With the growth of the Internet comes a growth in a ubiquitous networked society. Common Web 2.0 applications include a rapidly growing trend for social network sites. Social network sites typically converged different relationship types into one group of “friends.” However, with such vast interconnectivity, convergence of relationships, and information sharing by individual users comes an increased risk of privacy violations. We asked a small sample of participants to discuss what friendship and privacy meant to them and to give examples of a privacy violation they had experienced. A thematic analysis was conducted on the interviews to determine the issues discussed by the participants. Many participants experienced privacy issues using the social network site Facebook. The results are presented here and discussed in relation to online privacy concerns, notably social network site privacy concerns and managing such information.

KEYWORDS computer mediated communication (CMC), network communities, privacy, social network sites, society

INTRODUCTION

The increased prevalence and use of information communication technologies (ICTs) have transformed many people’s lives in terms of how they work, form, and maintain social relations and plan and use leisure time (Anawati & Craig, 2006). This rise in a networked society has not been without concern about, variously, the mental well-being of Internet users (Kraut et al., 2002; Kraut et al., 1998), the “pseudo” nature of communities and friendships.
forged online (Jones, 1995), dangers to children of either the content or time spent online (Hasebrink, Livingstone, Haddon, & Ölafrsson, 2009), and loss of social capital and trust in a virtual workplace (Handy, 1995). The work in the present paper addresses another concern raised frequently in discussions of the networked society: privacy. More specifically, we are interested in how privacy can be negotiated by people in social network sites (SNS) such as Facebook.

Social network sites typically share three common elements. They allow individuals to “construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by others within the system” (Boyd & Ellison, 2007, p. 211). A number of studies have demonstrated that the large-scale mobilization in Facebook is sparked by the opportunity to connect and communicate with people one has met or befriended off line (Ellison, Steinfeld, & Lampe, 2007; Golder, Wilkinson, & Huberman, 2007; Joinson, 2008; Lampe, Ellison, & Steinfeld, 2006) and to a lesser degree by the ability to investigate new others (Ellison et al., 2007; Joinson, 2008; Lampe et al., 2006). A range of content-sharing uses sustains these motivations, such as posting photographs, using applications, and changing the status update (Joinson, 2008). At a macro level, the intensity of using Facebook to maintain off line ties is related to different kinds of social capital formed within the off line community (Ellison et al., 2007).

Facebook, in addition to personal use and for keeping up with old friends (Joinson, 2008), is often used between colleagues, and managing such conflicting spheres can prove difficult (Binder, Howes, & Sutcliffe, 2009; DiMicco & Millen, 2007). Examples of violations are often seen in the media. For example, an employee in England was reported to have been dismissed because she wrote that her job was “totally boring” on her Facebook status (“Facebook Remark Teenager Is Fired,” 2009).

Social Networking and Privacy

In 2008, Internet access in the UK had increased to include 65% (16.46 million) of all households, an increase of 1.23 million since 2007. Great Britain has seen an increase of an average 1 million households per year since 2004 (UK Office of National Statistics, 2008).

Currently, Facebook has more than 350 million active users. Fifty percent of these users log in daily. There are more that 2.5 billion photos uploaded each month, with more than 3.5 billion pieces of content shared each week (including Web links, news stories, blog posts, notes, photo albums etc.) (Facebook, 2010). There are currently more than 70 translations of the site available, with 70% of Facebook users coming from outside of the United States (Facebook, 2010). The average user has 130 friends, sends 8 friend requests per month, is a member of 12 groups, and spends more than
55 minutes per day on the site (Facebook, 2010). As of December 2009, Facebook accounts for 7% of all time spent online in the United States (Lipsman, 2010). This increased use of social network sites has led to increased concerns about users’ privacy not only in terms of the data collected and used by the organization but also in light of the possible impact of mass sharing of personal information on social relations.

**Privacy and New Technology**

Westin (1967) defines privacy as “the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others” (p. 7). According to Westin, it is achieved through four main methods: “the voluntary and temporary withdrawal of a person from general society through physical or psychological means, either in a state of solitude or small group intimacy or, when among large groups, in a condition of anonymity or reserve” (Westin, 1967, p. 7).

Altman (1975, p. 24) defines privacy as “the selective control of access to the self” and argues that privacy is achieved through the regulation of social interaction. Both Westin’s and Altman’s theories have stimulated much of the research and theory development of privacy (Margulis, 2003). However, despite many attempts to create a synthesis of the existing literature in this area (e.g., Parent, 1983; Schoeman, 1984), a unified and simple account of privacy has yet to emerge. Because of this, more recent approaches have tended to focus on the different dimensions of privacy. For instance, Burgoon, Parrott, le Poire, & Kelley (1989) distinguish four dimensions of privacy and define it using these dimensions as “the ability to control and limit physical, interactional, psychological and informational access to the self or one’s group” (p. 132). DeCew (1997) also reflects the multidimensional nature of privacy in her definition, which distinguishes three dimensions: informational, accessibility, and expressive privacy. According to Schatz Byford (1996), “At no time have privacy issues taken on greater significance than in recent years, as technological developments have led to the emergence of an ‘information society’ capable of gathering, storing and disseminating increasing amounts of data about individuals” (p. 1).

