories from many different people and yet only have a singular understanding of their own potential for risk. In fact, our survey showed that users are actually more likely to take action

or protect information if a negative experience happens to the self as opposed to hearing about it happening to others. Thus, while a third-person effect is evident in measuring the *potential* risk of privacy invasion, personal violation of privacy is what actually prompts changes to stricter privacy settings rather than second-hand information. This means that risks are systematically projected into the environment and only if they morph from a potential risk to an actual violation, users will change their behavior. This points us to a model where real risks are hard to make evident to, or taken seriously by, everyday users who have not yet encountered actual privacy violations.

These Facebook users are providing a fair amount of detailed personal information to a loosely defined group, which echoes concerns raised by Acquisti and Gross (2006), Jagatic et al. (2005), and Jones and Soltren (2005) with respect to data mining and phishing. While most participants have a basic understanding of privacy issues, they tend to be satisfied with the mere *idea* of control through Facebook's privacy settings without much real control. Although many 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, which they tend to divulge quite generously. In other words, users are unaware of or unconcerned about temporal boundary intrusions—threats to privacy due to data persistence—as described similarly in Tufekci (2008). This is a typical instance of a simultaneously unintended and uncomprehended consequence of human action in complex socio-technical contexts. Due to their black-box nature, computer systems invite this deceptive perception (Johnson, 1997), and the move from predominantly *technical interfaces* of desktop computers and Web 1.0 to increasingly *social interfaces* of networked, user-oriented Web 2.0 systems has further obscured the complex processes and interactions underneath the surface—the invisible part of the iceberg.

There is no question that more robust privacy protection software is a necessary condition for safer networking on Facebook and similar systems. But the privacy flaws go deeper because social network services are *conceptually designed* to lower privacy levels and to exploit the social information users provide willingly in these novel risk communities (Ibrahim, 2008). Cautious users would therefore have to conduct a careful cost-benefit analysis before revealing extensive personal data and opening it up to a potentially unlimited number of people, including data thieves or third parties who may use those data commercially. Safer use of social network sites would thus require a dramatic change in user attitudes: a responsible and informed user with a high level of computer literacy—not just in the technical but in the sociocultural and ethical sense, as well.

Like most research, this study has some limitations. First, the quantitative results rely on an exploratory survey that utilized measures developed without proven psychometric properties; thus, the survey's measure of the constructs of interest may not be as reliable and valid as desired. Further, some variables (such as time spent on Facebook or number of Facebook friends) were measured as categorical rather than

quantitative; analyses thus treated these variables as nominal scales of measurement. A limitation to this approach is the loss of within category variability, which may mask nonlinear relationships. Second, the small sample size, coupled with online convenience sampling from a single university, may limit the survey's generalizability. Third, the veracity of self-reported data may be tenuous, given social desirability biases. Lastly, our research used a cross-sectional design and causal inferences cannot be drawn. Additionally, because these data represent a mere snapshot of the situation in mid 2007, they cannot be used to predict future Facebook behavioral patterns.

Facebook is a moving target. New applications and additional privacy features are developed and implemented continually. It can be assumed that users' attitudes and behaviors change, too, as the technological framework is changing. It would be desirable to conduct some longitudinal follow-up research and see how users' attitudes and behaviors are changing over time. It would also be interesting to observe if and how social network sites age with their users, whether they remain permanent, routinized features in their users' lives, and how this translates into long-term privacy protection strategies on the part of the users. Moreover, future research should further investigate the relationship between perceived gratification and risk perception, and the mediating factors that motivate users to change their privacy-related behavior. This would allow to develop strategies for user education and to make recommendations for effective and transparent privacy protection techniques.

Conclusion

This study utilizes both quantitative and qualitative techniques to explore the timely intersection between online social networking use and privacy concerns. It shows that the gratifications of using Facebook tend to outweigh the perceived threats to privacy. The most common strategy for privacy protection—decreasing profile visibility through restricting access to friends—is also a very weak mechanism; a quick fix rather than a systematic approach to protecting privacy. Most users do not seem to realize that restricting access to their data does not sufficiently address the risks resulting from the amount, quality and persistence of the data they provide. After all, restricting profile visibility to "friends only" simply means restricting it within the visible part of the iceberg. As long as users feed the invisible part of the iceberg with extensive personal data that they update voluntarily and continually, their privacy is at risk. Given the targeted age groups, the strong attraction of social network sites, and the fact that gossip, harassment, hacking, phishing, data mining, and (ab)use of personal data by third parties are a reality in these networks and not just a hypothetical possibility, this paper illustrates that young adults need to be educated about risks to their privacy in a way that actually alters their behavior. The authors hope that the findings of this study may contribute to this process of education in computer literacy.

