What is Privacy?

Natalie McCullough, Brooke Sims, Thomas Ballas, Jennifer Davis

ABSTRACT

We leave traces of ourselves everywhere we go, in person and online. Often people do not realize how much they are disclosing and how that affects their privacy. The purpose of this study is to understand what individuals disclose and why they disclose information online and in face-to-face interactions as well as to determine whether there are generational differences in disclosure. We conducted semi-structured interviews with faculty, staff, and students at Capital University to determine their perceptions of privacy. We found that most people value privacy but believe that society does not maintain privacy in healthy ways. In addition, many people believe that face-to-face interactions are more private than online interactions. Participants also indicated that there are generational differences to privacy. This research has the potential to make people aware of the risks of self-disclosure as well as inform institutional privacy policies.

INTRODUCTION

Eons in the future, some historian in a cyber-garret will aim a laser-cognitive receptor whatchamahooosis and record an obvious but profound truth: In the twenty-first century, privacy died (Kellerman, 2014, p. 286).

Privacy is understood in various ways. While there are definitions of privacy used in law, medicine, education, and research, little is known about how the general public understands privacy. With our ever-growing technological society, privacy is becoming an important issue to discuss and understand. This has led to the question of how people within our society define privacy. Can privacy have multiple meanings for different settings, or should it be defined as one cohesive concept? We examined these questions by interviewing a wide variety of individuals.

Palen and Dourish (2003) used a traditional view of privacy in their research on privacy and trust as a state of social withdrawal. That is, privacy was explained as a “dialectic and dynamic boundary regulation process”. The word “boundary” is often referred to in research studies about privacy as a key feature of what privacy really entails. Self-boundary is a boundary that is modified by self-disclosure (Joinson et al. 2010). Dyadic boundary involves alleged safety that the discloser feels related to his or her information being leaked to a third party (Joinson et al.). Both types of boundaries touch on the main issues related to defining privacy: Violation and disclosure. To understand the threats, we must first understand what is being threatened.

In relation to social networking a post is private if “(a) the student has changed their default settings such that their profile is no longer accessible in full by a non-friend, same-network user (i.e., only a truncated version is available); and/or (b) the student has changed their default settings such that their profile is no longer even searchable by a non-friend, same-network user” (Lewis et al., 2008). The individual has acted to make their profile less available to others making settings change into a “private profile.”

Nosko et al. (2010) identified three different types of information related to privacy issues: Standard identifying, sensitive, and potentially stigmatizing. Standard identifying information is the basic information that a person might disclose to a school, job, or bank. Sensitive information is the “details to locate or identify an individual and could be used to threaten or harm another” (Nosko et al.). Potentially stigmatizing information is the “sensitive personal information [e.g., religious views, political views, birth year, sexual orientation, interests, and about me] that could result in stigmatization within society” (Nosko et al.). All three types of information were found to be important for understanding threats to identity (personal and group).

The ability to be continuously connected to a network of friends and family via social networking sites has led to the development of a variety of new privacy threats. The overall goal of social networking sites (SNS) is to encourage connectivity with others by disclosing personal information, even if participants know disclosing said information can be potentially dangerous (Nosko et al., 2010). SNS users often can become the victims of crimes such as online-harassment, stalking, and identity theft.

Users expose themselves online to a high level of vulnerability due to posts that can reveal potentially harmful information such as addresses, current locations, and travel plans (Debatin et al., 2009). It is possible that seemingly harmless information can lead a user of SNS’s to become vulnerable to identity theft (Nosko et al., 2010). Lewis et al. (2008) discovered that students with private profiles have specific cultural preferences that differ from students with public profiles.

While privacy settings are available for most, SNS research has found that there is a disconnect between people’s perception of privacy, overall knowledge, and their actual behavior and disclosure levels (Joinson et al., 2010).
Users often feel more secure about the information they are posting when in reality it is much more accessible to others than the original poster might be aware. The disconnect between users’ perceptions of privacy and actual online behavior can be linked to users not reading the privacy statements or becoming informed about the websites privacy policies (Joinson et al.).

Standard privacy settings on many social networking sites are typically lax and allow for a high level of disclosure to seemingly anyone. Many SNS users do not change the default settings immediately to ensure a secure privacy. In fact, research indicates that people become more likely to actually change their privacy settings once they have been violated or hear about others having their privacy violated. In addition, it is easier to see risks to others than to see the risks to oneself (Debatin et al., 2009).