While the underlying concept of privacy is not new, modern technological advancements have meant that privacy concerns have evolved. New ICTs have transformed our ability to collect, aggregate, and share data. Modern technology has the ability and power, particularly in comparison to the precomputer era, to capture, store, aggregate, redistribute, and use data from individual users (Sparck Jones, 2003). Sparck Jones (2003) discusses the permanence and vast quantity of the records held in such databases. Noting that the owner of this information is often unaware of, or at least unconnected to, its storage and utilization, she argues that such ubiquitous
data collection is harmful to personal privacy and autonomy, regardless of whether individuals differ on what they determine is private (Sparck Jones, 2003). The resultant harms of privacy violations may be both physical (e.g., bodily privacy) and psychological (e.g., fear of surveillance) (Altman, 1975; Joinson, 2009; Krueger, 2005; Solove, 2006; Warren & Brandeis, 1890; Westin, 1967). Solove (2007) reflects on this with the modern story of “dog poop girl.” “Dog poop girl,” as she is now known, was subject to the use of her image by a fellow train passenger after she had refused to clean up her dog’s excrement on an underground train. The unauthorized use of her image by a fellow passenger resulted in widespread dissemination. Had it not been for the ease of dissemination and search ability offered by the Internet, this viral would not have been as far reaching, and not have resulted in her leaving university, humiliated (Solove, 2007). The Internet, arguably, has made such incidents far more common and much easier for the everyday person to partake in. Crucially, many people are also complicit in this erosion of privacy, in particular through the use of SNS to share personal information with peers and marketing organizations.

PRIVACY OF SOCIAL NETWORKING SITES

Typically, privacy concerns online have related to e-commerce transactions, notably credit card fraud, vendors’ use of personal details, and customer identification (Miyazaki & Fernandez, 2000), but with growing concern over what users are posting online, the concern is no longer related solely to such issues. In relation to SNS, this tends to develop around the topic of identity fraud based on users’ posting of information on their profiles or the SNS itself allowing unrestricted “default” access (e.g., Acquisti & Gross, 2009; Gross & Acquisti, 2005; Lampe, Ellison, & Steinfield, 2007; Young & Quan-Haase, 2009). Although identity fraud, credit card fraud, and data storage concerns are undoubtedly alarming, privacy is also harmed by users’ own behavior, such as teenagers’ trend of “sexting” one another (Betts, 2009), cyberbullying (Reed, 2009), and the inability to control one’s social spheres on SNS (Binder et al., 2009).

Privacy can be viewed from the perspective of control. Whether it is control over personal data, the choice to disclose data, the physical presence of others, the number of others present in disclosure, or choosing which person to discuss and share issues with, control is central to maintaining privacy (e.g., Altman, 1975; DeCew, 1997; Solove, 2006; Warren & Brandeis, 1890). In particular, Altman, with his emphasis on social interaction with our environment, proposed the concept of personal, dyadic, and group boundaries for controlling privacy and disclosure (Altman, 1975). In daily off line life, these boundaries tend to be obvious. We are aware of who we are talking to, through vocalization or bodily posture and gestures; who we write to; what we have heard and from whom; who can see us walk down the street; who
can see us use the toilet; if cameras are pointed at us (although some closed-circuit television requires actively looking for it); who or what has touched us; and who and what we have touched (whether friendly or unfriendly). However, controlling these boundaries and the information flow between them in a SNS environment can prove difficult due to the eclectic use of the term “friend” (Binder et al., 2009). In an SNS, the term “friend” is often used to denote any number of potential relationship ties.

Types of relationship tie

The need to control the flow of personal information to different types of relationship tie is central to our social world. We allow certain more detailed, intimate aspects of ourselves to be released or shared with another as part of a private bond of intimacy, whereas we release less information to those who we hold a lesser intimate relationship with (Rachels, 1975; Reiman, 1976). For example, we may share different information with an intimate partner than with a parent. Reiman (1976) notes, “Only because we are able to withhold personal information about—and forbid intimate observation of—ourselves from the rest of the world, can we give out personal information—and allow intimate observations—to friends and/or lovers, that constitute intimate relationships” (p. 31).

In deciding which elements of one’s personality and personal information to release to various types of relationship, the centrality of each may be useful in determining how intimate or detailed the information is. Altman and Taylor (1973) describe the centrality of personality as similar to different and deepening layers of an onion. The centrality of individuals within a social network has been suggested to relate to levels of expected privacy. If personal information is taken by another and spread to connections further from the individual than would reasonably be expected by their own means and intimate friend group then it is argued as a violation of privacy (Strahilivetz, 2004).