References

A race to the bottom: Privacy ranking of internet service companies—A consultation report. (2007, June 9). *Privacy International.* Retrieved September 15, 2007, from http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-553961 and http://www.privacyinternational.org/issues/internet/interimrankings.pdf

Acquisti, A., & Gross, R. (2006). *Imagined communities: Awareness, information sharing, and privacy on Facebook*. PET 2006. Retrieved October 2, 2007, from http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook2.pdf

Arrington, M. (2008, June 28). Want some Facebook stock at a $3 billion valuation? We know who to call. *TechCrunch*. Retrieved July 2, 2008, from http://www.techcrunch.com/2008/06/28/want-some-facebook-stock-at-a-3-billion-valutation-we-know-who-to-call/

Berkman, R. I., & Shumway, C. A. (2003). *Digital dilemmas: Ethical issues for online media professionals*. Ames: Iowa State Press.

Blumler J. G., & Katz, E. (Eds.). (1974). *The uses of mass communication: Current perspectives on gratifications research*. Newbury Park, CA: Sage.

boyd, d. (2008). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. *Convergence: The International Journal of Research into Media Technologies*, **14**(1), 13–20.

boyd, d., & Ellison, N. B. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, **13**, 210–230.

Brosius, H. B., & Engel, D. (1996). The causes of third-person effects: Unrealistic optimism, impersonal impact, or generalized negative attitudes towards media influence? *International Journal of Public Opinion Research*, **8**(2), 142–162.

Cocking, D., & Matthews, S. (2000). Unreal friends? *Ethics and Information Technology*, **2**, 223–231.

Couldry, N. (2002). *Media rituals: A critical approach*. London: Routledge.

Davison, P. W. (1983). The third-person effect in communication. *Public Opinion Quarterly*, **47**(1), 1–15.

Dawson, C. (2006, August 15). The fuzz wants to add you as a friend. *Education IT* [blog]. Retrieved December 4, 2007, from http://education.zdnet.com/?p=411

Does what happens in the Facebook stay in the Facebook? (2007). Retrieved June 19, 2007, from http://www.albumoftheday.com/facebook

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace," *Proceedings of AMCIS* 2007, Keystone, Co. Retrieved November 15, 2008, from http://csis.pace.edu/~dwyer/research/DwyerAMCIS2007.pdf

Ellison, N., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends": Exploring the relationship between college students' use of online social networks and social capital. *Journal of Computer-Mediated Communication*, **12**(4). Retrieved December 4, 2007, from http://jcmc.indiana.edu/vol12/issue4/ellison.html

Facebook principles. (2007, September 12). *Facebook.com*. Retrieved September 29, 2007, from http://www.facebook.com/policy.php

Fisher, W. R. (1987). *Human communication as narration: Toward a philosophy of reason, value, and action.* Columbia, SC: University of South Carolina Press.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, **25**, 153–160.

Govani, T., & Pashley, H. (2005). Student awareness of the privacy implications when using Facebook. *Carnegie Mellon*. Retrieved May 5, 2007, from http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Workshop on Privacy in the Electronic Society* (WPES). Retrieved October 2, 2007, from http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook1.pdf

Hamelink, C. J. (2000). *The ethics of cyberspace*. London: Sage 2005.

Ibrahim, Y. (2008). The new risk communities: Social networking sites and risk. *International Journal of Media & Cultural Politics*, **4**(2), 245–253.

Iachello, G. & Hong, J. (2007). End-user privacy in human–computer interaction. *Foundations and Trends in Human–Computer Interaction*, **1**(1), 1–137.

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2005). *Social phishing*. December 12, 2005, Indiana University, Bloomington. Retrieved September 22, 2007, from http://www.indiana.edu/~phishing/social-network-experiment/phishing-preprint.pdf

Johnson, S. (1997). *Interface culture: How new technology transforms the way we create and communicate.* San Francisco: Harper.

