“What Can I Really Do?” Explaining the Privacy Paradox with Online Apathy

ESZTER HARGITTAI[1]
Northwestern University, Illinois, USA

ALICE MARWICK
Fordham University, New York, USA

Based on focus group interviews, we considered how young adults’ attitudes about privacy can be reconciled with their online behavior. The “privacy paradox” suggests that young people claim to care about privacy while simultaneously providing a great deal of personal information through social media. Our interviews revealed that young adults do understand and care about the potential risks associated with disclosing information online and engage in at least some privacy-protective behaviors on social media. However, they feel that once information is shared, it is ultimately out of their control. They attribute this to the opaque practices of institutions, the technological affordances of social media, and the concept of networked privacy, which acknowledges that individuals exist in social contexts where others can and do violate their privacy.

Keywords: focus groups, Internet skills, networked privacy, online apathy, privacy, privacy paradox, young adults

While many Americans claim to be concerned about privacy (Madden & Rainie, 2015), their behavior, especially online, often belies these concerns. Researchers have hypothesized that this “privacy paradox” (Barnes, 2006), in which individuals affirm the importance of privacy while providing personal data to websites and mobile apps, may be due to a lack of understanding of risk (Acquisti & Gross, 2006); a lack of knowledge about privacy-protective behaviors (Hargittai & Litt, 2013; Park, 2013); or the social advantages of online self-disclosure (Taddicken, 2014). This is especially salient for young people, for whom social media may be intrinsic to social life, school, or employment. Using data from 10 focus groups totaling 40 participants ages 19–35, which were held during summer 2014, we examine young adults’ understanding of Internet privacy issues. We hypothesized, based on prior literature, that we would find

Eszter Hargittai: eszter@northwestern.edu
Alice Marwick: amarwick@gmail.com
Date submitted: 2016–01–24

[1] We are grateful to Merck (Merck is known as MSD outside the United States and Canada) for its support. For assistance with the project, we also thank Elizabeth Hensley and Northwestern University’s Summer Research Opportunity Program, Devon Moore, Somi Hubbard, and Karina Sirota through Northwestern’s Undergraduate Research Assistant Program. Hargittai also appreciates the time made available through the April McClain-Delaney and John Delaney Research Professorship for conducting this project.

evidence of the "privacy paradox": namely, concern over privacy, but little presence of privacy-protective behavior. Our central research question investigates whether and to what extent lack of Internet experiences and skills may explain this paradox. Research on Internet skills suggests that people vary considerably in their level of understanding and use of various Internet functionalities, including those concerned with privacy (Hargittai & Litt 2013; Litt, 2013; Park, 2013). Our project considers whether such skill differences may explain the paradox identified in the privacy literature.

The Privacy Paradox

In contemporary scholarship, the "privacy paradox" is usually described in relation to social media, digital technologies that facilitate personal information provision and dissemination to a networked audience (Acquisti & Gross, 2006; Barnes, 2006; Quinn, 2016; Tufekci, 2008). Before such technologies became commonplace, however, privacy scholars identified a gulf between self-reported privacy attitudes and actual privacy behaviors. Between 1978 and 2004, Alan Westin conducted over 30 surveys measuring Americans' privacy concerns. He found that 57% were "Privacy Pragmatists," evaluating risks and benefits of information provision; approximately 25% of people were "Privacy Fundamentalists," highly concerned about privacy and willing to engage in privacy-protective behavior; and 18% were "Unconcerned," happy to provide information to receive minor benefits, like discounts (Kumaraguru & Cranor, 2005). However, when Spiekermann and colleagues (Spiekermann, Grosslags, & Berendt, 2001, p. 8) tested these categories in experimental settings, they found that even "Privacy Fundamentalists" were willing to reveal "private and highly personal information" to an e-commerce chat bot that asked "non-legitimate and unimportant personal questions" during a shopping session.

This discordance between attitudes and behavior became more significant given the emergence in the early 2000s of social network sites like Friendster and MySpace, which popularized formerly niche communicative practices such as posting digital photographs, sharing thoughts online, and creating public profiles (boyd & Ellison, 2007). In several studies conducted during this period, posting information online served as evidence of a lack of concern about privacy, purportedly confirming the privacy paradox. Drawing on Westin's instruments, Acquisti and Gross (2006) compared the privacy attitudes of 294 college students to their information-sharing practices on Facebook. Their study discovered no relationship between privacy attitudes and information provision. Among students with the highest reported privacy concerns, 48% posted their sexual orientation, 21% posted their partner's name, and 47% posted their political orientation. The researchers hypothesized that this paradox might be explained by trust in the network (at the time Facebook was restricted to American college students with .edu email addresses) or a lack of risk awareness. A smaller comparative study of 194 college student users of Facebook and MySpace similarly recorded no relationship between privacy concerns and information provision (Dwyer, Hiltz, & Passerini, 2007).

Another subset of literature considered social network site profile settings. In scraping the Facebook profiles of all Carnegie Mellon University users, Gross and Acquisti (2005) found that very few students changed their default privacy settings, and many made their profiles entirely public. This finding was contradicted in several later studies. Tufekci (2008) found that 42% of Facebook-using college students had a publicly accessible profile compared to 59% of those who used MySpace; Thelwall (2008) scraped 20,000 MySpace profiles, of which 27% were set as private; and boyd and Hargittai (2010) found that most of a diverse set of college students changed their Facebook privacy settings at least once, a practice that increased over time, based on panel data.

Generational Differences?