In online interaction, such as a SNS, the distinction between who is able to see, obtain, and use various bits of our data or image becomes blurred. Virtuality creates a person management problem (Handy, 1995). By adding multiple types of “ties” to our “friends” list on, for example, Facebook, it becomes difficult to manage access and sharing with different people and types of “friend” (Binder et al., 2009; DiMicco & Millen, 2007). For example, photos of drunken excursions may be willingly shared with friends, but are they so eagerly shared with family, work colleagues, or even potential employers? Online, unless controlled and managed through often complicated privacy settings, everybody in the “friends” list can access these photos. Therefore, managing social spheres becomes complicated (Binder et al., 2009; DiMicco & Millen, 2007), and such complications and unforeseen circumstances may lead to privacy harms.
Issues of privacy on SNS can depend on the site used and the user’s site settings and personal privacy preferences. For instance, Facebook provides the ability to create a visible personal profile including photographs, hometown, date of birth, relationship status, and e-mail address (e.g., Christofides, Muise, & Desmarais, 2009; Joinson, 2008; Lampe et al., 2007) that is then openly available to potentially unknown others. Furthermore, unless privacy settings are customized, users may be unaware to whom they are disseminating information. Release of personal and private information may cause additional security problems including phishing, information leakage, and stalking (Gross & Acquisti, 2005; Hasib, 2008; Westlake, 2008). Social network sites that do not openly provide personal details are not exempt from privacy issues, potentially providing enough information to identify the user, such as by a photograph common with other SNS by default (Gross & Acquisti, 2005). Recent changes to the privacy settings of Facebook have further complicated this issue by making much information (e.g., photographs, lists of “friends”) open to everyone by default for the majority of users.

Discussion of privacy and social network sites has tended to focus on the potential threat posed by either outside access, such as reidentifying profile pictures, demographic data, or unique interests from other SNS (Gross & Acquisti, 2005). Other outside threats may originate in the general use of unsecured login connections used by SNS allowing easy access for third parties, such as hackers, identity thieves, and government (Gross & Acquisti, 2005). However, there are further privacy issues within the SNS and the network of contacts, even if private information is willingly disclosed by a site user (Gross & Acquisti, 2005). These include the open discussion of personal information among contacts, the posting and tagging of photographs that identify other users, disclosure of demographic data, and posting personal information on profile pages that implicates other users (Acquisti & Gross, 2006; Christofides et al., 2009). Furthermore, the availability of hometown and date of birth information has been shown to facilitate the calculation of Social Security numbers (SSN) in the United States (Acquisti & Gross, 2009).

Bonneau and Preibusch (2009) report a wide variety in the privacy control settings available across the 45 SNS they visited. Bonneau and Preibusch (2009) add that privacy policies, privacy controls, and informative measures are often complicated and below expectancy. In managing privacy within a SNS, sites rarely publicize their privacy enhancing tools even if they are available (Bonneau & Preibusch, 2009). Thus, if users are unaware that privacy threats exist, they are not likely to be prompted by the SNS that does not publicize such features, and so the unknown information sharing may continue. SNS may not publicize their features due to the effects of privacy salience: even for unconcerned users, raising attention to privacy controls may lead to users becoming more cautious and to sharing less information (Bonneau
Privacy concerns are rife throughout modern Internet usage. The increasing number of SNS and SNS users makes information sharing and concealing difficult to manage. The cumulative nature of social spheres, or relationship types, under the “friends” umbrella in SNS works only to amplify the issues. Users are often unaware of ubiquitous and large scale data collection and storage (Sparck Jones, 2003) and are often unaware of the harms of a collective “friends” group (Binder et al., 2009). Frequently researched privacy issues of online and SNS use typically include credit card fraud, identity theft, and what type of information users put on their SNS profiles (Acquisti & Gross, 2009). Although such issues are concerning, it is not clear what participants deem to be privacy violations or if their concerns match those of researchers.

To determine the difficulties and consequences of managing and experiencing a privacy violation, we interviewed a number of participants about their experiences and friendships. Although we asked about privacy violations in general rather than online, it became apparent that a majority of interviewees experienced a privacy violation due to their use of Facebook. Furthermore, as privacy can be seen as a control mechanism for limiting certain information flows to different types of relationship tie, we asked interviewees what friends and friendship meant to them to explore such links with privacy.

METHODOLOGY

This exploratory study used an open and unstructured approach to enhance the understanding and knowledge of what people mean when discussing friendships, privacy, and privacy violations. An opportunistic sample of eight individuals were interviewed using an unstructured approach but were provided with an initial question and discussion to set the topic. The 8 individuals were aged between 23 and 32 years old, of whom 3 were male and 5 were female. All participants had an education of at least an undergraduate degree, but from different disciplines. Participants were interviewed in similar, quiet environments at their convenience. The interviews were recorded using open source software (Audacity) and a standard PC microphone, and each lasted approximately 15 minutes, ranging from 10–26 minutes. Care was taken by the interviewer to avoid the use of leading questions or suggestive body language to ensure that the participant felt comfortable, open to discussion, and unbiased.

Participants were initially asked what their friendships meant to them followed by questions about a privacy violation that they had experienced at some point in their lives. This was to allow an insight into the results of
privacy violations on friendships before and after a violation had occurred. Friendships and their benefits were asked about in general terms, whereas the questioning related to the privacy violation was more specific.

Ethical concerns, while only marginal, were considered, thus steps were taken to reduce such risk. Informed consent was given. Participants were told of their right to withdraw their data at any point. Participants were informed that they could give as much or as little detail as they felt comfortable with and were reminded of this during the interview when privacy issues were discussed. The interviewer was not to coercer further information from the interviewee if the topic seemed potentially upsetting or too sensitive. Finally, should any unforeseen consequences have arisen, the interviewee could discuss these with the interviewer, who could then advise on suitable help and referral to specialists in that area (using the NHS Direct Web site).

Of the eight participants, all the interviews were transcribed, and none indicated any distress or wish to withdraw their data from this study. Thematische analyses were then conducted on the transcriptions to reveal modal themes and issues.

