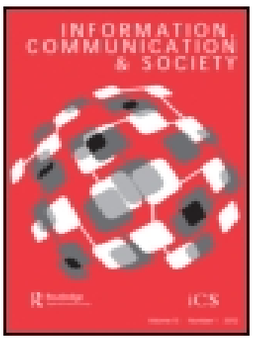
Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online

Marwick, Alice ; Hargittai, Eszter

Abstract: What incentives and disincentives do Internet users weigh as they consider providing information to institutional actors such as government agencies and corporations online? Focus group participants list several benefits to sharing information including convenience, access to information, personalization, financial incentives, and more accurate health information, but also recognize that not all sharing may be in their interest. Disincentives to sharing include skepticism, distrust, and fears of discrimination. Decisions about sharing are related to the information type, the context in which information is revealed, and the institution to which they are – or think they are – providing information. Significantly, many participants were mistrustful of both governmental and corporate actors. Participants displayed awareness of privacy risks, but frequently mischaracterized the extent to which information could be aggregated and mined. They displayed resignation towards privacy violations, suggesting that they perceived little control over their ability to protect their privacy, which may influence their privacy behaviors. This calls into question the privacy calculus, as individuals misunderstand the risks of their information provision and do not believe opting out of information-sharing is possible.

DOI: https://doi.org/10.1080/1369118x.2018.1450432



Routledge
Taylor & Francis Group

Information, Communication & Society

ISSN: 1369-118X (Print) 1468-4462 (Online) Journal homepage: https://www.tandfonline.com/loi/rics20

Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online

Alice Marwick & Eszter Hargittai

To cite this article: Alice Marwick & Eszter Hargittai (2018): Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online, Information, Communication & Society, DOI: 10.1080/1369118X.2018.1450432

To link to this article: https://doi.org/10.1080/1369118X.2018.1450432

INFORMATION, COMMUNICATION & SOCIETY, 2018
https://doi.org/10.1080/1369118X.2018.1450432

Routledge
Taylor & Francis Group

Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online

Alice Marwick[a] and Eszter Hargittai[b]

[a]Department of Communication, University of North Carolina, Chapel Hill, NC, USA; [b]IKMZ, Institute of Communication and Media Research, University of Zurich, Zurich, Switzerland

ABSTRACT

What incentives and disincentives do Internet users weigh as they consider providing information to institutional actors such as government agencies and corporations online? Focus group participants list several benefits to sharing information including convenience, access to information, personalization, financial incentives, and more accurate health information, but also recognize that not all sharing may be in their interest. Disincentives to sharing include skepticism, distrust, and fears of discrimination. Decisions about sharing are related to the *information type*, the *context* in which information is revealed, and the *institution* to which they are – or think they are – providing information. Significantly, many participants were mistrustful of both governmental and corporate actors. Participants displayed awareness of privacy risks, but frequently mischaracterized the extent to which information could be aggregated and mined. They displayed resignation towards privacy violations, suggesting that they perceived little control over their ability to protect their privacy, which may influence their privacy behaviors. This calls into question the *privacy calculus*, as individuals misunderstand the risks of their information provision and do not believe opting out of information-sharing is possible.

ARTICLE HISTORY
Received 29 August 2017
Accepted 22 February 2018

KEYWORDS
Information provision; privacy calculus; privacy paradox; institutional privacy

Concerns around online information privacy have multiplied in the last decade (Smith, Dinev, & Xu, 2011; Solove, 2008; Trepte & Reinecke, 2011). Data provided to private companies are susceptible to data breaches and being aggregated by data-brokers (Schneier, 2015; Turow, 2017). Moreover, Edward Snowden revealed in 2013 the scale and scope of the US government's investment in collecting the personal data of its citizens (Mills, 2015). Research demonstrates that people are concerned with the effect of online information on employment and education, while simultaneously acknowledging their inability to control what information friends and family disclose about them (Hargittai & Marwick, 2016; Vitak, Blasiola, Patil, & Litt, 2015). Despite these anxieties, people continue to use online technologies that require the provision of personal information. As a result, many scholars identify a disconnect between privacy concerns and privacy behavior, dubbed the privacy paradox (Barnes, 2006; Kokolakis, 2015; Norberg, Horne, & Horne,

CONTACT Alice Marwick amarwick@gmail.com Department of Communication, University of North Carolina, CB# 3285, 115 Bingham Hall, Chapel Hill, NC 27599-3285, USA

2007). In other words, while people voice concerns about privacy, they nevertheless willingly provide personal information to websites and mobile apps. Research explains this through the *privacy calculus* model in which individuals rationally weigh the risk of privacy violations against the benefits of engaging online (Pavlou, 2011; Smith et al., 2011).

It is important to note, however, the context in which information is provided and to whom or what it is provided, since what is considered appropriate to disclose depends on context and audience (Li, Sarathy, & Xu, 2010; Litt, 2012). Raynes-Goldie distinguishes between social privacy – limiting other people's access to information – and institutional privacy, or limiting companies' or government access to information (2010). Previous qualitative research has examined the strategies young people use to maintain *social* privacy in the face of widespread social media use (Marwick & boyd, 2014; Hargittai & Marwick, 2016; Tufekci, 2012; Young & Quan-Haase, 2013). This paper uses data from 10 focus groups administered in 2014, totaling 40 participants ages 19–35, to investigate what factors influence whether young people provide, or share, information with *institutions* online, including private companies, government websites, health care websites, and e-commerce sites. What risks and benefits do young adults see when choosing to share information about themselves with institutions online? Is there a contradiction between people's stated concerns about privacy and their likelihood to share information with institutions?