Notably, these studies primarily used samples of college students. Scholars, journalists, and pundits have repeatedly exhibited concern about young people's use of social network sites (Kornblum, 2007; Nussbaum, 2007) and asserted that revealing personal information online is risky. In Barnes's article coining the term "privacy paradox," for example, the author mentions cyberstalking, pedophiles and rapists, and sexually explicit images (2006) as potential sources of concern. Expressing incredulity at a perceived rift between youth attitudes and behavior, Barnes wrote in the abstract:

> Teenagers will freely give up personal information to join social networks on the Internet. Afterwards, they are surprised when their parents read their journals. Communities are outraged by the personal information posted by young people online and colleges keep track of student activities on and off campus. The posting of personal information by teens and students has consequences. (Barnes, 2006, abstract)

While some of these concerns were valid, others were vague and lacked empirical evidence (Schrock & boyd, 2008) or reflected the popular media's moral panic concerning "online predators" (Marwick, 2008). The locus of concern regarding the privacy paradox, in other words, centered around a perceived schism between young people's stated concern for privacy and their enthusiasm for social network sites that require users to share personal information (boyd & Hargittai, 2010). The privacy paradox was thus primarily associated with young people and identified as a generational marker of difference, often summarized in the statement, "Young people don't care about privacy."

Scholars have identified three primary causes of the privacy paradox. First, young people share information online because they lack an adequate understanding of risk and awareness of danger (Acquisti & Gross, 2006; Tufekci, 2008). This is supported by later studies finding greater privacy-protective behaviors over time, during a period correspondent to significant media attention to the risks of social network sites (boyd & Hargittai, 2010; Stutzman, Gross, & Acquisti, 2013). Second, people share information online because they lack the skills to protect their personal information successfully (Hargittai & Litt, 2013; Park, 2013; Stenger & Coutant, 2010). Sites like Facebook frequently change their privacy settings, making it difficult even for savvy Internet users to post content in a way that corresponds to their privacy preferences (boyd & Hargittai, 2010; Stutzman et al., 2013).

Finally, recent studies have suggested that the paradox can be explained by the importance of social media sites for young people's socialization and, increasingly, education and employment. Taddicken (2014) found that users disclosed more personal information on applications perceived as "socially relevant" and that the greater their privacy concern, the more social relevance mattered. Similarly, Chang and Heo (2014) reported that social motives for using Facebook, time spent on Facebook, and number of Facebook friends all predicted personal information provision, including information considered highly sensitive. The centrality of social media to young people's lives is supported by research showing that behaviors that adults view as evidence of lack of concern for privacy, such as posting on social media, do not necessarily correspond to the way in which teenagers conceptualize privacy (Marwick & boyd, 2014; Steeves & Webster, 2008). One large empirical study, involving more than 7,000 college students, found that 75% of participants were concerned about the security of their passwords, credit card numbers, and social security numbers; they did not, however, see sharing personal information on social network sites as a privacy risk (Jones, Johnson-Yale, Millermaier, & Perez, 2009). A smaller study found that "as teenagers perceived more benefits from information disclosure, they were more willing to provide information" (Youn, 2005, p. 86). The operationalization of online information provision as a metric of privacy concern may, therefore, be problematic (Livingstone, 2008; Marwick, Murgia-Diaz, & Palfrey, 2010).

The generational aspect of the privacy paradox has further been called into question by studies that have found either little difference between privacy attitudes and practices among generational cohorts (Hoofnagle, King, Li, & Turow, 2010; Madden, Lenhart, Cortesi, & Gasser, 2013) or greater privacy-protective behaviors among younger people (Blank, Bolsover, & Dubois, 2014; Madden, Lenhart, Cortesi, Gasser, et al., 2013; Rainie & Madden, 2015). In a large sample of British Internet users, Blank and colleagues noted that "young people are the most likely of any age group to report having taken action to protect their privacy on social networking sites" (2014, p. 15). Similar surveys by the Pew Research Center in the United States found that young people were as likely as adults to engage in privacy-protective behaviors in mobile app environments (Madden, Lenhart, Cortesi, & Gasser, 2013) and more likely to have engaged in privacy-protective behaviors on social media (Madden, Lenhart, Cortesi, Gasser, et al., 2013). These studies suggest that if the privacy paradox does exist, it cannot be explained by generational divides.

In order to examine the privacy paradox critically, both general privacy attitudes and specific information-provision behavior, particularly on social media, must be examined. While the literature has identified general patterns of how attitudes and behaviors may or may not correspond to each other when it comes to privacy issues online, we lack a deeper understanding about these connections. Do young users understand the potential privacy risks associated with their online behavior, particularly on social media? To what extent do they believe it is up to them to protect their privacy on the wider Internet? What actions might they take to safeguard their information? Do they have the necessary skills to do what they believe they should be doing?

To address this gap in the literature, this project investigated young adults' knowledge about privacy in general and privacy-protective behaviors specifically by asking the following research questions:

RQ1: *What do participants know about Internet privacy issues; specifically, to what extent do participants understand potential privacy risks?*

RQ2: *To what extent do participants feel that social needs for sharing information online outweigh potential privacy risks?*

RQ3: To what extent do participants believe that keeping their information private is their personal responsibility?

RQ4: What do participants know about protecting their information online, namely, how skilled are they at online privacy protection? What do young people actually do to protect their privacy online?

Data and Methods

Data Collection

During the summer of 2014, we conducted 10 focus group interviews with a total of 40 young adults enrolled in college or graduate school. We recruited participants through flyers posted across a Midwestern urban campus and its environs; through ads on Facebook; and by emailing people in the first author’s network asking them to forward information to relevant people in the area. Students did not have to be enrolled at a particular school to participate, but they had to come to the project lab on campus for the session. We advertised the study as focused on general Internet use rather than privacy, so as not to bias recruitment toward participants who are especially interested in that aspect of digital media use. Each participant received $20 cash at the end of the session. The average interview session lasted about 1 hour. The principal investigator’s Institutional Review Board for Human Subjects Research approved the study.

Most sessions had four participants, one had five, and one had three. Before the discussion started, participants filled out a short survey regarding their demographic background, experiences using social media, and Internet skills. We explained what a focus group session entails and started the conversation. First, we asked participants whether their Web use had undergone any major changes in the past few years, followed by a similar question about sharing content and using social media like Facebook.