RESULTS AND DISCUSSION

The interviews highlighted a variety of issues relating to what friendship meant to each participant and what constituted a privacy violation. Some interviewees were relatively certain in their conceptualization of privacy, whereas others were more unsure. Privacy violations were varied, too. Some participants were unable to recall a privacy violation or were unconcerned that their privacy could be violated, whereas others were more certain about what had happened and what it meant to maintain privacy.

Of the eight privacy violations discussed by participants, five related specifically to social network sites, and three to offline violations (although they incorporated technology in some form or other). The violations reported are outlined in Table 1.

Common Issues with Violations

Participants’ usual response on experiencing, or becoming aware of, a privacy violation was to change their relationship with the violator, on one occasion even when the violator was clearly an innocent bystander. P5, for example, was subject to a third party using a friend’s Facebook account in an attempt to elicit money from her via a cry for help using the chat feature. Acknowledging that this was a loose friend, the participant transferred some of the blame onto the friend and has not spoken to the friend since.
Furthermore, P5 has “defriended” the person on Facebook with no further contact (Facebook being their only means to communicate).

Incurring an emotional or surprised response to a violation appeared unanimous across all interviews. Participants commented on feeling “upset,” “angry,” and “shocked.” For example, P1, who had recently broken up with her partner, suffered a privacy violation because this partner put details of the relationship’s demise onto a mutual friend’s Facebook wall. This led the participant to be “so shocked that he would do that, because it was sort of unfeeling…not cruel but…harsh.” When discussing this further the participant suggested that timing was key to the “painful experience…of [it] broadcast everywhere.” P1 noted that because the violation had occurred approximately two days after the breakup of the relationship (perceived as a short time by P1, especially for a three-year relationship), it may have caused more harm, suggesting that “if it had been later on, I don’t think it would’ve annoyed me.”

Across the interviews, time was frequently mentioned in reactions to privacy violations. Time was a concern if too brief a period passed between discussing something with another and their subsequent dissemination of the information, as in the case of P1, P2, P4, and P6 (see Table 1). Time was also a concern when a violation occurred too close to the sensitive event, such as

<table>
<thead>
<tr>
<th>Participant</th>
<th>Summary of violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Boyfriend sharing detailed relationship information with a friend via the public medium of the Facebook “wall” feature</td>
</tr>
<tr>
<td>P2</td>
<td>A confidant sharing sensitive financial information (failures) with a group of mutual friends</td>
</tr>
<tr>
<td>P3</td>
<td>Postal service employee obtaining credit cards and the personal information needed to activate them then using them to purchase valuable items</td>
</tr>
<tr>
<td>P4</td>
<td>A trusted friend dropping subtle comments into a conversation with a group of friends that could potentially allow this entrusted, dyadic information to become group knowledge</td>
</tr>
<tr>
<td>P5</td>
<td>An unauthorized user of an acquaintance’s Facebook account attempting to persuade the participant to transfer large sums of money to their account using the Facebook “chat” (instant messaging) feature</td>
</tr>
<tr>
<td>P6</td>
<td>A (now ex-) boyfriend discussed snide comments the participant had made with their parents, leading them to think she was not a good or appropriate person or girlfriend</td>
</tr>
<tr>
<td>P7</td>
<td>Friends using a Facebook group discussion board to gossip about silly things from the participant’s past, issues she no longer wishes to discuss or have discussed about her</td>
</tr>
<tr>
<td>P8</td>
<td>Discusses several issues to do with Facebook friends but focuses on an offline violation—the participant’s mother went through his room and discovered a home pregnancy test kit and discussed it with one of the participant’s friends, who in turn used it to mock the participant, leading him to feel annoyed with his mother for (a) snooping in his room and (b) sharing the information with others</td>
</tr>
</tbody>
</table>

Furthermore, P5 has “defriended” the person on Facebook with no further contact (Facebook being their only means to communicate).

Incurring an emotional or surprised response to a violation appeared unanimous across all interviews. Participants commented on feeling “upset,” “angry,” and “shocked.” For example, P1, who had recently broken up with her partner, suffered a privacy violation because this partner put details of the relationship’s demise onto a mutual friend’s Facebook wall. This led the participant to be “so shocked that he would do that, because it was sort of unfeeling…not cruel but…harsh.” When discussing this further the participant suggested that timing was key to the “painful experience…of [it] broadcast everywhere.” P1 noted that because the violation had occurred approximately two days after the breakup of the relationship (perceived as a short time by P1, especially for a three-year relationship), it may have caused more harm, suggesting that “if it had been later on, I don’t think it would’ve annoyed me.”

Across the interviews, time was frequently mentioned in reactions to privacy violations. Time was a concern if too brief a period passed between discussing something with another and their subsequent dissemination of the information, as in the case of P1, P2, P4, and P6 (see Table 1). Time was also a concern when a violation occurred too close to the sensitive event, such as