Literature review: information-sharing and institutional privacy concerns

Information privacy is of interest in many disciplines, including communication, information science, law, and economics (Li, 2011; Pavlou, 2011). This paper focuses on scholarship that investigates why users share information online. The *privacy calculus* literature draws from Social Exchange theory, which holds that face-to-face interaction is shaped by mutual exchange of rewards (Blau, 1964; Homans, 1961). Building on this, the privacy calculus maintains that individuals decide whether to disclose information to others by rationally evaluating costs and benefits (Laufer & Wolfe, 1977). Culnan and Armstrong applied this concept to e-commerce; their survey data revealed that individuals are more likely to disclose personal information in exchange for benefits if they believe their privacy will be protected with few negative consequences (1999). Similarly, individuals make a privacy calculus when choosing when to disclose information through social network sites (SNS) such as Facebook, often perceiving their benefits to outweigh possible risks (Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). Specifically, the ability to use SNS to maintain relationships and manage impressions often outweighs privacy concerns (Bryce & Fraser, 2014; Min & Kim, 2015).

In terms of sharing with institutions, business and marketing researchers have determined that *trust* plays a significant role in whether people choose to use a website or purchase a service. E-commerce and banking require very sensitive information, such as credit card numbers, which many are reluctant to provide. Thus, people heavily weigh whether or not a site is trustworthy when deciding to use it (Gefen, 2000; Luo, 2002; Pavlou, 2011). For example, Bonsón Ponte et al. found that people were more likely to purchase travel online from a website they trusted, which they determined based on its quality of information and how secure it seemed (2015).

Other recent work investigates the role of *context and information type* in determining trust. Bansal et al. (2016) conducted a lab experiment which used banking, e-commerce, and health contexts to measure internet privacy concern and intention to disclose information. In low-sensitivity contexts, trust was less important, whereas in high-sensitivity contexts such as banking and health, privacy concern was very important in forming trust. A study of digitized health records found that context influenced willingness to disclose; individuals weighed what information would be used for, the stakeholder requesting it, and the type of information requested (Anderson & Agarwal, 2011). For instance, people were much less likely to disclose information in scenarios with seemingly negative personal consequences (Woodruff et al., 2014). In addition to Anderson and Agarwal (2011), other researchers have also found that *information type* is a key element in deciding whether to disclose. For example, people are more concerned with the privacy of their financial records than general interests or demographic information, as they perceive a greater risk if the former were compromised (Culnan, 1993; Phelps, Nowak, & Ferrell, 2000). A study of self-disclosure on a health social network site found that individuals undertook a cost–benefit analysis of whether to provide information based on perceived benefits (Wang & Midha, 2012). These studies demonstrate the existence of a privacy calculus and corroborate qualitative work on social privacy, which attends to the importance of context and audience (boyd, 2014; Vickery, 2015).

We take up Dowd and others' (2010) suggestion that qualitative studies of privacy-related decision-making can provide important insights to augment quantitative work, allowing participants to define privacy and explore nuance and context in their experiences. Thus, this study uses a qualitative approach to investigate why individuals choose to share information with institutions. While this paper is part of a larger project on privacy attitudes and practices (Hargittai & Marwick, 2016), here we focus on three research questions:

R1: What incentives do people see to sharing information with institutions online?

R2: What disincentives do people see to sharing information with institutions online?

R3: What factors affect whether people are willing to share information with institutions online?

Based on prior studies, we expected that individuals would undertake a cost–benefit analysis when determining when to disclose information, and that context (information type, institution) would be significant to that determination. The next section details our data collection and method of analysis.

Data and methods

Much research on privacy attitudes and behaviors focuses on young adults given their high use of social media and public rhetoric about their carefree attitude toward privacy (Duggan, 2015). This is particularly true for studies of social media (Christofides, Muise, & Desmarais, 2009; Gross & Acquisti, 2005) and digital privacy in general (Marwick, Murgia-Diaz, & Palfrey, 2010). We thus sampled a group of young people to place our findings in conversation with prior work, and chose focus groups as the most fitting method of data collection. For this topic, focus group interviews work better than

individual interviews as they give the researcher a less directive and dominating role, allowing participants to converse with each other rather than simply responding to one person (Krueger, 1994). Similarly, a survey would require greater preexisting knowledge about the research questions than the existing literature offers.

Data collection

We conducted ten in-person focus group interviews on a Midwestern urban campus with an average of four people each, for a total of 40 young adult participants enrolled in college or graduate school. Recruitment included flyers posted on campus and nearby establishments (such as cafes); Facebook ads; and email sent to the second author's local colleagues and neighbors to help identify potential respondents. The ads did not specify a focus for the study beyond general Internet use, to avoid biasing respondents. Sessions took place in the project lab on campus and lasted approximately one hour. Participants received $20 each at the end of the session. The principal investigator's Institutional Review Board for Human Subjects Research approved the study.

First, participants filled out a short survey regarding their demographic background and Internet experiences. We started with this survey since it asked participants to report online experiences, and we did not want responses influenced by the focus group. Next, we explained how focus groups work, and then asked everyone the first question to ensure that all participants equally participated. Rather than imposing a definition of privacy on the conversations, 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 in various contexts, and what types of technological or policy innovations would make them feel more in control, given that most expressed a lack of control. While the focus group included questions about privacy more generally, this paper highlights discussions about institutional privacy.