Sex has been shown to play a role in the level of privacy an individual chooses to maintain. Women generally tend to be more private than men (Lewis et al., 2008; Nosko et al., 2010). Nosko et al. found that men are more likely to disclose sensitive information and potentially stigmatizing information (e.g., political and religious views) than women.

Previous research indicates that younger people, compared to older adults, are more skilled Facebook users. The younger population’s use of social networking is more purpose-driven because young people use these sites to stay connected with friends via email, instant messaging, and/or short message service. This younger generation uses Facebook to micro-coordinate their lives as well as a general communication tool. Many older adults view Facebook’s purpose as a nostalgic communication tool to connect with old friends. This view is less purpose-driven because it derives from curiosity. Younger people tend to check their Facebook accounts multiple times a day for a few minutes at a time; whereas, older people are more likely to log into Facebook less often, but for longer periods of time. As more advanced users of Facebook, the younger generation is more of aware of Facebook’s privacy features, which leads to more confident Facebook usage. They possess more knowledge about consent-sharing practices; however, they are less concerned about the possibility of Facebook using their personal information. For the younger generation, disclosing personal information across a variety of domains (e.g., school, online) is part of everyday life. Thus, younger people may be less cautious when disclosing highly personal details and feel more comfortable with online disclosure. Older adults are more concerned about privacy threats, but are not as aware of the usage and privacy policies (Brandtzæg et al., 2010). Nosko et al. (2010) revealed that as age increased, disclosure of all types of information decreased. This correlation suggests the older generation is more cautious about disclosing details about themselves. A possible explanation for this is that social communication that is asynchronous yet personal may not provide the forum for communication that is comfortable for adult users. In addition, older adults can be overall less trusting of technology due to a lack of experience.

Relationship status is also an important factor in privacy disclosure on social networking sites such as Facebook. Relationship status is important in distinguishing levels of disclosure for personal information. In general, users who either indicated they were single or in a relationship, disclosed significantly more information than did users who did not disclose their relationship status. Users who indicated their relationship status as single had significantly more information present in their profiles than all other users. Single users may be seeking a relationship and therefore they use Facebook as a less overt dating site. Seeking a relationship could be motivation to reveal highly personal information across a variety of topics regardless of the dangers or threats associated with disclosing this information. Users who are single may be looking for a relationship through Facebook and therefore reveal more information in order to spark a connection (Nosko et al., 2010).

Network analysts have long studied the ways in which peers influence behaviors and preferences. It is noteworthy to examine the effect of social influence on privacy disclosure through social networking sites. Lewis et al. (2008) found that students are more likely to maintain private profiles if other students in their network also have private profiles. Students are even more likely to maintain private profiles if their roommates maintain private profiles as well (Lewis et al.).

Findings of research about online social disclosure indicate a strong connection to SNS activity. According to Lewis et al. (2008) privacy settings positively vary with online activity, suggesting that the more frequently a user manipulates his or her profile, the more likely the user is to adopt a private profile. In a similar study, Debatin et al. (2009) concluded that perceived benefits of Facebook would appear to outweigh the observed risks of disclosing personal data. The gratification that Facebook provides can determine the amount of personal information a person discloses. The more gratification the social media outlet provides to the student, the greater likelihood that students disclose information. The gratifications approach looks at how people use media to fulfill their various needs such as the need for diversion and entertainment, the need for (para-social) relationships, and the need for identity construction. Facebook can offer a strong promise of gratification in all three dimensions. If the gratification is great enough, the possibility of overriding privacy concerns is high.

Routine Facebook usage has also been linked to a ritualistic function. Students indulge in Facebook as a part of a weekly or daily ritual. The theory of ritualized media use states that media are not just consumed for informational or
entertainment purposes, but also habitually as a part of people’s everyday life routines as diversions and pastimes (Debain et al., 2009).

People’s level of present trust in the media can moderate their privacy behavior and disclosure. The level of disclosure is determined by how much people trust the site they are using (Joinson et al., 2010). Factors that influence an average user’s trust in a site include the functionality of the site, its overall aesthetics, and whether they or someone they know has used the site before. According to Joinson et al., individuals were less likely to disclose information when there was a weak privacy policy combined with cues to reduce trust. Without trust in a website or individual a SNS, disclosure of information is much more unlikely.