<table>
<thead>
<tr>
<th>Participant</th>
<th>Summary of violation</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>Boyfriend sharing detailed relationship information with a friend via the public medium of the Facebook “wall” feature</td>
</tr>
<tr>
<td>P2</td>
<td>A confidant sharing sensitive financial information (failures) with a group of mutual friends</td>
</tr>
<tr>
<td>P3</td>
<td>Postal service employee obtaining credit cards and the personal information needed to activate them then using them to purchase valuable items</td>
</tr>
<tr>
<td>P4</td>
<td>A trusted friend dropping subtle comments into a conversation with a group of friends that could potentially allow this entrusted, dyadic information to become group knowledge</td>
</tr>
<tr>
<td>P5</td>
<td>An unauthorized user of an acquaintance’s Facebook account attempting to persuade the participant to transfer large sums of money to their account using the Facebook “chat” (instant messaging) feature</td>
</tr>
<tr>
<td>P6</td>
<td>A (now ex-) boyfriend discussed snide comments the participant had made with their parents, leading them to think she was not a good or appropriate person or girlfriend</td>
</tr>
<tr>
<td>P7</td>
<td>Friends using a Facebook group discussion board to gossip about silly things from the participant’s past, issues she no longer wishes to discuss or have discussed about her</td>
</tr>
<tr>
<td>P8</td>
<td>Discusses several issues to do with Facebook friends but focuses on an offline violation—the participant’s mother went through his room and discovered a home pregnancy test kit and discussed it with one of the participant’s friends, who in turn used it to mock the participant, leading him to feel annoyed with his mother for (a) snooping in his room and (b) sharing the information with others</td>
</tr>
</tbody>
</table>

Furthermore, P5 has “defriended” the person on Facebook with no further contact (Facebook being their only means to communicate).

Incurring an emotional or surprised response to a violation appeared unanimous across all interviews. Participants commented on feeling “upset,” “angry,” and “shocked.” For example, P1, who had recently broken up with her partner, suffered a privacy violation because this partner put details of the relationship’s demise onto a mutual friend’s Facebook wall. This led the participant to be “so shocked that he would do that, because it was sort of unfeeling…not cruel but…harsh.” When discussing this further the participant suggested that timing was key to the “painful experience…of [it] broadcast everywhere.” P1 noted that because the violation had occurred approximately two days after the breakup of the relationship (perceived as a short time by P1, especially for a three-year relationship), it may have caused more harm, suggesting that “if it had been later on, I don’t think it would’ve annoyed me.”

Across the interviews, time was frequently mentioned in reactions to privacy violations. Time was a concern if too brief a period passed between discussing something with another and their subsequent dissemination of the information, as in the case of P1, P2, P4, and P6 (see Table 1). Time was also a concern when a violation occurred too close to the sensitive event, such as
P1, P2, P4, and P8 (see Table 1). In addition, P8 alluded to being caught “preparing to masturbate on my bed” and feeling “a little bit embarrassed” but that “ten minutes later, I went outside, faced the music, people laughed at me, I got over it.” P8 demonstrates that even if rather brief, there was an initial shock in the information dissemination quite soon after the event. Time was discussed further in reference to looking back at the violation after a long period and consequently no longer finding it harmful or painful. For instance, P6 said that “now the relationship’s over it doesn’t really matter, they [sic] can tell them all they want for all I care.”

Furthermore, participants were concerned with the ways in which friends/trusted others did not behave in the manner in which they expected a trusted other to behave with regard to their information. For example, P1 was “shocked” that her partner would divulge information about their relationship publicly. Also, participants found the friendship itself to be misinterpreted, resulting in a behavior that was unexpected at the time but would perhaps have been expected if they knew what sort of relationship they shared with the other person. For example, P2 said, “To me, it was really out of line...she didn’t realise what was wrong...and the understanding...that I could just tell her things that are on my mind [was not there].” Uncertainty Reduction Theory (URT) argues that people are motivated to reduce uncertainty in relationships, in particular about the character of the other person or their commitment and beliefs (Berger & Calabrese, 1975). To reduce uncertainty, we need to trade information with the people with whom we communicate (Berger & Calabrese, 1975). Therefore, to understand the expectancies of the dyad, individuals should share information to reduce uncertainty in their future behaviors before sharing more detailed personal information. Furthermore, Berger (1979) suggests three preconditions for uncertainty reduction: deviations from expected behavior, potential costs or rewards, and the likelihood of future interaction. A misunderstanding of these, similar to a misunderstanding due to poorly negotiated rules in communication privacy management (Petronio, 2002), may explain why participants endured a privacy violation and found it unpleasant emotionally. In the previous examples, the experienced unpleasantness was the participant’s surprise of the trusted other’s deviation from behavioral expectancy and the trusted other’s inability to realize the detrimental impact on their future interactions.

Many of the issues discussed previously are similar to issues raised by Petronio (2002) in her theory of communication privacy management (CPM). When participants’ expectations of others’ behavior differs from actual behavior, the implicit rule negotiation is broken and the management of information has failed. In sharing information with another or via an SNS, the participants were unaware of the condition of the boundaries surrounding them and their information. “Condition” refers to the permeability of the boundary and the choice of the trusted other to respect it or break it if it
prevented their sharing of this information. In online communication, sharing information with new contacts may serve to reduce uncertainty of their behavior and intentions (Tidwell & Walther, 2002), but this may also lead to increased risk of privacy management issues. Thus, boundary control becomes erroneous, highlighting the difficulties of maintaining multiple social spheres, as noted by Binder and colleagues (2009) and DiMicco and Millen (2007).