Analysis

Sessions were audio recorded and transcribed. We read through the material and highlighted quotations that addressed our research questions, grouping quotes by theme. Both authors and a research assistant participated in this analysis. The survey responses offer basic descriptive statistics about the study participants.

Participants

Most participants (77%) were enrolled as undergraduate students, while the rest were pursuing graduate study. All the graduate students were from the hosting institution, while undergraduate students came from an additional five institutions. Half of the participants were between the ages of 19 and 21, 27% were between 22 and 24, 13% were between 25 and 30, and 10% were between 31 and 35. Most participants identified as White (65.9%), several as Asian-American (19.5%), and fewer as African-American (9.8%) and Hispanic (4.9%). Most 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 journalism and communication (17%). While we did not see a difference among participants by gender, we specify age and gender for context when quoting participants.

Almost all study participants had continuous Internet access; only one did not have Internet access on their phone. To establish the participants' experience with social media, we asked whether they had heard of and/or used some popular sites. All reported having heard of Facebook, Twitter, LinkedIn, Instagram, and Google Plus, and all but one had heard of Snapchat, Tumblr, Pinterest, and Flickr. Everyone used at least one such site, and most used more than one.

Incentives to share with institutions

Participants mentioned a variety of various reasons for sharing information with institutions. Many saw clear benefits. 'I can't imagine a point at which I would be uncomfortable sharing my personal information as long as it improved life,' summarized one 19-year-old man. Specific advantages to sharing information included personalization, convenience, improved service, and financial and health benefits. Respondents considered it impossible to use most websites or apps without sharing information, so the alternative was seen as nonuse. Generally, participants viewed sites like Facebook and LinkedIn as having considerable benefits and framed opting out as impossible.

Sharing information enabled several participants to receive more accurate search results due to personalization. Others thought their matches on dating apps or roommate-matching questionnaires would be better if they provided personal information. Many mentioned convenience, including purchasing online, saving passwords to one's browser, and syncing software across devices:

> When I was connecting my information with Hulu and then Vimeo and Spotify, […], I just allow them to use [my data] and then make sure that in the settings I do all the settings right so that they can't do anything about it … Because I need it. It's so much more convenient if I allow them to just connect the two accounts. (Woman, 22)

Connecting accounts, which often allows companies to aggregate personal data, was viewed unequivocally positively. One man (22) explained 'I think Google Chrome is fantastic. It links everything together. It's really functionally great.'

Financial benefits were also mentioned, including loyalty cards that provided discounts; free trips from ride-sharing services like Uber; and coupons:

> If you sign up for – say if you're shopping on a certain website – if you make an account, oftentimes they'll send you an email for 15 or 20 percent off your first purchase, and if I know it's a place that I'll buy something once and never use it again, yeah I'll give my email to them, buy [laughs] something and then unsubscribe afterwards. I guess they'll still have my information on file in the future, but it doesn't matter that much to me. I don't really care. (Man, 21)

It is worth considering whether people fully understand the tradeoffs they are making in these instances, as participants frequently discussed financial/information exchanges in inaccurate or misleading terms. For instance, many mentioned that they would rather receive online services for free by providing trivial information than pay for them.

When asked if she would be willing to pay for a service with more control over her data, one woman (20) replied, 'I'd rather it still be free and then some advertisement company can know that I'm prone to buy granola bars in bulk or something.' Of course, a site like Facebook knows far more than whether you buy granola bars in bulk; it may have ascertained your sexual orientation, your closest friends and family, and your political leanings, to mention just a few types of sensitive information (Kosinski, Stillwell, & Graepel, 2013). Similarly, when considering whether to provide an email address, the only downside mentioned was possible spam:

> Because there's membership programs for stores and stuff and I'm like, 'I don't really particularly want Target to have all this information about me, but I do want this, that, or the other thing.' So on a case by case basis, I generally do decide to share information that they don't need, but I'll live with whatever emails, spam, consequences there are. (Woman, 33)

Few respondents – and indeed, few people in the US – understood that providing email addresses to companies acted as a unique identifier that provided access to larger demographic and data profiles constructed by third parties (Crain, 2016).

Several participants saw health benefits as a worthwhile tradeoff for providing personal information. While virtually all focus group respondents considered health information to be sensitive, a few would disclose information for better care or cheaper insurance. One woman (33) explained:

> I actually do think about health. However, I have kids, a husband who doesn't have health insurance, and I need to have health insurance, because I have a chronic condition, so there's stuff that I would sign up for. But at the same time, I think I would be more wary about having the particulars of my condition be public information, but I still think the tradeoff would work the same way. If it was something that was going to get me better care or save a significant amount of money, then I'd just be like, 'well, the world knows I have this now.'

While this woman had particularly acute health concerns, she was willing to provide personal information if it would improve health care or insurance. Later, we discuss health as a sensitive context which required respondents to evaluate carefully whether to provide information.