Rather than imposing a definition of “privacy” on the group, we asked participants what privacy meant to them and how they would define it. We then asked to what extent participants felt that they had control over their personal data. We inquired into their knowledge of recent privacy-related events such as Edward Snowden’s leaks of the U.S. National Security Agency’s classified information, which had occurred a year prior to our interviews (Landau, 2013), and the Heartbleed security bug incident, which had come to light a few weeks prior to our study, and concerned the vulnerability of sensitive information online such as passwords (Randall, 2014). We also discussed privacy-related policies such as the “Right to be Forgotten” law in the European Union (Court of Justice of the European Union, 2014; Jones, 2016), which gives individuals the right to ask search engine companies to remove links to, and listings of, material about them on third-party websites from search results pages. Finally, we discussed whether participants might feel more in control or more comfortable online with technological or policy innovations. With some questions, we went around the room and asked that everybody respond. With others, we let the conversation flow among participants as they saw fit. All sessions were audio recorded and then transcribed.

Analysis

The survey data were entered into online forms. These resulted in spreadsheets imported into a statistical program that allowed us to aggregate figures about participants' background and Internet experiences, as detailed next. After transcribing the interview sessions, we split up the text by general topic. Interview questions were grouped by topical focus (e.g., definition of privacy, social media experiences and expectations, policy know-how). We then combined all the interview material by theme into one document. We read through the thematic sections and highlighted especially illustrative and representative quotations. Both authors and a research assistant participated in this analysis.

Participants

Since the privacy paradox is typically discussed in regard to young people, we chose university students for the study. Participation was limited to undergraduate and graduate students to control for some level of education. Most participants were college undergraduates: some (12%) had just completed their first year, just over a third (35%) had finished their sophomore year, some (12%) had completed their junior year, and some (18%) had recently graduated. The remaining 23% of participants were in a graduate program at the time of the study. All the graduate students were from one institution. Of the undergraduate students, three were enrolled at other Midwestern schools at the time of the study and two were visiting from schools in the Northeast.

Half the participants were between the ages of 19 and 21 (50%), whereas 27% were between 22 and 24, 13% were between 25 and 30, and 10% were between 31 and 35. Most participants were White (65.9%), followed by Asian American (19.5%), African American (9.8%), and Hispanic students (4.9%). The majority of participants came from a highly educated family, as over two-thirds had at least one parent with a graduate degree (68%), 22% had at least one parent with a college degree, and only 10% had parents who had not completed college. Just over a third of interviewees were in the humanities (35%), just under a third in the sciences (30%), just under a fifth in the social sciences (18%), and a similar proportion in journalism and communication (17%). While we did not see a difference among participants by gender, we specify age and gender for context in the excerpts that follow.

Internet Experiences

All participants were Internet users, and all but one reported having Internet access on their phone, meaning these users had continuous access to digital media. To determine whether privacy on social media was relevant to participants' online experiences, we asked them whether they had heard of various services and whether they used them currently or had used them in the past. All participants had heard of Facebook, Twitter, LinkedIn, Instagram, and Google Plus, and all but one had heard of Snapchat, Tumblr, Pinterest, and Flickr. Even the least known service in our sample, Foursquare, was familiar to 87.5% of focus group participants. Familiarity with a site or app, however, did not necessarily translate into using it. The only site that every participant had used at one point was Facebook, followed in popularity by Twitter (67.5%), Snapchat (65%), LinkedIn (52.5%), Instagram (40%), Tumblr (37.5%), Pinterest (17.5%), Google Plus (15%), Foursquare (5%), and Flickr (5%).

The survey included information about participants’ Internet skills, both general (Hargittai, 2005) and privacy specific (Hargittai & Litt, 2013; Park, 2013). Since skills are of central concern to the research questions, we wanted to establish baseline measures and determine whether there was any level of variation in respondents’ understanding of the Internet. The general skills measure can range from 1 to 5; the range in the sample was 2.3–5 with a mean of 3.47 (SD = .77), which is very similar to the skills measure of a different young adult group of 547 respondents who were 22–23 years old at the time (Mean= 3.46, SD = .80) (Hargittai & Litt, 2013). This suggests that our study participants were not outliers in their level of general Internet skills relative to their age cohort and levels of education.

Regarding privacy-specific skills, we replicated the measure used by Hargittai and Litt (2013) and found that our respondents were savvier (Mean = 4.04; SD =.61) in this domain than the 547 participants in the previously mentioned study, which relied on data from 2012 (Mean = 3.78, SD =.79). We also asked some of Park’s (2013) true–false questions about knowledge of institutional privacy policies and practices. Just under half of our participants got all five questions right; a quarter missed one, a quarter missed two, and one person missed three out of five statements. This suggests that our participants were more knowledgeable about privacy matters, on average, than Park’s 419 nationally representative adults of all ages. Perhaps this is not surprising, however, given that Park collected his data in 2008 and public discussion of privacy issues has increased considerably since that time (boyd & Hargittai, 2010). Finally, we included two multiple-choice questions related to privacy matters. First, we asked, “What is Google Glass?” which most (87.5%) participants answered correctly. Second, we asked, “What is an Internet cookie?” which just over half (55.0%) of participants identified correctly. We also inquired whether participants had “ever taken a course that covered questions of privacy and/or surveillance” and a quarter reported having done so, six in the immediate past year, and four in a prior year. It is interesting that, having taken such a course is not correlated with our various privacy skill indicators. These measures imply that our participants were fairly knowledgeable about the Internet but varied in their know-how.