Despite all of this research about privacy, disclosure, trust, and threats identity, there is limited understanding of how people define and interpret privacy. We interviewed university students, faculty, and staff about their understanding of privacy, threats to privacy, and how understanding privacy varies based on whether an interaction is face-to-face or online. Through the use of a semi structured interview, we sought to discover how privacy is viewed and defined across a variety of different demographic domains.

**METHOD**

**Participants**

The participants were 5 students, 5 faculty members, and 6 staff members from a small private college in the Midwest. There were 6 men and 10 women. The mean age was 41 years and the range of ages was 20 to 61 years. This research was approved by the university’s Institutional Review Board (IRB). Participants received a $5.00 gift card as compensation for their time.

**Materials**

Interviews were conducted for this study. Participants were first asked a series of demographic questions followed by questions dealing with privacy perceptions. Questions concerning privacy perceptions were open-ended. Examples of interview questions include: Do you use in any social networking sites? How do you determine what you choose to put on social networking sites? How would you define privacy? What are the differences between online privacy and face-to-face privacy? Would you be more willing to have less privacy if it ensured safety? Do you share things with people about your personal life on a daily basis that are a potential threat to privacy? Does the level of trust you have with a person or a website determine how much you share with them? Do you think that society values privacy? What steps do you take to keep private the aspects of your life that you don’t want others to know about?

**Procedure**

The interview process was conducted in person with one student researcher asking the questions and a second student researcher recording the participants’ responses. The participants were asked a variety of open-ended questions about the aspects of privacy and how privacy varies based on situational variables.

**RESULTS**

In our first interview question we asked, “Do you use in any social networking sites? If so, which ones? We found that every participant used at least 1, and most participants reported using between 2 and 4 different sites with Facebook as the top response. Following this, we asked how the participants determine what they share on social networking sites. Our responses included, the majority of respondents saying that they always try to post things that are “clean and appropriate”. This was followed by themes of appropriate professionalism, as well as using posts for networking and socialization.

Our main question of “How would you define privacy?” resulted in people identifying different definitions of privacy. Some participants were asked this question at the beginning of the interview and others were asked the question at the end of the interview to see whether thinking about privacy resulted in different definitions of privacy. We did not find a consistent pattern in definitions of privacy based on whether the question was asked at the beginning or the end. We did find that some participants had a more difficult time coming up with a definition when asked at the end of the interview. Definitions of privacy often included issues of privileged information and control over information. Five individuals indicated that there are different levels of privacy. Four people related privacy to a moral code and connected it with personal values.

Participants also were asked, “What are the differences between online privacy and face-to-face privacy?” Many participants indicated that face-to-face privacy means one-to-one communication and face-to-face interactions are more intimate while online interactions are more public. Many expressed that there is more control in face-to-face interactions. We followed with a question about the possibility of risk. When asked “do you think privacy is at risk for both face-to-face interactions and online?” for face-to-face interactions, 6 participants stated yes as to believing they are at risk, 6 said no, and 4 were in between. Students identified less risk for face-to-face interactions than faculty and staff. Most people said there is no privacy online.

When participants were asked to respond of a time when their own privacy was violated, 9 people described unintentional disclosure by a third party. Other examples included identity theft, and out of context statements.
Regarding the topic of having less privacy for more safety, 7 participants stated yes they would agree to have video cameras in student common areas and workplaces to ensure more safety with less privacy being a possibility; 6 participants stated no and 3 participants were in between. A primary theme that developed from this question was the importance of protecting individuality. Many had general reservations about giving up privacy in support of greater safety.

When the topic of trust was raised during the interview many emphasize the importance of trust as it relates to disclosure. The question asked was “Does the level of trust you have with a person or a website determine how much you share with them?” All 16 participants stated yes. Past experience was a big determinant of the level of disclosure (N = 12). How well a person knows the person or website was also a determinant (N = 12). Five people said they would never trust a random website. Four people said reputation of the website or company was important.

The next question was “Do you think that society values privacy?” Seven people stated yes, 6 said no, and 3 said maybe. These responses were followed by comments related to the theme of privacy being an ideal, but we do not take the necessary steps to ensure privacy. We did find some generational differences: People indicated that the different generations value privacy differently. Eight people said we sacrifice privacy through gossip and sharing information in unhealthy ways.