Opting out is not an option

Respondents felt that sites like Facebook, Twitter, and LinkedIn, which obligate users to share information,[1] were essential. Students used Facebook, for instance, to organize group projects, work on extracurricular activities, and learn about assignments. The site felt compulsory in that going without such benefits – information, relationships, and reputation management – had too high a cost. Other participants considered social media sites necessary for job-hunting or personal promotion. A 20-year-old woman explained, 'I'm looking for a job in communication social media, so I see Twitter as more important to my future now; it's a little more career-focused.' Another woman (22), elaborated:

> Being completely invisible from the Internet is not good, especially for, at least for college students and post, because it's weird like if a professional, there's someone that claims to be a professional doesn't exist on Google in some way. And when people say, 'no, I don't have Facebook' or 'I deactivated from Facebook,' well I just I start to wonder, 'oh, what happened?' [*laughter from group*]

This respondent saw a social and professional cost to opting out of social media. Such comments reveal the employment worries of graduating college students, as most considered it risky to avoid sites that might help them gain employment. Notably, participants framed disclosure to Facebook or LinkedIn in terms of sharing information with the site rather than friends or contacts. Information provision to SNS is often thought of as *social* privacy, but in these contexts respondents considered the site to be an institution.

Sharing information was also required to participate in e-commerce, which seemed so beneficial as to be compulsory. For instance, buying a book from Amazon required a credit card number and address. One respondent (female, 22), laughingly noted that while you can use a fake name on Twitter, 'With Amazon, you can't. Your shipping address is your shipping address if you want to get your package!'

In sum, interviewees mentioned reasons for sharing personal information with institutional actors ranging from professional necessities to health benefits and personal conveniences. They also mentioned a variety of disincentives, which we discuss next.

Disincentives to sharing

Participants mentioned varied situations in which they would refrain from sharing information, including skepticism of benefits; fear of discrimination; and lack of trust in the institution with which they were sharing. In some cases, respondents were happy with their current technologies, and were skeptical that providing more information would improve them:

> Woman (20): I'm pretty satisfied with the quality of results I get, and I don't – [*laughter from group*] Like I feel like I know my Google-fu is pretty up to snuff, and I'm not like sitting there frustrated, going 'oh if only Google knew that I liked anime right now' and then I would have a much better time, you know, that's not happening.

In such cases, participants did not believe that increased personal information provision would improve the quality of technology.

While participants did not provide concrete examples of information-based discrimination, several viewed this as a possibility and were thus cautious, particularly regarding health. One woman (34) was skeptical of so-called wellness metrics which could involve detailed fitness and diet information:

> I know there are all these sort of concerns about employers now wanting more and more health information, and, in theory, being able to tailor your health insurance plan to better meet your health needs. But I don't want my employer saying like 'You're eating too many French fries, you have to lose 20 pounds or something.' So in some ways, I'm worried about who specifically would access that information, whether there would suddenly be for like large employers, some way to access that.

Other participants mentioned sexually transmitted infections, depression, and cancer as information they wanted to keep private, since they saw these conditions as potentially detrimental to professional goals or health care options.

Many respondents were cynical about providing information to actors that they did not believe would protect their information, whether public or private entities:

> Man (20): In a sense, the program [NSA] certainly cares more about a planned covert operation than it does about my online Facebook photos that I don't like, and if it can't protect the information about the covert plans from [hacker collective] Anonymous, then it's certainly not going to be able to protect my online presence.

As noted in the literature review, studies have repeatedly identified trust as a major factor in information provision. As expected, participants were less likely to provide information to institutions they did not trust. As we discuss below, many mistrusted both government and private corporations.

Contextual factors

When deciding whether to share information, participants considered information type; the context in which information was shared, and with whom they shared. Photographs, likes and dislikes, and purchases were considered less sensitive, while health and financial information were highly sensitive and thus most important to protect. Notably, both governments and private companies were viewed as untrustworthy.

Focus group respondents were least likely to share their address, contact information, financial details, and health data. Other information was less important. Thus, willingness to share depended on the type of information requested. One woman (34) weighed her shopping habits against her personal health background:

> Yeah, I'm a little more protective of my health information than like my shoe shopping. I don't want to give the impression that I have a lot of shoes, just to be clear [*group laughs*] […] So, for me no. I'm more protective of my health information and my health background and my family's health information than other kinds of information, I would say.

Similarly, a 22-year-old man said he would be willing to share his schedule, but not financial information. In such cases, participants were happy to share information they considered innocuous, but were more careful when evaluating whether to share information they considered sensitive.

Participants were generally suspicious of giving out health information, especially those with extensive medical histories:

> Woman, 20: And I definitely wouldn't want my health information shared. [*Laughter from group*] That just seems like that would screw you over really bad.
>
> Interviewer: Like in what ways?
>
> Woman: I mean, it's harder to get a job when you've got the diagnosis of like clinical depression, general anxiety disorder, and also, you know, cancer and stuff. Not exactly something that needs to be a lot harder, impossible to get insurance and stuff. So.

Because health information was sensitive, participants were only willing to input personal information into sites like WebMD if they could not be personally identified:

> If [health information] had something like my name or something attached to it, I would want more assurance that anything else I added would be protected, but if it was just general WebMD, where you just search something and they don't know who it is … I'm not so bothered. (Woman, 20)

Interestingly, health concerns were one of the few areas where participants analogized between online and offline contexts. One female respondent (22) explained:

> Don't we already kind of give up our privacy a lot of times to get healthcare? [*sounds suggest agreement from group*] I mean like, you go into the room and you take off your clothes and you put on a paper bag, and someone who you don't really know comes and looks at you and touches you and stuff like that. And that's just something that we give up our privacy because it's within the context of receiving medical care. So maybe it just sort of translates from real life to digital. We're still willing to give up private things about ourself for healthcare.