To see whether participants might have reason to be concerned about privacy, the survey asked whether they or somebody they knew had experienced negative consequences due to something that they or someone else had posted on the Internet. The majority (70%) answered affirmatively, with up to five negative experiences. When including data about the experiences of someone they knew—which is relevant as people may not always be conscious of the consequences of their own actions or may refrain from reporting them due to social desirability—all but one person reported that someone they knew had experienced negative consequences. The most frequent negative experience concerned embarrassment (94.6%), followed by feelings of betrayal and hurt (75.7%), problems with a job application (73%), trouble with family (73%), a fight with someone (67.6%), trouble at school or on the job (56.8%), the end of a friendship (43.2%), a romantic breakup (37.8%), and legal consequences (16.2%). These responses suggest that most of our participants or someone they knew had experienced negative consequences of content shared about them online, whether by themselves or others, and thus would have reason to give thought to privacy considerations. Our Internet skill measures show a range of know-how among participants, including several highly skilled users, while almost everyone in the study had had negative experiences with privacy-related issues online. This suggests that skills are not the only issue at hand when handling the exposure of one's personal information online. To see whether this was indeed the case, we turned to our interview data.

Findings

Knowledge About Privacy and Risks

Our first research question asked what participants knew about privacy online. As demonstrated by the survey responses, study participants had more knowledge about privacy than both nationally representative samples and samples of similar age and educational background. However, this understanding was not necessarily sophisticated or accurate. In line with previous studies, respondents demonstrated a range of privacy knowledge about topics such as privacy policies, targeted advertising, website information collection, and U.S. privacy laws. Focus group questions about privacy-related current events such as the Edward Snowden revelations and the Heartbleed bug elicited varying responses, with many members professing little to no familiarity with these issues. For instance, one woman (34) said about Snowden:

> I wish that I had done a little more reading about him, maybe, that, you know, and sort of what he found beyond what was being posted on Facebook by my friends. So I feel a little undereducated and maybe I would've changed my behavior if I had actually done more research, but I didn't. And I haven't.

This suggests that a typical person's understanding of privacy practices may be quite different from that of privacy scholars and advocates.

Our survey data also suggested that participants were well aware of the risks of sharing information online, since most had experienced a negative consequence or knew someone who had. It is interesting that in the discussions there was more focus on the social risks of sharing information, such as embarrassment or conflict with friends, family, or romantic partners, than institutional risks from technology companies, marketers, or law enforcement.[2] One woman (21) described her attitude in this way:

> When I think of online privacy, I think more of, not the threat of people stealing your identity and ruining your financial situation, but . . . more like what an individual would do to another individual, like finding out dark secrets. *[She clarified that by "dark secrets" she meant risqué photos.]*

[2] This distinction between social and institutional privacy is inexact but nonetheless useful in distinguishing consequences within personal social networks (things like embarrassment and romantic tension) from those caused by governments, employers, educational institutions, and so forth. See Raynes-Goldie (2010).

While social risks were clear, many participants were unclear as to what institutional risks might be beyond the financial. Another woman (20), discussing Heartbleed, said:

> It didn't completely seem worth it to me to change all my passwords that I remember. Because . . . I don't really care if somebody gets a hold of my Facebook, like I don't have anything with credit cards really linked . . . the most they could do would be to delete my content, which would be kind of sad for me, but, I dunno.

Similarly, a 20-year-old woman said:

> I don't really read the fine print, I'm sort of like apathetic in a sense because I don't know what the worst thing that can happen is besides shooting dirty spam mail off my email account or something, that's the worst thing I've seen happen to anyone I know. So it's hard to be really invested as a user, for me at least.

While this apparent lack of concern would seem to support the idea of a privacy paradox, it seems instead that our participants were concerned and knowledgeable about the risks of social privacy violations but had little concrete experience with other types of privacy violations.

Similarly, several respondents saw a clear distinction between personal information they considered harmless, and information such as credit card numbers or health records that could have more malicious impact if leaked:

> The criterion is always: can that information come back to hurt you? And so, what . . . books and movies I browse for on Amazon, I can't see any harm in that, but health information starts crossing that line into, well, is an employer gonna discriminate against you because you have a history of depression or something like this? So if it's any kind of information that you could see coming back to actually hurt you, that's where I draw the line at sharing it online. (Female, 27)

Other students agreed that they might care more about online privacy as they got older and were concerned with health or employment records. These findings support previous research that the blanket operationalization of "online information provision" as a lack of concern for privacy is misguided. It is more accurate to say that our participants were concerned with particular types of information. One man (20) explained, "I think that any passwords, codes that you know, this one string of letters and numbers, if you have that you have access to my entire bank account information. Anything like that is personal data and private information."

Lack of Control and Networked Privacy

Our second question asked to what extent people feel that there are social advantages to sharing personal information online even if such content might compromise their privacy. Many participants acknowledged that they lacked control over personal information posted online, especially on Facebook.

While they were not always clear on exactly how this happened, they knew that information leaked beyond its intended origins. One man (22) said:

> On Facebook, I think it's been drilled into me that you just have to assume anything you post is public. You can set your privacy settings at the strictest you want, but you just have to assume that anything you put out there can be made public to the world.

A female graduate student (33) concurred:

> I categorize it with some talk that I got in middle school about talking behind someone's back. You can think you're behind their back but you ultimately don't really have control over it, so . . . even if I said, "Okay, only the group of grad student peers can see us, " or whatever I can—I mean, I don't understand how the Internet works all that well, but I can imagine, even in sort of my rough way, a scenario where somebody would see it and it would just be out. No good. So I'd rather just not post it.

This student recognized that even if she set up a private Facebook group to discuss personal issues, it was likely that someone excluded from the filter might see the content anyway. It was easier, then, just not to post it.

Participants recognized that privacy is networked (Marwick & boyd, 2014)—in other words, that well-meaning family and friends could contribute to violating one's privacy, even unintentionally. One woman (21) explained:

> It's not only your privacy because on your social media activity or whatever website activity you're doing, you're relating a lot to the people you are close with, around with. For example, if you're in a relationship with someone, and if you indicate that on Facebook even if it's not your friends, everyone who searches for you can know that. So I feel like it's also related to your friends' and family's privacy too.