The final question asked was “What steps do you take to keep certain aspects of your life private?” Eleven respondents stated that they monitor their electronic usage and 8 stated that they monitor face-to-face interactions as well. Other themes included not participating in a lot of social media, shredding or record keeping.

Discussion

A key finding of this study focused on people’s evaluation of society’s value of privacy. A large number of participants stated that society values privacy, but does not try to protect privacy in an appropriate manner. Several participants stated that gossip and unhealthy sharing of information outweighs the desire to keep aspects of their lives private. The value of privacy question relates to the previous questions concerning social networking websites. Though all of the participants said they engage in social media, participants that engaged in multiple social media sites were more likely to express that oversharing is a threat to privacy. This could be attributed to the access social media sites give to people’s lives. For example, Facebook gives others insight into our interests, locations, and daily thoughts. As a person is more involved in social media, the more access people are given into their lives; therefore, they have a greater risk of having their information shared in an unhealthy way. It might be considered that privacy is becoming less valuable to society because of the presence of social media sites and the access it gives into people’s lives. Questions in concern might be, the more popular social networking becomes how will people then choose to monitor their privacy and will privacy be obtainable in our “connected” society?

Another important finding of the research is people’s desire to protect individuality and how this relates to privacy. Several participants stated that protecting their privacy was also a way of protecting their individuality. This relates to the question about giving up privacy in order to have safety. Participants who did not agree to give up privacy for safety stated that this has the potential to infringe on individual rights. Of these participants, most stated that the presence of cameras in common areas lead to situations being taken out of context and people’s actions might be misinterpreted because cameras do not show the full context of a situation. Participants who answered no to this question value safety, but do not believe that more cameras are an effective way of protecting safety. The majority of participants who answered yes to this question did so with hesitation. People are weary of having their every action documented with video evidence. Most people realize the importance of video surveillance when cameras are used for positive reasons, such as decreasing crime. However, they realize that a level of privacy must be compromised in order to achieve safety.

Several participants indicated that control is an important aspect of privacy. All of the participants use at least one social networking site and therefore have standards for what they put online. With social media sites users have a level of control over what others see. Only when indulging in unhealthy behaviors do people sacrifice privacy for connection, this however, is done, intentionally, by the individuals themselves. People exhibit control by adhering to their own standards of acceptability. Control gives people a sense of comfort and feeling of authority over their decisions. This could help explain why all participants engaged in social media but were hesitant to allow cameras to be placed in common areas for safety. With social media, the user has the ability to control privacy settings; however, with video surveillance the control is placed in the hands of another person. People were hesitant to agree to video surveillance because of uncertainty about camera locations and use. With uncertainty, comes hesitation. This might explain why few participants agreed to video surveillance only if they knew where the video cameras were placed.

In summary, the findings of this research have the potential to make people more aware of the risks of self-disclosure as well as inform institutional privacy policies.
The sample size and diversity among the population was a limitation of the current study. Increasing the sample size could add more variety in responses. This might allow for more generational differences to become apparent. We also suggest increasing the time length of the study to cover a full academic year. This would allow for more time to recruit participants as well as increase the amount of interview times that are available.

A potential limitation of the current study could be misinterpretations that occurred when students were typing the participant’s responses. Two groups or researchers conducted the interviews and it is possible that the two groups could have resulted in different methods of paraphrasing the responses. This could have led to a difference in data presentation, which could have then influenced the final coding process.

For future research, it would be interesting to discuss the boundaries people have with video surveillance, privacy, and safety. For example, where would people agree or disagree to put cameras, how many cameras are acceptable per area, etc. It would also beneficial to discover to what degree people are willing to sacrifice their privacy for safety. This could improve upon the current study in a way that would help us better understand a person’s view on the relationship between privacy and safety.

Focusing more in-depth on online privacy could help provide a closer look into problems that affect privacy. The questions about face-to-face interactions of the current research are relevant and important for comparison purposes; however, the threats to online privacy are highlighted, daily, in news media and this is the primary issues society must address. We found that most people had experienced an incident of their privacy being violated online. Therefore, the researchers believe that it would be beneficial to place a greater emphasis on online privacy for future studies.

REFERENCES