Participants were willing to share online in spaces where they felt preexisting informational norms around health contexts were maintained (Nissenbaum, 2010). For instance, respondents thought online prescription services, Healthcare.gov, and hospital websites were governed by HIPAA laws (Health Insurance Privacy and Accountability Act) which protect health information.[2] In such cases, participants trusted that their information would be protected as it would be in a doctor's office.

As in previous research, participants considered the recipient when deciding whether to share information. Some were more likely to share with private companies because they mistrusted the US government after the Snowden revelations. One 22-year-old woman stated, 'If you're concerned about your privacy, then I don't think you should trust the government.' Others were more likely to share with the government, which they considered stable and secure, as demonstrated by this exchange discussing what they 'think about the idea of a central agency, possibly a private company, looking after [their] online privacy':

> Woman A (20): I don't know if I like that it could be a private company, maybe if it's a government controlled thing, because my information is going to be out there no matter what, and I want it to be in secure hands, maybe not private company, where it can be hacked and like get even worse.
>
> Interviewer: So you think the government couldn't get hacked?
>
> Woman A: Maybe like less chance of getting hacked.
>
> Woman B (20): In theory it could get hacked, but it's not for profit. Like nothing they do is for profit, so you don't even have to worry about that aspect.
>
> Woman C (22): Yeah, I was more worried about a private company, like what if they go bankrupt or something? What happens then? What do they do with all of it?

While the government was viewed as untrustworthy and incompetent, private companies were considered vulnerable to hackers, motivated by profit and likely to sell personal data, with the potential to go out of business.

Since both institutional types had shortcomings, many mistrusted both. A woman (20), explained 'I don't want to, wouldn't want to give out my personal data, especially to a private company, but really not to a government agency either probably.' In a different focus group, the participants discussed the downsides of both government and corporations:

> Woman, 20: Mhm. I think they're scary for different reasons. Cause like a private company seems very mercenary to me, I would be frightened for that reason, but the government, I'm like, 'oh god, you're like bloated and bureaucratic and incompetent in other arenas, so why are you now in charge of my data?' Like why can't I do that myself?

> Man, 22: And there could be punitive consequences if the government had access to all your data.
>
> Woman: Oh right, because you don't want to trust the government with your OKCupid 'yes, I like do drugs all the time' [*laughter from group*] cause they're probably, like in some dimension legally required to act on that.

These discussions are telling. Participants knew that private companies were likely to sell their data, but they believed the government was equally likely to invade their privacy. Neither was trustworthy, so when respondents stated a preference, they framed it as the lesser of two evils.

However, participants did consider individual websites to be trustworthy, specifically, Amazon and Google. In this case, respondents felt comfortable providing even highly sensitive information such as their address and credit card number. On 'shady' or 'sketchy' sites, they believed that they had to be very careful and use extra precautions, such as incognito mode. One woman (22) explained:

> For me, I think the individual responsibility; it goes as far as choosing what sites they trust and what information they give out and rest of the exploitations that comes after it is the company's issue of morality and abiding by what they said was in their privacy policy. So, for example, I would agree to subscribe to a mailing list of a sketchy website to get information about upcoming concerts, but then it's also my responsibility to, if my privacy information feels threatened because the site is really, really sketchy, then it's my responsibility to unsubscribe from it and then ask to remove my information, but that's as far as my responsibility goes.

This respondent believed it was her 'responsibility' to assess a site's credibility and provide or withhold information accordingly. These quotes, and other moments throughout the interviews, give support to literature showing that trust is a key metric when considering whether to share information.

Is online privacy possible?

While the answers to our three research questions support previous research, the focus groups revealed two surprising implications. First, participants often viewed privacy violations as inevitable; and second, many believed privacy was necessary only if you had 'something to hide.' Both call into question the validity of the rational, 'privacy calculus' approach to evaluating online information disclosure in the current information environment.

Inevitability

Many focus group participants regarded privacy violations as inevitable. For example:

> Interviewer: Okay. So do you think it's possible to have privacy online? Like when using social media or shopping?
>
> Woman X (20): No.
>
> Woman Y (21): No.
>
> Woman Z (22): No.

When making a cost–benefit analysis to share information, participants did not measure their actions against an ideal world in which their privacy was perfectly protected and they controlled how their information flowed. Instead, they recognized that, in many cases, information was already widely available to e-commerce sites, advertisers, and the US government, making privacy-protective measures somewhat futile. Dismay over the 'privacy paradox' fails to consider the current information landscape where most people use multiple devices, struggle to remember dozens of passwords, and must take heroic measures to protect information in the face of software defaults which encourage sharing. As one participant explained:

> But it's getting more and more difficult to control my information. Because [cloud service companies] are actually kind of just making it more easy to upload those things on the website, compared to you not trying to do. [*Sounds of agreement from group*]. And you don't want to do that. And also every device and every program has a different kind of access and things. It's really hard to control everything because I need to remember every ID and password and every condition, which file should go where, which drive, iCloud, Dropbox, Google Drive. (Man, 35)

Given these complicated conditions, it is unsurprising that users prefer to save passwords in their browser, use Facebook to log into multiple sites, and shop on e-commerce sites that remember credit card numbers. These technologies are part of the reality of contemporary internet use because they meet a significant need.