A 21-year-old male bemoaned that he came from "a family of oversharers" and that even though he chose to share very little online, someone could learn a great deal from what his family said about him. In other words, while the privacy paradox focuses on individual self-presentation of personal information, participants were cognizant that the maintenance of privacy was in many ways a collective process that was out of their control (Litt, Spottswood, Birnholtz, Hancock, & Reynolds, 2014).

Many focus group participants demonstrated a sophisticated understanding of how other people's Facebook privacy settings might affect them. One woman (34) said:

> I have a group of close friends [whom] I post the majority of my posts to, but I know that if they have their settings set to public, things that I post that they like or that they comment on will become public.

As a result, in an attempt to maintain privacy, respondents reported trying to manage the behavior of others. For example, one female (19) explained that at parties, “I’m always like, ‘Okay guys, don’t tag me!’ before we take pictures, ‘Please don’t tag me!’ Like I don’t want people knowing I party every night, let’s just keep this DL, down low.” However, participants recognized that this was often futile, as exemplified by this comment from a 34-year-old woman:

> I have friends who are not really paying attention to their privacy settings at all, which is totally up to them, but as soon as something gets shared from them or liked by them, too . . . I don’t have any control over that. I’m not gonna contact each of my friends and be like, “Fix your privacy settings!” You know, it’s not my job, fortunately.

One graduate student (28) made the group laugh in recognition when she discussed how the different people in her life might react to the request not to be tagged:

> I think it really depends who your family and friends are [sounds of amusement from group]. I think some people would be responsive to you saying, “Oh, please don’t tag me,” and others would be like, “I’ll just tag you, you don’t have to approve it,” then it’s kind of like, “Well, it’s available to all the people you know, but I can make sure that maybe five people don’t see it,” but that’s not really helpful.

These quotes suggest that at least some respondents understood Facebook’s privacy settings well; it is precisely because they understood them—and how they interacted with their social groups—that they grasped the system’s limitations.

Moreover, several participants discussed how Facebook’s privacy settings were liable to change at any moment, which made it even more difficult to maintain control over information. One male graduate student (32) explained:

> I feel like it’s a losing battle, like it changes so quickly. I could be like, “Yeah, I want to take an hour and a half out of my life to read privacy statements on Facebook and configure all that.” After not using it for two years and getting back on I’m like, “This is so freaking complicated,” it’s like, “Whoa, whoa, whoa, this used to be so simple!” but now there’s all these dropdown menus like, “[Whom] do you share this with?” so I really don’t have any faith that even if I do what [another focus group participant] says and select who I share it with, I don’t have any faith, that like how do I know I’m not missing some—like, “Oh, sorry, it’s shared with my friends of my friends” who then share with people?

Students were realistic that Facebook’s combination of difficult-to-manage technical affordances, networked privacy, and constantly changing settings made it very challenging, if not impossible, to maintain the level of privacy they desired. In response, they adopted a variety of creative privacy-protective practices, on Facebook and off, with varying degrees of success.

Responsibility

Our third research question asked to what extent young people believe they are responsible for keeping personal information private. In our sessions, respondents debated whether individuals, corporations, a hypothetical nonprofit, or the government were ultimately responsible, but they were unable to come to a conclusion. Some participants like this 26-year-old female believed that it was the individual's responsibility to keep private information off the Internet in the first place:

> We're talking about direct responsibility, right? For me, it's like if you want to put things out there, you have zero control of that thing, so if you . . . don't want it to go around, do not put anything at all. So, it's all about your own control. You decide to put things out there, and once it's out there, it's out there.

This perspective, which was echoed by others, assumed a dichotomy in which information could only be kept private if it was entirely absent online, presuming that privacy-protective behaviors such as filters or privacy settings were ineffectual and that self-editing was the only effective tactic (discussed in the next section).

The most common viewpoint expressed by participants was that once an individual chose to share personal information, the technology company was responsible for keeping it secure:

> Whatever service you're using, they need to make sure that I have clear understanding of what [the service is going to do with one's personal information], and I'm not hearing like some story that you're actually doing something different than what you're telling me. (Male, 23)
>
> I think as long as there's a way for an individual to [protect their information], it's their responsibility. So if there are privacy controls on a website, if you don't take action to set the ones that you want, then that's your own fault, but if a website doesn't provide something that maybe you need to feel controlled or safe, then I think that's the website's responsibility. (Female, 22)

Others complicated the idea of individual responsibility by recognizing the power differential between individuals and companies. One man (32) said, "I'm really [made] uncomfortable by the idea that we need to be vigilant to whatever crazy privacy loopholes companies are making us jump through to help us." Another male (22) pointed out that "there's a lot of fine print that makes it extremely difficult as a user to have that sort of agency over your information," and still others mentioned that technology companies had a vested interest in encouraging people to provide personal information.

A smaller group of respondents believed it was the government's responsibility to ensure adherence to privacy regulations or expressed the desire for stronger privacy legislation. One young woman (21) said wistfully, "It's partly an individual thing, but partly also a, I don't know, government thing, too. Like there needs to be some kind of oversight, I think, in terms of making sure that people know exactly what information of theirs is being shared, what’s being captured.” This opinion was viewed as overly idealistic; in several sessions, the European Union’s “Right to Be Forgotten” decision was dismissed as unrealistic and impractical.

While participants did not come to a consensus about who held responsibility for keeping personal information private, they overwhelmingly believed that their privacy could, and would, be violated as long as they posted information online. Do participants know, then, how to protect their privacy online? The next section examines the types of skills on which respondents draw to safeguard their online actions.

Privacy-Protective Behaviors

Our fourth research question asked how skilled participants are at online privacy protection and what they actually do to protect their privacy online. Students mentioned a vast array of privacy-protective behaviors, some sophisticated and others less so, with some participants stating outright that they do not understand how the Internet works. The strategies included using different sites and apps for different purposes, configuring settings on social network sites, using pseudonyms in certain situations, switching between multiple accounts, turning on incognito options in their browser, opting out of certain apps or sites, deleting cookies, and even using Do-Not-Track browser plugins and password-management apps. These strategies were highly individual and varied among users.