Jones, H., & Soltren, J. H. (2005). *Facebook: Threats to privacy*. December 14, 2005. Retrieved September 30, 2007, from http://www-swiss.ai.mit.edu/6805/student-papers/fall05-papers/facebook.pdf

Jump, K. (2005, September 1). A new kind of fame: MU student garners a record 75,000 Facebook friends. *Columbia Missourian*. Retrieved July 3, 2007, from http://www.columbiamissourian.com/stories/2005/09/01/a-new-kind-of-fame/

Kelly, C. (2007, June 4). *The hour's blog: CBC links up with Facebook* [blog]. Retrieved June 2, 2008, from http://www.cbc.ca/thehour/blog/2007/05/the_cbc_links_up_with_the_face.html#comments

Kessler, T. R. (2007, May 25). Internet 'joke' lands UNH student in trouble. *Citizen.com*. Retrieved October 2, 2007, from http://www.citizen.com/apps/pbcs.dll/article?AID=/20070525/CITIZEN_01/105250444

Kvale, S. (1996). *Inter views: An introduction to qualitative research interviewing*. Thousand Oaks, CA: Sage.

LaRose, R., Mastro, D., & Eastin, M. S. (2001). Understanding internet usage: A social-cognitive approach to uses and gratifications. *Social Science Computer Review*, **19**(4), 395–413.

Liebes, T., & Curran, J. (Eds.). (1998). *Media, ritual and identity*. London: Routledge.

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and selfexpression. *New Media & Society*, **10**(3), 393–411.

Luedtke, J. (2003, July 17). Toward pervasive computing—RFID tags: Pervasive computing in your pocket, on your key chain and in your car. *DMReview.com*. Retrieved September 22, 2007, from http://www.dmreview.com/article_sub.cfm?articleId=7096

Lull, J. (1990): *Inside family viewing: Ethnographic research on television's audiences*. London: Routledge.

Maher, M. (2007). You've got messages: Modern technology recruiting through text-messaging and the intrusiveness of Facebook. *Texas Review of Entertainment and Sports Law*, **8**(1), 125–151.

McKenna, K. Y., & Bargh, J. A. (2000). Plan 9 from cyberspace: The implications of the Internet for personality and social psychology. *Personality and Social Psychology Review*, **4**(1), 57–75.

Mayring, P. (1990). *Qualitative inhaltsanalyse: Grundlagen und techniken* [Qualitative content analysis: Foundations and techniques] (2nd ed.). Weinheim: Deutscher Studien Verlag.

NACE Spotlight Online (2006). Facebook, MySpace, etc. and getting hired. *Louisiana State University in Shreveport Career Center: Announcements*, June 22, 2006. Retrieved October 2, 2007, from http://www.lsus.edu/career/announcements_details.asp?ID=43 (mirrored at http://blog.thelifeofbrian.info/2006/07/12/privacy-big-brother-and-all-that-jazz/)

Pankoke-Babatz, U., & Jeffrey, P. (2002). Documented norms and conventions on the Internet. *International Journal of Human-Computer Interaction*, **14**(2), 219–235.

Patton, M. Q. (1990). *Qualitative evaluation and research methods* (2nd ed.). Newbury Park, CA: Sage.

Perez, J. C. (2007, November 30). Facebook's Beacon more intrusive than previously thought. *PC World*. Retrieved July 28, 2008, from http://www.pcworld.com/article/140182/facebooks_beacon_more_intrusive_than_previously_thought.html

Pross, H. (1992). *Zwänge: Essay über symbolische gewalt* [Constraints: Essay on symbolic violence]. Berlin: Karin Kramer Verlag.

Riffe, D., Lacy, S., & Fico, F. (1998) *Analyzing media messages*. Mahwah, N.J.: Lawrence Erlbaum.

Romano, A. (2006, September 25). Facebook's 'news feed.' *Newsweek*. Retrieved October 7, 2008, from http://www.newsweek.com/id/45681

Rosengren, K. E., Palmgreen, P., & Wenner, L. A. (Eds.). (1985). *Media gratification research: Current perspectives*. Beverly Hills, CA: Sage.

Rubin, A. M. (1984). Ritualized and instrumental television viewing. *Journal of Communication*, **34**, 67–77.

Salwen, P. B., & Dupagne, M. (2000). The third-person effect: A meta-analysis of the perceptual hypothesis. *Mass Communication & Society*, **3**(1), 57–85.

