A NEW PRIVACY PARADOX? YOUTH AGENTIC PRACTICES OF PRIVACY MANAGEMENT DESPITE 'NOTHING TO HIDE' ONLINE

Pre-publication accepted version, forthcoming in Canadian Review of Sociology, February 2019

ABSTRACT

Focus groups conducted with Canadian teenagers examining their perceptions and experiences with cyber-risk, center on various privacy strategies geared for impression management across popular social network sites. We highlight privacy concerns as a primary reason for a gravitation away from Facebook towards newer, more popular sites such as Instagram and Snapchat, as well as debates about the permeability of privacy on Snapchat in particular. The *privacy paradox* identifies a disjuncture between what is said about privacy and what is done in practice. It refers to declarations from youth that they are highly concerned for privacy, yet frequently disregard privacy online through 'oversharing' and neglecting privacy management. However, our participants, especially older teens, invoked a different mindset: that they have 'nothing to hide' online and therefore do not consider privacy relevant for them. Despite this mindset, the strategies we highlight suggest a new permutation of the privacy paradox, rooted in a pragmatic adaptation to the technological affordances of social network sites, and wider societal acquiescence to the debasement of privacy online.

KEY WORDS

Youth and cyber-risk; privacy paradox; nothing to hide; social network sites; focus groups

AUTHOR DETAILS

Michael Adorjan (corresponding author)
Department of Sociology, University of Calgary
madorjan@ucalgary.ca

Rosemary Ricciardelli
Department of Sociology, Memorial University of Newfoundland
rricciardell@mun.ca

INTRODUCTION

Teen use of the internet has generated concern, which we refer to as *cyber-risk*, specifically around their use of online social network sites (SNS) (boyd 2014), their potential for contact with 'predators' online (Tynes 2007), and participation in digital sexual expression (i.e., 'sexting') (Karaian 2012; Marker 2011). Cyber-risk is complicated by the specific affordances of SNS, i.e., technological features that mediate how they are used. These include persistence or permanency of the data posted to SNS: content is *searchable* (e.g., 'Googling' information); content can be *replicated* outside of its original context; and *invisible audiences* make it difficult or impossible to anticipate those who ultimately receive the content posted in networked publics, outside of intended audiences (boyd 2008a, 2014). Despite the risks associated with privacy breaches related to these affordances, the belief among some that 'youth today' are not at all interested in or neglect considerations of their privacy online seems to retain purchase. The media have underscored this stereotype with headlines and editorializing that suggest youth are shameless and have no sense of privacy (boyd 2014; Livingstone 2008; Nussbaum Feb 12, 2007). Studies on Facebook conducted soon after the site became available to the general public also provide some evidence that youth were, at the time, not concerned about online privacy (e.g., Barnes 2006). However, what quickly emerged was a disjuncture between what youth said about privacy versus their actual behaviours online. This 'privacy paradox' involves statements *declaring* privacy to be a paramount concern, despite ongoing practices of open sharing of personal information through various online platforms (Barnes 2006; Hargittai & Marwick 2016). Tufekci's (2008) study of undergraduate students in the United States found student motivation to be publicly visible is mitigated by selective disclosures balancing publicity with

privacy. While many youth are aware of privacy risks related to their online activities, they see the compromise of their privacy as unavoidable, even imperative, in order to connect with peers online and acquire social and personal benefits through accessing social network sites (Regan & Steeves 2010). Simply put, 'cyber abstinence' is not a viable option for the majority of teens; many sacrifice privacy to gain social connection through visibility. As Tufekci (2008:34) argues "the need to be seen is greater than the fears students have about privacy intrusions."

In this paper, we reveal an additional permutation of the privacy paradox. Drawing from focus group discussions with Canadian teen 'digital natives' (Prensky 2001), referring to youth who grew up immersed in technology, we unpack what may indicate a new discursive mentality towards online privacy, especially among older teens: that privacy breaches are not concerning because youth have 'nothing to hide' when posting online. Despite this mindset – which we frame using an online application of Mead's (1962 [1934]) generalized other, a "cyber-based generalized other" (Altheide 2000:9) – we highlight a number of newer and agentic privacy management strategies that we interpret using Goffman's theory of impression management. We give attention to both user practices in managing context collapse, referring to the 'flattening' of audiences online (Marwick & boyd 2011) –but also highlight "how platforms themselves afford privacy management" (J. Davis & Jurgenson 2014:482). For instance, we center on discussions around newer and ostensibly 'ephemeral' SNS such as Snapchat, focusing on how youth use Snapchat given its particular affordances, as well as the pros and cons of 'blocking' other users. While the original 'privacy paradox' juxtaposed declarations of the importance of privacy management despite online activities risking privacy violations, our research indicates this paradox has now shifted to one where a discursive stance of having 'nothing to hide' online is juxtaposed by a range of agentic privacy management strategies

geared to manage impressions across variegated audiences. What does not appear to have changed, however, is that privacy concerns remain centered on 'horizontal' peer groups (e.g., family, friends, employers), rather than 'vertical' groups such as corporations and governments. We divide our paper into four sections. First, we explicate the framework for analysis of online privacy and privacy management, followed by this study's methodology. We then turn to highlight a theme that emerged from our focus group discussions on privacy and surveillance (the latter is beyond our scope in this paper): that of 'having nothing to hide' online. We follow this by an explication of the various privacy management strategies raised during our discussions with teens, centering on Snapchat and 'blocking'. The discussion which follows highlights broader sociological implications, study limitations and informs attitudes toward and strategies for privacy and privacy management online.