> The way I share content has become a lot more targeted. Instead of putting it on Facebook for a thousand people to see, it becomes a lot more targeted and I’ll email pictures or something to a specific set of people or I’ll snapchat it to a specific set of people, but . . . it has less of a reach now. (Female, 22)

> I use my name when it comes to Facebook and Instagram ’cause I do it for connecting with family because they’re all distributed, and I have friends, like international friends, that are like really far away and I want to talk to them. . . . But when it comes to Twitter, yeah, I don’t use my real name, because I just tweet nonsense or like about my daily life and it’s like I don’t want you to know that about me personally, it’s just like I’m bored, I’m trying to entertain myself so I’m just going to speak. (Female, 19)

Some respondents were well aware of the uncertain efficacy of these practices. One woman (28) explained, “I use the . . . Google . . . they have the Incognito box that I try to use, but I don’t know the extent of how helpful it is. But I figure it is an easy thing for me to do, so I’ll do that.” A man (20), discussing password-storage apps, remarked:

> I know there are apps on your phone where a password keeper keeps track of all the different passwords for different sites and stuff like that, and I’ve always been hesitant and all my passwords tend to be a riff or variation of the same password, which I think a lot of people do, which is probably not very smart . . . so I thought, oh, I could change up my passwords and make them very different for each site, and then put them all in a password keeper or something like that, but then I still think . . . this third party might

> be good on paper, but who's to say that the people running it or one person who has access behind the scenes to all that isn't a sketchy guy trying to get my information?

This is indicative of the cynicism revealed through several respondents' comments about the effectiveness of even well-intentioned privacy-enhancing technologies (discussed in the next section).

While virtually all our participants had adopted different approaches to protecting privacy, the only widely agreed-upon technique was self-censoring, or leaving information off the Internet entirely. One female graduate student (33) explained:

> I think there's a privacy setting issue in terms of managing, but there's also the human privacy setting in the sense that you feel constrained to actually just not say stuff. In addition to the privacy setting, there's always, there's also—at least for some people—some amount of inhibition about saying it publicly in the first place. There's kind of a computer privacy setting and also like a privacy setting in your brain.

Respondents mentioned several categories of information that they would not post online: political beliefs, "emotional things," pictures of exes, articles that other people had already shared, anything "unprofessional," and "duck-face selfies," to name a few. These findings are concurrent with those of Sleeper et al. (2013) and Vitak, Lampe, Gray, and Ellison (2012), who found that self-censorship on social media was a common social strategy to avoid embarrassment or conflict.

Simultaneously, participants extolled the benefits of social media sites for staying in touch with friends and family, keeping up with schoolwork, and participating in student groups:

> As for me, I'm living abroad because I'm from [country of origin]. My class, we are about like 84 people in the class, and we have our own Facebook page where we share logistical information and then sometimes how to get our assignments done. . . . I don't check my Facebook every few hours, I'm already out of the loop with other people, so I think I observe that I use more nowadays [than in college] and I see myself checking every few minutes actually. (Female, 26)

"Opting out" was viewed as unrealistic, given the likely resulting social consequences. One respondent (20) explained that Facebook boosted his "whole social clout that affects you in the real world offline, and so I find a heightened use because of making connections with other students this year." This is supported not only by studies that find a link between Facebook participation on campus and social capital (Ellison, Steinfield, & Lampe, 2007, 2011), but also by explanations for the privacy paradox that discuss the importance of social media to young people's lives (Taddicken, 2014).

Apathy and Cynicism

Recognizing the difficulties stemming from networked privacy, the inevitability of privacy violations, and the necessity of using social media made some participants express resignation about privacy violations and a lack of ability to change this situation.

> I feel like [pause], then you have the choice between not using the Internet and therefore keeping free of the surveillance, or living with it. So, I do care [about privacy]; but I guess I don't care enough not to use the Internet. And I'm not sure what the alternative is at the moment. (Female, 21)

Another respondent (21) knew that there were options available to help him protect his privacy but was unclear of how to use them:

> I know there's like certain browsers, and proxies, and things—that may not even be the correct term. I read [an article about privacy] but then like obviously I was like, "Oh, that sounds like too much work." [laughs] But, so I feel like there are—in terms of keeping third parties from seeing data you don't want them to see or data in general, I feel like there's more options than with other issues regarding Internet security and privacy. But I still haven't paid attention to what those options are, and I still don't know the extent of the problem.

These attitudes could come across as quite cynical. A 21-year-old female respondent said gloomily, "In terms of serious privacy control, I never feel like I've lost something. I just feel like I've never had it to begin with, which is kind of interesting." A male (35) simply stated: "Cynically, there's no privacy." These attitudes may appear apathetic, implying support for the privacy paradox.

We suggest two alternative explanations. First, participants were well aware of the likelihood of social privacy violations, given their knowledge of, and experience with, a variety of negative consequences from information shared on social media. This is partly due to the existence of networked privacy, partly due to constantly changing privacy settings, and partly due to the affordances of social network sites, which made respondents dependent on how friends and family configured their settings. Thus, in their experience, and given these conditions, privacy violations are inevitable. The only way to prevent privacy violations was to opt out entirely—which was disregarded as unrealistic—or to refrain from posting certain types of information online in the first place. Second, many of our participants with lower technical skills knew they were at a tactical disadvantage and thus believed they could do little to keep themselves safe from hackers or identity thieves:

> I don't consider myself a tech-savvy person and so just the idea of there being people out there who just with a computer in front of them can hack this database or get my information, to some extent, I think like, "Oh I better add a few random numbers in this password," or do this or that, but you know besides that I'm also wondering, what can I really do? (Male, 20)