CPM also defines information as co-owned once shared. Participants expecting the information to be entirely controlled by themselves may not have appreciated the idea that once information is shared, the recipient becomes a co-owner (Petronio, 2002), and while the desire of the sharer should be respected, it often may not be. For example, P6 was concerned that “my boyfriend would go away and tell his parents” about arguments that had arisen in their relationship. This is contrary to the view taken in the late 19th century by Warren and Brandeis (1890) that information should remain the right of the creator, and subsequently even letters written to others should remain in control of the author. Only when writings are published do they suggest that ownership is relinquished.

Today, in a ubiquitous computing environment with users creating much of the content of Web 2.0, it is increasingly important for users to realize the nature of boundaries, possible violations, and the importance of ownership of information. While it is not wholly acceptable to generalize from such a small sample, the participants of this sample population illustrate a few of the difficulties in establishing and maintaining operational privacy boundaries in the online ubiquitous society of today.

Thematic Analysis

From the range of privacy issues discussed in the interviews, a thematic analysis was conducted to determine several broader categories based on participants’ responses and information divulged. Items were first split by whether they represented either friendship in general or a privacy violation. The data in each split were then ranked by the total number of utterances a particular category received across all interviews. Data that arose from three or more utterances were filtered by the number of participants that uttered them. Any themes uttered less than thrice were removed to ensure the utterance constituted a repetitive theme. This resulted in 18 categories for privacy violations and 16 categories for general friendship components (see Tables 2 and 3, respectively).

This thematic analysis on privacy violations surfaces four main issues underlying the majority of mentioned themes: issues of control, boundary expectations and uncertainties, an initial shock/startle reaction, and a temporal component whereby the situation may be perceived differently. The privacy themes suggest a basis in Uncertainty Reduction Theory.
In particular, initial interactions are suggested to be a key time period whereby communication is increased to reduce uncertainty (Berger & Calabrese, 1975), and it is in initial dissemination of new information whereby privacy harms are most sensitive, suggested by a shock/startle reaction.

**TABLE 2** Thematic Analysis of Privacy Violations: Recurring Themes and the Number of Occurrences Across All Interviews

<table>
<thead>
<tr>
<th>Category/Theme</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uncertainty of information spread (loss of control)</td>
<td>11</td>
</tr>
<tr>
<td>Time component</td>
<td>8</td>
</tr>
<tr>
<td>Upsetting emotional reaction</td>
<td>8</td>
</tr>
<tr>
<td>Disparity of boundary rules</td>
<td>7</td>
</tr>
<tr>
<td>Release/share information outside of dyad/relationship</td>
<td>7</td>
</tr>
<tr>
<td>Increased caution/awareness (specific)</td>
<td>7</td>
</tr>
<tr>
<td>Expectancy to maintain boundary/secret</td>
<td>6</td>
</tr>
<tr>
<td>Shock/surprised emotional reaction</td>
<td>5</td>
</tr>
<tr>
<td>Increased caution/awareness (general)</td>
<td>5</td>
</tr>
<tr>
<td>Too many others know (or shared with)</td>
<td>4</td>
</tr>
<tr>
<td>Defriended</td>
<td>4</td>
</tr>
<tr>
<td>No value to violator (or loss)</td>
<td>4</td>
</tr>
<tr>
<td>Separation of violator from his or her org./group</td>
<td>4</td>
</tr>
<tr>
<td>Angry emotional reaction</td>
<td>3</td>
</tr>
<tr>
<td>Disparity/conflict of trust (loss of trust included)</td>
<td>3</td>
</tr>
<tr>
<td>No value to victim (or loss)</td>
<td>3</td>
</tr>
<tr>
<td>Not talk in public with others</td>
<td>3</td>
</tr>
<tr>
<td>Feeling embarrassed</td>
<td>3</td>
</tr>
</tbody>
</table>

**TABLE 3** Thematic Analysis of the Concept of Friendship: Recurring Themes and the Number of Occurrences Across All Interviews

<table>
<thead>
<tr>
<th>Category/Theme</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Different types of friends (e.g., some to socialize, some for humor, some to feel secure, some due to proximity)</td>
<td>18</td>
</tr>
<tr>
<td>Common experiences or tastes</td>
<td>12</td>
</tr>
<tr>
<td>Trust (inc. reciprocal trust and varying degrees of)</td>
<td>10</td>
</tr>
<tr>
<td>Sharing (non-descript)</td>
<td>9</td>
</tr>
<tr>
<td>To share humor/amusement</td>
<td>6</td>
</tr>
<tr>
<td>Feeling secure (security)</td>
<td>6</td>
</tr>
<tr>
<td>Count on/rely on/fall back on</td>
<td>6</td>
</tr>
<tr>
<td>Being close</td>
<td>6</td>
</tr>
<tr>
<td>To socialize</td>
<td>5</td>
</tr>
<tr>
<td>Respect</td>
<td>5</td>
</tr>
<tr>
<td>Reciprocal (e.g., giving and taking)</td>
<td>5</td>
</tr>
<tr>
<td>Enjoyment</td>
<td>4</td>
</tr>
<tr>
<td>Solve issues (gain inspiration)</td>
<td>3</td>
</tr>
<tr>
<td>Ask for help</td>
<td>3</td>
</tr>
<tr>
<td>Friends reflect part of you</td>
<td>3</td>
</tr>
<tr>
<td>Geographically unconcerned (far but close, close but far)</td>
<td>3</td>
</tr>
</tbody>
</table>
Issues of Control