Previous research has found that people's perceived ability to control whether their privacy is violated may affect their willingness to share information online (Cho, Lee, & Chung, 2010; Turow, Hennessy, & Draper, 2015). Since many respondents felt powerless over their ability to protect their privacy, this may affect their likelihood to share information online, which is supported by other studies. Turow et al. (2015) found that, in contrast to the way the privacy paradox is typically framed, people with the most knowledge about online privacy were most likely to share information. While our paper does not address that specific question, our data do support Turow's conclusion: that people are 'resigned to giving up their data – and that is why many appear to be engaging in tradeoffs' (2015, p. 3). Similarly, in focus groups about big data, Andrejevic (2014) found that people used technological systems that they disliked because they felt they had no other option. That is not to say that our participants did not see a utility to privacy, but that violations seemed inevitable. Such attitudes may appear cynical (Hargittai & Marwick, 2016), but they are more appropriately labeled resignation or powerlessness.

This is amplified by the feelings of many participants that social media sites were required for their day-to-day activities. If such applications are required, how much of a privacy calculus can individuals afford to make? Such requirements question the voluntary nature of social media participation and the inevitability of privacy violations. One participant (Woman, 21) told a story of her friend, a long-term Facebook holdout, who felt forced to join the site in order to buy some furniture from the campus 'Free and For Sale' group. In this case, the individual wanted to buy cheap furniture, not share information about herself with Facebook, let alone the many third-party companies to which Facebook sells information. Participants saw opting out as impossible, but opting in implied that one was willing to share data, which was not necessarily true.

Nothing to hide, nothing to lose

When discussing whether to share data, participants framed their choice not as a risk/benefit calculus but as having *nothing to hide*. For instance, one respondent stated that unless she had done something illegal, none of her information would harm her if made public:

> I think the only thing I would fear is like being treated differently or being like discriminated against because of a health issue, just some information about myself. I can't really think of anything, 'cause when, when we think about people's information being revealed, it's usually in a case where they are in trouble and they did something wrong, so an investigation was gone into them and like their history and things. You could think of like shooting incidents or like, acts of terrorism or whatever. That's the only case I can really think of was when that kind of information becomes really public and sought after. So I wouldn't, it's not really something I really fear. (Woman, 22)

This reflects the fact that information tends to be public by default on social media, and can only be made private with effort (boyd, 2010). Our participants are not necessarily choosing to provide information, but instead, *not taking the extraordinary effort to make it private*. One woman (33) summarized:

> I feel like I don't really believe in privacy in the sense that I don't think that I have that choice. People sort of say, 'you can do this, this, and this to make sure "X" person doesn't know "Y"', and I think my sense of my ability to actually manage that in the way that I think it's going to be managed – I don't think that I can. So I think if I have a web presence at all and am not living off the grid in the woods or something, I think that I might as well just accept the fact that I am there and exist for the government or whoever to see.

To this participant, privacy isn't a choice; she must use the internet, and therefore her information will be compromised. Thus, the calculus cannot be rational, as she has no other option. She believes that *privacy*, an active process of managing information, can only take place in situations where there is an implied choice, although this, too, may be an illusion.

Such effort seemed unnecessary to our participants, who often found it hard to articulate harms. One woman (24) shrugged off her worries, saying 'Even if someone stole my identity, I have like $200 in the bank [*group laughs*], so it's not as big of a deal as if I was Donald Trump.' As quoted earlier, privacy harms exist only when 'information becomes really public and sought after' which only happens to 'terrorists' or other bad people. A man (22) asked 'why do you need private browsing? Are you doing things you're not supposed to be doing, illegal?' Even participants who were likely the subjects of government data collection had a hard time believing it:

Interviewer:	Okay, so similar to what you said before, what you're doing, it's not really going to be of interest?
Woman, 22:	Because I'm not a citizen here, I just didn't even worry that I would be a threat because I'm not really. I have a social security number, but I didn't even think of myself as registered by the US government.
Interviewer:	You don't think they're watching foreigners?
Woman:	But I'm like a very healthy foreigner. [*Laughter from group*]

This woman saw herself as 'healthy' and therefore unlikely to be scrutinized, although it is precisely foreigners whose data are most likely to be surveilled by the US government. To

these young people, privacy was necessary only if you had something to worry about. To people with 'normal' internet habits, privacy-protective behaviors were unnecessary. Of course, the 'nothing to hide' argument is easy to argue against. Solove, who has written extensively about this issue (2007), points out that privacy is necessary for a democratic, free society, and that even people who believe strongly in national security use curtains on their windows and wear clothes in public. Our participants, faced with privacy violations they viewed as inevitable, minimized any possible harms by assuring themselves that they either had nothing to hide, or nothing to lose.

Conclusion

While much research has examined how privacy concerns influence what people share online in social settings, our paper adds to the literature by extending that question to institutional actors. It is not without limitations. We are specifically concerned with user attitudes towards institutional privacy, rather than user behaviors. We also recognize that there is frequently a disconnection between self-reported and actual behavior. Therefore, we are not attempting to make a causal argument. Further research might investigate how the attitudes we have recorded towards institutional privacy affect how people disclose information to online institutions, as well as how the 'nothing to hide' rhetoric is used to diminish fears of privacy violations in the face of widespread violations.