This is entirely sensible given the prevalence of information breaches, such as the exposure of over 100,000 tax returns in a hacker attack on the Internal Revenue Service (Pagliery, 2015), the cyberattack revealing 80 million of Anthem's insurance records (Weise, 2015), and the hack of 145 million records from eBay (Peterson, 2014). Many such breaches involve extremely personal information, such as social security numbers, health records, and credit card numbers. Similarly, Edward Snowden's revelations of the National Security Agency's data-collecting practices make attitudes that may have been dismissed as paranoid a few years ago seem eminently pragmatic today:

> But in the event that I become a person of interest, I think that I lose every privacy—I never had any privacy, but I lose any kind of mystery about me. When someone decides that they want to or the government especially decides that they want to learn who I am, they can. (Male, 22)

Notably, this cynicism does not stop young people from engaging in privacy-protective behaviors; rather, it engenders a type of resigned pragmatism in which young people are aware their privacy may be violated at any minute and that there is little they can do about it, but that there are things they can do to make losing control of their information more difficult (see also Turow, Hennessy, & Draper 2015). This is quite different from the assumption that "young people don't care about privacy."

Conclusion

While our focus group data do suggest some lack of understanding of risk, misunderstandings around the efficacy of certain privacy-protective behaviors, and lack of knowledge of privacy-related current events, several participants demonstrated knowledge and use of a variety of privacy-protective behaviors. The simultaneous presence of lack of knowledge of risk and use of privacy-protective behaviors suggests that the privacy paradox cannot be attributed solely to either a lack of understanding of or a lack of interest in privacy.

Instead, participant comments suggest that users have a sense of apathy or cynicism about online privacy, and specifically believe that privacy violations are inevitable and opting out is not an option. We explain this apathy using the construct of networked privacy (Marwick & boyd, 2014), which suggests that in highly networked social settings, the ability of individuals to control the spread of their personal information is compromised by both technological and social violations of privacy. Privacy is not an individual process, but rather a collective effort that requires the cooperation of those with whom we connect on social media, as well as the technological affordances of the social media sites themselves. Understanding this, young adults turn to a variety of imperfect, but creative, social strategies to maintain control and agency over their personal data. While participants engaged in a range of privacy-protective behaviors, they recognized that these were likely insufficient in the face of online data mining, widespread identity theft, ever-changing privacy settings, and highly networked social situations.

Our data suggest that the existence of fatigue surrounding online privacy and the simultaneous presence of concern over privacy and widespread self-disclosure is not necessarily paradoxical, but rather a pragmatic response to the contemporary networked social environment, given existing U.S. policy and corresponding business-sector affordances. Specifically, there is no comprehensive online privacy protection in the United States. Instead, privacy laws exist in silos; there are laws that govern health records, educational records, and even video rental records, but no laws that specifically protect social media profiles or health data collected by wearables or fitness apps, for instance (Angwin, 2014). As a result, individuals have little legal protection from employers, data brokers, or even law enforcement accessing their personal data. The current patchwork of privacy regulations in the United States is inadequate and remains one step behind technological development. Comprehensive data protection laws that apply across domains could provide a framework for emerging technologies, and ease the minds of people worried about how their data are being used.

The existing technical functionality of social media makes it very difficult for individuals to regulate how their information flows from person to person, and the privacy controls available change frequently and are often confusing. The assumption behind the existing opaque system is that businesses thrive on users sharing as much content as possible, and so do not benefit from clearer, more user-friendly options. The result of the current arrangement, however, is frustration that yields both apathy as well as self-censorship. That is, as users understand their lack of control over their information, they retreat in certain ways when it comes to sharing. Thus, it is not paradoxical that young people want to share information about themselves while simultaneously recognizing the inability of technical solutions or social norms to protect their privacy adequately. In addition to clearer systems and better privacy regulation, more focus on an informed user based could address some of the concerns that stem from networked privacy. Recognition of the types of privacy-protective behaviors that are more or less effective might result in fewer potential repercussions from sharing content.

References

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *Lecture Notes in Computer Science*, *4258*, 36–58.

Angwin, J. (2014). *Dragnet nation: A quest for privacy, security, and freedom in a world of relentless surveillance*. New York, NY: Times Books.

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First* Monday, *11*(9). Retrieved from http://firstmonday.org/article/view/1394/1312

Blank, G., Bolsover, G., & Dubois, E. (2014). A new privacy paradox: Young people and privacy on social network sites. American Sociological Association Annual Meeting, San Francisco, CA. Retrieved from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2479938

boyd, d., & Ellison, N. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1). Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2008.00408.x/full boyd, d., & Hargittai, E. (2010). Facebook privacy settings: Who cares? *First Monday*, *15*(8). Retrieved from http://firstmonday.org/article/view/3086/2589

Chang, C-W., & Heo, J. (2014). Visiting theories that predict college students' self-disclosure on Facebook. *Computers in Human Behavior*, *30*, 79–86. doi:10.1016/j.chb.2013.07.059

Court of Justice of the European Union. (2014). *Press release No 70/14*. Luxembourg. Retrieved from http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf

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 from http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1849&context=amcis2007

Ellison, N., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication*, *12*(4). doi:10.1111/j.1083-6101.2007.00367.x

Ellison, N., Steinfield, C., & Lampe, C. (2011). Connection strategies: Social capital implications of Facebook-enabled communication practices. *New Media & Society*, *13*(6), 873–892. doi:10.1177/1461444810385389

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*. New York: ACM Press, 71-80. doi:10.1145/1102199.1102214

Hargittai, E. (2005). Survey measures of Web-oriented digital literacy. *Social Science Computer Review*, *23*(3), 371–379. doi:10.1177/0894439305275911

Hargittai, E., & Litt, E. (2013). New strategies for employment? Internet skills and online privacy practices during people's job search. *IEEE Security & Privacy, 11*(3), 38–45. doi:10.1109/MSP.2013.64

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How different are young adults from older adults when it comes to information privacy attitudes and policies? Berkeley, CA: University of California, Berkeley. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864

Jones, M. L. (2016). *Ctrl + Z: The right to be forgotten*. New York: NYU Press.