Schonfeld, E. (2008, May 17). Facebook's friends data has already left the barn. *TechCrunch*, Retrieved June 6, 2008, from http://www.techcrunch.com/2008/05/17/facebooks-friends-data-has-already-left-the-barn/

Singel, R. (2007, June 28). Facebook fixes search glitch, explains privacy strategy. *Threat Level. Wired Blog Network.* Retrieved October 2, 2007, from http://blog.wired.com/27bstroke6/2007/06/facebook-fixes-.html

Soghoian, C. (2008a, March 19). Flaws emerge in Facebook's new privacy controls. *CNet News.Com*. Retrieved May 28, 2008, from http://news.cnet.com/8301-13739_3-9898098-46.html

Soghoian, C. (2008b, January 23). Exclusive: The next Facebook privacy scandal. *CNet News.Com*. Retrieved May 28, 2008, from http://news.cnet.com/8301-13739_3-9854409-46.html

Sophos Facebook ID probe shows 41% of users happy to reveal all to potential identity thieves. (2007, August 14). *Sophos.com*, Retrieved September 22, 2007, from http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html

Spinello, R. A. (2005). Beyond copyright. A moral investigation of intellectual property protection in cyberspace. In R. J. Cavalier (ed.), *The impact of the Internet on our moral lives* (pp. 27–48). Albany: State University of New York Press.

Sridharan, V. (2008, June 26). It's official: Facebook not worth $15 billion. *Silicon Alley Insider.* Retrieved July 2, 2008, from http://www.alleyinsider.com/2008/6/it-s-official-facebook-not-worth-15-billion

Stehr, M. (2006, February 2). Unsafe Internet habits can lead stalkers to your door. *Daily Nebraskan*. Retrieved September 22, 2007, from http://www.dailynebraskan.com/home/index.cfm?event=displayArticlePrinterFriendly&uStory_id=7926276f-6141-430a-b417-32b71c7da93a

Stone, B. (2007, October 25). Microsoft buys stake in Facebook. *New York Times*. Retrieved July 2, 2008, from http://www.nytimes.com/2007/10/25/technology/25facebook.html?_r=2&oref=slogin

Tavani, H. T., & Grodzinsky, F. S. (2002). Cyberstalking, personal privacy, and moral responsibility. *Ethics and Information Technology*, **4**, 123–132.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, **28**(1), 20–36.

Tyma, A. (2007). Rules of Interchange: Privacy in online social communities: A rhetorical critique of MySpace.com. *Journal of the Communication, Speech & Theatre Association of North Dakota*, **20**, 31–39.

Privacy pilfered: When pole-vault champion's photo was posted all over web, she felt violated (2007, June12). *The Daily News.* Retrieved September 22, 2007, from http://www.tdn.com/articles/2007/06/12/this_day/news05.txt

Weber, M. (1972). Die veralltäglichung des charisma [The routinization of charisma]. In: M. Weber, *Wirtschaft und Gesellschaft* [Economy and Society] (pp. 142–148). Tuebingen: Mohr. (Original work published 1921).

Weber, R. P. (1990). *Basic content analysis*. Newbury Park, CA: Sage.

Weinberger, D. (2005). Anonymously yours. *KM World*, May 2005, 18–19.

Wrigley, B. J. (2002). Glass ceiling? What glass ceiling? A qualitative study of how women view the glass ceiling in public relations and communications management. *Journal of Public Relations Research*, **14**(1), 27–55.

About the Authors

Bernhard Debatin is Associate Professor for Multimedia Policy and Director of Tutorial Studies at the E. W. Scripps School of Journalism at Ohio University. His research interests include online communities, media ethics, online journalism, public sphere and philosophy of technology. He holds a Ph.D. in philosophy from Technical University Berlin (Germany) and a Master's degree in mass communication from Free University Berlin (Germany).
Address: E. W. Scripps School of Journalism, Scripps Hall 118, Ohio University, Athens, OH 45701. E-mail: debatin@ohio.edu

Jennette P. Lovejoy is a Scripps Howard Teaching Fellow and Ph.D. candidate at Ohio University's E.W. Scripps School of Journalism. Her research interests include mass communication theory, social networking, health communication, and discourses and beliefs of health and disease.

Address: E. W. Scripps School of Journalism, Scripps Hall 105, Ohio University, Athens, OH 45701. E-mail: jl141705@ohio.edu

Ann-Kathrin Horn graduated in 2009 from Leipzig University (Germany) with Master's degree in Communication Science. Her research focuses on social online networks. In 2006/07, she had a Fulbright and university exchange grant for the Master's program of the E.W. Scripps School of Journalism.
Address: E. W. Scripps School of Journalism, Scripps Hall 118, Ohio University, Athens, OH 45701. E-mail: ah637706@ohio.edu

Brittany N. Hughes graduated in 2009 from the Honors Tutorial College at Ohio University with a Bachelor of Science in Journalism. Her recent research, which resulted in an honors thesis, focused on the coverage of religion in *Time* magazine in the years before and after 9/11, 2001.
Address: Honors Tutorial College, 34 Park Place, Ohio University, Athens, OH 45701, USA, Ohio University, Athens, OH 45701. E-mail: bh125705@ohio.edu