Issues of control typically related to the participant feeling they had no or little control over the occurrence of a privacy violation. P1 was upset that the dissemination of the information was unsure and out of her immediate control: “It came up on the news feeds. . . . I don’t know [if] everybody gets the same news feeds but it came up on the news feeds.” P1 adds, “There wasn’t anything I could really do about it because . . . you can’t go onto somebody else’s wall and delete it.” Control issues arose for P3 when he felt “quite sick because I didn’t know what to do.” P5 discussed readjusting privacy settings on Facebook after a privacy violation to gain control over the access others have to her information. P5 also defriended their friend’s Facebook account to prevent future occurrences or an immediate risk of data leakage to the unauthorized third party. P6 discussed control in terms of wanting to “make a good impression on [her boyfriend’s] parents” and that issues arose when she could not control her boyfriend from “go[ing] to their [sic] parents and say ‘she’s done this and she’s done that.’” When P7 discovered widespread dissemination of gossip about her as a child she removed herself from that Facebook group and would speak to the members only individually.

Control as a method to manage privacy is suggested by privacy theorists and finds support in these interviews. For example, “Selective control of access to the self” (Altman, 1975, p. 24) and “the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others” (Westin, 1967, p. 7). Furthermore, in Petronio’s (2002) theory of CPM she notes that boundaries can be used as a mechanism of control and are instigated by rule negotiation. Such boundaries are protected from loss of control by the enforcement of consequences, such as ex-communication. Support is found here from P2 who says that “we are not friends anymore.”

Boundary Expectancies and Uncertainties

The second underlying issue is how participants have an expectation of a boundary of privacy. A violation then occurs when the boundary is broken, either deliberately or unintentionally. Work on boundaries for maintaining privacy was proposed as a method of controlling physical access to the self or access to the intimate zone surrounding an individual (Altman, 1975). Furthermore, by instigating these physical boundaries it allows a physical and mental environment for one to reflect and self-evaluate (Altman, 1975; Westin, 1967). This issue is taken further to include boundaries for withholding information about the self and the co-ownership of such information when it is shared within such boundaries (Altman, 1975; Petronio, 2002). Support for idea of boundary usage in information management is found
in URT. Managing communication boundaries and sharing information is motivated by a need to reduce uncertainty of others (Berger, 1979).

Such boundary issues and motivations are raised by the interviewees when discussing privacy violations. P1 says that her partner shared “a lot of information...more than I would have expected him to mention.” P2 experienced a disrupted dyadic boundary when “[name] just turned around and told everyone.” P4 became aware of the need to manage her boundaries in future because her friend “may not keep things to herself, and [because of] her judgement of what is something for her or something that she could say to everyone else.” P8 suffered an issue of boundary disparity when his mother broke the dyadic boundary around himself and his girlfriend by snooping around his room and finding a pregnancy test kit.

As noted earlier, controlling such differing social spheres becomes difficult on SNS because they are often converged to a single tie type (Binder et al., 2009; DiMicco & Millen, 2007; Gilbert & Karahalios, 2009). P1’s privacy violation broke the dyadic boundary surrounding her and her partner to all those that had access to a mutual friend’s Facebook wall. Those with access could be friends, family, or colleagues of one or multiple of the three parties. P7 endured privacy harms when stories and gossip from primary school were spread around a group of friends that she now had little or nothing in common with. Ideally, the information would have stayed between the very few who knew or alternatively have been discussed only by those with whom she is close. In this instance, the converging spheres were different types of friends rather than a friend and a family sphere blurring.

Initial Startle/Shock Reaction

The interview data suggests that the majority of participants’ initial reaction to a privacy violation was either to be shocked/startled or to have an emotional reaction such as anger or upset. This concept was closely related to that of “time” in the temporal component, as participants frequently mentioned being shocked at how soon the information had been disseminated. Alternatively, the shock resulted in others discussing events that occurred too far in the past. For example, P7 reacted to information about her becoming public on Facebook by saying that “for me it’s [a] bit annoying because I don’t want someone [to] actually talk about me in public and they even post lots of photos of me when I was a kid.” P1 reported, “It was just a shock for me when I first saw it.” P2 said, “I honestly wasn’t expecting her to just go around and tell everyone I know....How could she have done that to me?” P3 reflected, “I was very shocked. I then felt quite sick.” P4 agreed with the interviewer that there was a shock reaction to the violation. P6 admitted to feeling “a bit angry” about her boyfriend’s open discussion of private matters with his parents. P8 recalled being “really quite angry” at his mother and even “confronted her about it” and “also quite angry towards her friend for
bringing it up” when discussing the violation regarding his mother’s covert discovery of a pregnancy test kit.

Contrary to the deficit of such immediacy of information, SNS such as Facebook typically encourage interaction based on current thoughts, links, events, and discussions. For example, when posting a new status update, sharing a link or sharing a photograph on Facebook, the text box asks “What’s on your mind?” Answering in this immediate time frame may encourage users to post information before giving thorough thought to potential consequences. Such behavior may subsequently result in privacy harms and violations for themselves and others.

Time and a Temporal Component

This last underlying category demonstrates the temporal nature of privacy, that time can be not only a healer but that a lack of time can agitate the immediacy of the unpleasant emotion. Time, then, is a fundamental privacy process. Privacy preferences are said to be different for different situations, contexts, and points in time, and desired privacy fluctuates over time (Altman, 1975; DeCew, 1997; Petronio, 2002; Westin, 2003). The data from these interviews supports this notion yet further identifies that privacy violations do not necessarily result in defriending. Forgiveness may occur when such trust is breached within online interaction, as is suggested by Vasalou, Hopfensitz, and Pitt (2008).