This paper finds, in accordance with previous research, that individuals make a privacy calculus, carefully weighing the costs and benefits of providing personal information to institutions such as governments and corporations. Users are incentivized by financial benefits, health benefits, convenience, and necessity. They are disincentivized by lack of trust, fears of online harassment, and fears of discrimination. When choosing whether to share information, they evaluate the information type, context, and institution requesting the information. However, we also find that participants viewed privacy violations as inevitable and social media use as necessary, calling into question the cost–benefit privacy calculus model of information provision. Many participants shrugged off the risk of privacy harms by saying they had nothing to hide and little to lose.

While participants mentioned many different risks, including discrimination and distrust, virtually no-one grasped the extent of data-mining; they saw information like the products they bought, or even their email address, as completely trivial, because they mainly understood them as disconnected and disparate. Concepts like third-party data collection were unfamiliar to them, as they are to most Americans. For instance, a 33-year-old woman said,

> I think that it's possible that nobody is taking the data that you could find out about me because it just sort of exists, and it would take dedicated effort to put it all together into some kind of narrative that actually said something that I would care about people knowing about.

Yet such dossiers are automatically generated by data-mining apparatus and regularly sold to corporations and governments by data-brokers. Participants simultaneously thought they had more legal and policy protection than they did (e.g., HIPAA governance of health information websites), while feeling resigned to inevitable privacy violations. Since nobody in our sample had experienced a significant institutional privacy violation (e.g., loss of

money or major opportunities due to information provided to institutional actors), they often had a 'bad feeling' about privacy, but had few concrete risks to weigh against providing information.

Our findings suggest a need for greater public awareness about how personal data are aggregated and used to create detailed profiles available to companies and, potentially, government agencies. The hope is that increased awareness might open up discussion of policy solutions to regulate such practices. They also suggest the need for more research on the accuracy of individuals' privacy calculus; if people misunderstand the risks of their information provision and do not believe opting out of information-sharing is possible, they cannot accurately assess the risks and benefits of providing information to institutions.

Notes

1. One can use Twitter without an account, but participants discussed using Twitter for self-promotional purposes which implied posting content and interacting with others on the site.
2. Whether healthcare.gov is governed by HIPAA became a political issue when US Representative Joe Barton, a Republican, claimed that the site violated the law in a House hearing on the Affordable Care Act. This complex issue is still under debate.

Acknowledgements

We are grateful to Merck (Merck is known as MSD outside the United States and Canada) for its support. We greatly appreciate Robert Babich's assistance with data coding and the opportunity provided to him by the Institute for Policy Research Summer Research Assistant Program at Northwestern University. For assistance with data collection and transcription, we thank Elizabeth Hensley through Northwestern's Summer Research Opportunity Program, Devon Moore, Somi Hubbard, and Karina Sirota supported by Northwestern's Undergraduate Research Assistant Program. Marwick thanks the Data & Society Research Institute Fellows Program for providing the opportunity to work on this project. Hargittai appreciates the time made available through Northwestern's April McClain-Delaney and John Delaney Research Professorship for conducting this research.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported by Merck (Merck is known as MSD outside the United States and Canada) through a research gift.

Notes on contributors

Alice Marwick (PhD, New York University) is an Assistant Professor in the Department of Communication at the University of North Carolina at Chapel Hill. Her research interests include networked privacy; gender and social media; far-right internet cultures; and media manipulation and disinformation online. She is the author of Status Update: Celebrity, Publicity and Branding in the Social Media Age (Yale 2013) and co-editor of the Sage Handbook of Social Media (2018). [email: amarwick@unc.edu] (return).

Eszter Hargittai (PhD Sociology, Princeton University) is Professor and Chair of Internet Use and Society at the Institute of Communication and Media Research of the University of Zurich. Her research looks at how people may benefit from their digital media uses with a particular focus on how differences in people's Web-use skills influence what they do online. She is working on a data base of survey questions concerning the study of people's Internet uses. She is editing the Handbook of Digital Inequality [email: pubs@webuse.org].

References

Anderson, C. L., & Agarwal, R. (2011). The digitization of healthcare: Boundary risks, emotion, and consumer willingness to disclose personal health information. *Information Systems Research*, *22* (3), 469–490.

Andrejevic, M. (2014). The big data divide. *International Journal of Communication*, *8*, 1673–1689.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*(1), 1–21.

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9), Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1394

Blau, P. M. (1964). *Exchange and power in social life*. New Brunswick, NJ: Transaction.

Bonsón Ponte, E., Carvajal-Trujillo, E., & Escobar-Rodríguez, T. (2015). Influence of trust and perceived value on the intention to purchase travel online: Integrating the effects of assurance on trust antecedents. *Tourism Management*, *47*, 286–302. doi:10.1016/j.tourman.2014.10.009

boyd, d. (2010, March). Making sense of privacy and publicity. Presented at the South by Southwest Interactive Conference, Austin, TX. Retrieved from http://www.danah.org/papers/talks/2010/SXSW2010.html

boyd, d. (2014). *It's complicated: The social lives of networked teens*. New Haven, CT: Yale University Press.

Bryce, J., & Fraser, J. (2014). The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions. *Computers in Human Behavior*, *30*, 299–306. doi:10.1016/j.chb.2013.09.012

Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987–995.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *CyberPsychology & Behavior*, *12*(3), 341–345.