Jones, S., Johnson-Yale, C., Millermaier, S., & Perez, F. S. (2009). Everyday life, online: U.S. college students' use of the Internet. *First Monday, 14*(10). Retrieved from http://firstmonday.org/article/view/2649/2301

Kornblum, J. (2007, October 22). Online privacy? For young people, that's old-school. *USA Today*. Retrieved from http://usatoday30.usatoday.com/tech/webguide/internetlife/2007-10-22-online-privacy_N.htm

Kumaraguru, P., & Cranor, L.F. (2005). Privacy indexes: A survey of Westin's studies. Institute for Software Research International, Carnegie Mellon University. Retrieved from http://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf

Landau, S. (2013). Making sense from Snowden: What's significant in the NSA surveillance revelations. *IEEE Security Privacy*, *11*(4), 54–63. Retrieved from https://www.computer.org/csdl/mags/sp/2013/04/msp2013040054-abs.html

Litt, E. (2013). Understanding social network site users' privacy tool use. *Computers in Human Behavior, 29*(4), 1649–1656. doi:10.1016/j.chb.2013.01.049

Litt, E., Spottswood, E., Birnholtz, J., Hancock, J. T., & Reynolds, L. (2014). Awkward encounters of an "other" kind: Collective self-presentation and face threat on Facebook. *Proceedings of CSCW 2014*, 449–460. doi:10.1145/2531602.2531646

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society, 10*(3), 393–411. doi:10.1177/1461444808089415

Madden, M., Lenhart, A., Cortesi, S., & Gasser, U. (2013). Teens and mobile apps privacy. Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/2013/08/22/teens-and-mobile-apps-privacy/

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A., & Beaton, M. (2013). Teens, social media, and privacy. Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/2013/05/21/teens-social-media-and-privacy/

Madden, M., & Rainie, L. (2015). Americans' attitudes about privacy, security and surveillance. Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Marwick, A. (2008). To catch a predator? The MySpace moral panic. *First Monday, 13*(6). Retrieved from: http://firstmonday.org/article/view/2152/1966

Marwick, A., & boyd, d. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society, 16*(7), 1051–1067. doi:10.1177/1461444814543995

Marwick, A., Murgia-Diaz, D., & Palfrey, J. (2010). Youth, privacy and reputation (literature review). Cambridge, MA: Berkman Center for Internet & Society at Harvard University. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163

Nussbaum, E. (2007, February 12). Kids, the Internet, and the end of privacy. *New York Magazine*. Retrieved from http://nymag.com/news/features/27341/index7.html

Pagliery, J. (2015, May 26). Criminals use IRS website to steal data on 104,000 people. *CNNMoney*. Retrieved from http://money.cnn.com/2015/05/26/pf/taxes/irs-website-data-hack/

Park, Y. J. (2013). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215–236. doi:10.1177/0093650211418338

Peterson, A. (2014, May 21). eBay asks 145 million users to change passwords after data breach. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/

Quinn, K. (2016). Why we share: A uses and gratifications approach to privacy regulation in social media use. *Journal of Broadcasting & Electronic Media*, *60*(1), 61–86. doi:10.1080/08838151.2015.1127245

Rainie, L., & Madden, M. (2015). Americans' privacy strategies post-Snowden. Washington, DC: Pew Research Center. Retrieved from http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/

Randall, M. (2014). *Heartbleed explanation*. Retrieved from https://xkcd.com/1354/

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1–4). Retrieved from: http://firstmonday.org/article/view/2775/2432

Schrock, A., & boyd, d. (2008). Online threats to youth: Solicitation, harassment, and problematic content. Cambridge, MA: Berkman Center for Internet & Society at Harvard University, 62–142. Retrieved from http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/RAB_Lit_Review_121808_0.pdf

Sleeper, M., Balebako, R., Das, S., McConahy, A. L., Wiese, J., & Cranor, L. F. (2013). The post that wasn't: Exploring self-censorship on Facebook. *Proceedings of CSCW 20'13,* 793–802. doi:10.1145/2441776.2441865

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. *Proceedings of the 3rd ACM conference on Electronic Commerce*, 38–47. New York, NY. doi:10.1145/501158.501163

Steeves, V., & Webster, C. (2008). Closing the barn door: the effect of parental supervision on Canadian children's online privacy. *Bulletin of Science, Technology & Society, 28*(1), 4–19. doi:10.1177/0270467607311488

Stenger, T., & Coutant, A. (2010). How teenagers deal with their privacy on social network sites? Results from a national survey in France. *AAAI Spring Symposium: Intelligent Information Privacy Management.* Retrieved from http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1079

Stutzman, F., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of Privacy and Confidentiality, 4*(2): Article 2. Retrieved from http://repository.cmu.edu/jpc/vol4/iss2/2/

Taddicken, M. (2014). The "privacy paradox" in the social Web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure*. Journal of Computer-Mediated Communication, 19*(2), 248–273. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/jcc4.12052/abstract

Thelwall, M. (2008). Social networks, gender, and friending: An analysis of MySpace member profiles. *Journal of the American Society for Information Science and Technology, 59*(8), 1321–1330. doi:10.1002/asi.20835

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. doi:10.1177/0270467607311484

Turow, J., Hennessy, M., & Draper, D. (2015). The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. Philadelphia, PA: The Annenberg School for Communication, University of Pennsylvania. Retrieved from https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Vitak, J., Lampe, C., Gray, R., & Ellison, N. B. (2012). Why won't you be my Facebook friend?: Strategies for managing context collapse in the workplace. *Proceedings of the 7th Annual iConference,* 555–557. Ontario, Canada. doi:10.1145/2132176.2132286

Weise, E. (2015, February 5). Massive breach at health care company Anthem Inc. *USA Today.* Retrieved from http://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/

Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: A risk–benefit appraisal approach. *Journal of Broadcasting & Electronic Media, 49*(1), 86–110. doi:10.1207/s15506878jobem4901_6