P1 reflected a change in the anger she felt at the time and at the present: “Not now, but at the time.” P2, however, is no longer a friend with the violator once the “trust . . . and respect” had gone. P3’s insight is optimistic of a “worst case scenario” whereby a friend created a serious breach of trust but reflects on the idea that a true friend would have such a deep trust that any privacy violation would be repairable and perhaps would even strengthen the relationship.

Friendship Aspects

DIFFERENT TYPES OF FRIEND (TIE)

The most common theme throughout the interviews for friendship was that there are different types of friend. Participants spoke of the different things they enjoy with some friends and the implicit links between the type of friend and the expectancies associated with it. For example, P2 suggested that friends could be there to have fun with or to be a “safety net.” This links closely with work on management of boundaries. Boundaries are suggested to allow an individual (or group) to control who has access to different information about them and to determine when and in what situations this information is transferred (Altman, 1975; Petronio, 2002). Additionally, different
types of “tie,” or friend, exist within a social network, both off line and online. Ties are suggested to vary based on network structure and their position within the network (Granovetter, 1973; Haythornthwaite, 1996).

Rachels (1975) and Reiman (1976) both propose that we share more information about ourselves with those with whom we wish to be intimate to allow a social distinction of the type of relationship had. Therefore, we can determine that if a friend we thought of as particularly close does not share the same detailed information in return, this friend may not consider himself or herself as close a friend as we do him or her (Rachels, 1975; Reiman, 1976). In SNS contexts, ties are usually compounded as only one type, although this has caused discussion in the difficulties of managing the boundaries surrounding the realistic and actual occurrence of multiple tie types (Binder et al., 2009; DiMicco & Millen, 2007).

In our interviews, P3 discusses having different types of friend for different purpose. He suggests that friends who are proximally close are not necessarily those whom he considers his closest friends. His closest friends are those whom he has known since childhood despite their geographic dispersion. About longstanding friends, he says they are “the type of friends where the friendship is based on trust.” Whereas regarding his local friends he suggests they are “perhaps valuable in the sense of a career or contacts.”

Trust

The topic of trust was mentioned frequently across all interviews. CPM theory suggests that with those with whom we share personal information, there is a requirement that the shared boundary is thick, or less permeable. We expect information to be kept within the boundary due to trust in implicit or negotiated rules that the other parties are expected to sustain.

When discussing friendships, a number of participants suggested that trust is a very important factor. For example, P2 said, “I think trust is important between two people, if they want to share information, and also with trust that comes openness and respect.” This quote also highlights the importance of reciprocity in relationships.

Reciprocal Interaction

The topic of reciprocal interaction includes the categories of common experiences or tastes, sharing (nondescript), and any utterances that discussed a reciprocal interaction. P3 discusses that friends are people “who make the effort back . . . and they incite me to do in return.” Furthermore, he mentions that some friendships are based on “common interests, it’s social interaction, we go out, we do things together that we both like doing.” P4 indicates that friendship is about “sharing something with you.” P5 alludes to having
“friendships because you have things in common with those people... people you work with or live with or go to uni with.”

Support for the nature of sharing common items as a method to reduce cohesion and build relationships can be found in social psychology literature on group conflict (e.g., Eisenhardt, Kahwajy, & Bourgeois III, 1997; Sherif, 1958). Furthermore, the reduction of individual differences for success has been investigated within online global virtual teams that use ICTs (Panteli & Sockalingam, 2005).

CONCLUSIONS

This work aimed to determine what happens before and after a privacy violation with regard to friendship and resultant relationship changes. The data developed through a series of open interviews on what privacy and friendship meant to the participants and on their examples and thoughts about experienced violations. Although there are many and countering theories, circumstances, dynamic demands, and subjective and objective approaches to privacy, it is important to determine that what is theorized is what is experienced. The interviews have shown and supported many of the aspects of privacy as shown in the discussion. However, it is acknowledged that there are numerous other issues surrounding privacy, what has become apparent are the key concepts from this sample.

The sample supports the idea of boundaries within which information can be shared, the importance of co-owned information, that different boundaries exist around different types of friend or tie, and that privacy issues are ubiquitous with online SNS use. Furthermore, with such large scale use and development of SNS in the culture of the Internet, managing these boundaries, social spheres, aspects of information, and the relationships they entail may become increasingly difficult. It is necessary for users to be aware of such issues before they are experienced and for the development of SNS to include the options to prioritize information with different social spheres, similar to that managed physically in off-line environments. Currently, Facebook and LinkedIn are the only SNS to allow users to view their profile from the perspective of other users to see what information is visible about them (Bonneau & Preibusch, 2009).

Limitations

Although this work embraces the subjectivity of the qualitative, open methodology used, there are several limitations that are acknowledged here. The small sample size will affect the ability to generalize this sample to the greater population. There are also a number of topics that were raised in the interviews that were unfortunately not discussed within this article due to scope...
limitations. However, this work can be used as an indication and building block as to what are seen as important aspects of privacy to those not knowledgeable of or researching the area.

REFERENCES