Crain, M. (2016). The limits of transparency: Data brokers and commodification. *New Media & Society*, doi:10.1177/1461444816657096

Culnan, M. J. (1993). 'How did they get my name?': An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly*, *17*, 341–363.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Dowd, M. (2010). Contextualised concerns: The online privacy attitudes of young adults. In S. Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, & G. Zhang (Eds.), *Privacy and identity management for life* (Vol. 352, pp. 78–89). Trento: Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-642-20769-3_7

Duggan, M. (2015, August 19). Mobile messaging and Social Media 2015. Retrieved from http://www.pewinternet.org/2015/08/19/mobile-messaging-and-social-media-2015/

Gefen, D. (2000). E-commerce: The role of familiarity and trust. *Omega*, *28*(6), 725–737. doi:10.1016/S0305-0483(00)00021-9

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on privacy in the electronic society* (pp. 71–80). New York, NY: ACM Press.

Hargittai, E., & Marwick, A. (2016). 'What can I really do?' Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 21.

Homans, G. C. (1961). *Human behavior: Its elementary forms*. New York, NY: Harcourt, Brace.

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167404815001017

Kosinski, M., Stillwell, D., & Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences*, *110*(15), 5802–5805. doi:10.1073/pnas.1218772110

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, *25*(2), 109–125.

Krueger, P. R. A. (1994). *Focus groups: A practical guide for applied research, Second Edition*. Sage (1994), Edition: 2nd, Paperback, 272 pages.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*(3), 22–42.

Li, Y. (2011). Empirical studies on online information privacy concerns: Literature review and an integrative framework. *Communications of the Association for Information Systems*, *28*(1), 453–496.

Li, H., Sarathy, R., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *Journal of Computer Information Systems*, *51*(1), 62–71.

Litt, E. (2012). Knock, knock. Who's there? The imagined audience. *Journal of Broadcasting & Electronic Media*, *56*(3), 330–345.

Litt, E., & Hargittai, E. (2016). The imagined audience on social network sites. *Social Media+Society*, *2*(1), doi:10.1177/2056305116633482

Luo, X. (2002). Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management*, *31*(2), 111–118. doi:10.1016/S0019-8501(01)00182-1

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

Marwick, A., Murgia-Diaz, D., & Palfrey, J. (2010). *Youth, privacy and reputation (literature review)* (No. Berkman Center Research Publication No. 2010-5). Boston, MA: Berkman Center for Internet and Society at Harvard University. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163

Mills, J. (2015). The future of privacy in the surveillance age. In R. Goldfarb (Ed.), *After Snowden: Privacy, secrecy, and security in the information age* (pp. 193–251). New York, NY: St. Martin's Press.

Min, J., & Kim, B. (2015). How are people enticed to disclose personal information despite privacy concerns in social network sites? The calculus between benefit and cost. *Journal of the Association for Information Science and Technology*, *66*(4), 839–857. doi:10.1002/asi.23206

Nissenbaum, H. F. (2010). *Privacy in context : technology, policy, and the integrity of social life*. Stanford, CA: Stanford University Press.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, *35*(4), 977–988.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27–41.

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/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2775/2432

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world* (1st ed.). New York, NY: W. W. Norton & Company.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1016.

Solove, D. J. (2007). 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review*, *44*, 745.

Solove, D. J. (2008). *Understanding privacy*. Cambridge, MA: Harvard University Press.

Trepte, S., & Reinecke, L. (2011). *Privacy online: Perspectives on privacy and self-disclosure in the social Web*. New York: Springer.

Tufekci, Z. (2012). Facebook, youth and privacy in networked publics. Presented at the International AAAI Conference on Weblogs and Social Media. Retrieved from http://www.aaai.org/ocs/index.php/ICWSM/ICWSM12/paper/view/4668

Turow, J. (2017). *The Aisles have eyes: How retailers track your shopping, strip your privacy, and define your power*. New Haven, CT: Yale University Press.

Turow, J., Hennessy, M., & Draper, N. (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

Vickery, J. R. (2015). I don't have anything to hide, but … ': The challenges and negotiations of social and mobile media privacy for non-dominant youth. *Information, Communication & Society*, *18*(3), 281–294. https://doi.org/10.1080/1369118X.2014.989251. (ahead-of-print)

Vitak, J., Blasiola, S., Patil, S., & Litt, E. (2015). Balancing audience and privacy tensions on social network sites: Strategies of highly engaged users. *International Journal of Communication*, *9*, 20.

Wang, Y., & Midha, V. (2012). User self-disclosure on health social networks: A social exchange perspective. Presented at the International Conference on Information Systems (ICIS), Orlando, FL, AIS. Retrieved from http://aisel.aisnet.org/icis2012/proceedings/ResearchInProgress/99/

Woodruff, A., Pihur, V., Consolvo, S., Schmidt, L., Brandimarte, L., & Acquisti, A. (2014). Would a privacy fundamentalist sell their DNA for $1000 … If nothing bad happened as a result? The Westin categories, behavioral intentions, and consequences. In *Proceedings of the tenth symposium on usable privacy and security*. Menlo Park, CA: The USENIX Association. Retrieved from https://www.usenix.org/system/files/conference/soups2014/soups14-paper-woodruff.pdf

Young, A. L., & Quan-Haase, A. (2013). Privacy protection strategies on Facebook. *Information, Communication & Society*, *16*(4), 479–500. doi:10.1080/1369118X.2013.777757