SELF, SOCIETY AND PRIVACY

Anthony, Campos-Castillo and Horne (2017) define privacy simply as "the access of one actor (individual, group, or organization) to another," referring to "what people conceal and reveal and what others acquire and ignore" (p. 251). While a number of theoretical frameworks are useful to examining privacy vis-à-vis "technologically mediated sociality" (Tufekci 2008:21), those drawing from Goffman's (1959) dramaturgical model of impression management are especially attuned to the various – and often competing – *imagined audiences* youth project on SNS (boyd 2008b; Marwick & boyd 2011). Scholars, in line with Goffman's (1959) theories of presentation of self and impression management, examine how youth online and offline grapple with the need to manage "multiple selves for multiple performances" and related audiences (Robinson 2007: 96). This presentation management involves a habitual monitoring of "how people respond to

them when presenting themselves" (Marwick & boyd 2011:123; see also Cooley 1902). As Robinson (2007:96) notes, "through its performances, the self strives to convey an identity consistent with the expectations formed by the audience and with the situation, or stage, that frames the interaction." This striving for situated and *contextual integrity* (Nissenbaum 2004, 2011) involves performances that "do not violate the context of community interaction" (Robinson 2007:106).

Influentially, Nissenbaum (2004) challenges dichotomous treatments of privacy with her concept of contextual integrity; in particular she argues that two types of informational norms govern most contexts: "norms of appropriateness" and "norms of flow or distribution" (p. 138). Norms of appropriateness "dictate what information about persons is appropriate, or fitting, to reveal in a particular context" while norms of distribution involve the "transfer of information from one party to another or others" (Nissenbaum 2004:138, 140). Adherence to both types of norms upholds contextual integrity, while violations occur through breaching either or both of these norms. On SNS especially, these norms are mutually reinforcing – it is not, for instance, appropriate to transmit or redistribute nude images of a person online without their consent. While it holds true that "the scope of informational norms is always internal to a given context, and, in this sense, these norms are relative, or non-universal" (Nissenbaum 2004:143), online SNS problematize the ability of users to discern which contexts (i.e., imagined, projected audiences) – more distinct in offline space/time – are salient when they post content to SNS. Marwick and boyd's (2011) term *context collapse* captures this dramaturgical complication applied to "radically heterogeneous" (Nissenbaum 2011:38) SNS such as Facebook, Twitter, and more recently Instagram and Snapchat (see also boyd 2002). Collapsed contexts can lead to embarrassment or even harm and victimization when "diverse Generalized Others [e.g., parents,

teachers, employers] converge into a single mass" (J. Davis & Jurgenson 2014:478). Most SNS are structured on the principle of "public by default, private through effort" (boyd 2014:61), placing the emphasis on users to take proactive strategies to manage their privacy.

A number of recent studies (boyd 2008a; J. Davis & Jurgenson 2014; Marwick & boyd 2011) contribute significant knowledge to *how* users navigate context collapse, characterizing the problem as one of impression management and 'face work' (Goffman 1955). This is particularly relevant to digital communication technologies such as SNS, given their affordances of persistent contact and pervasive awareness (see also J. Davis & Jurgenson 2014; Hampton 2016). For instance, Acquisti and Gross's (2006) study with US college students (when the SNS was still restricted to high school and college students) found Facebook users who expressed the least concern about the privacy of their posts explained this lack of concern by the control they felt over their information. However, for those who felt they have nothing to hide regarding the information they post, the same ostensible lack of concern is not explained through a sense of control over information (quite the opposite), but avoidance of problematic content altogether in relation to a wider "cyber-based generalized other" (Altheide 2000:9). Of note however is the unique and popular SNS Snapchat. In the academic literature on Snapchat to date, the SNS is frequently identified as unique to others in that content posted to it 'self-destructs' between one to ten seconds, ostensibly safeguarding concerns for the permanency of what is posted online (boyd 2014; J. Davis & Jurgenson 2014; Utz Muscanell and Khalid 2015). Utz and her colleagues (2015:142) point to a report in the United States which "showed that college students …felt they have the most privacy on Snapchat", likely due to the assumption of the ephemerality of the content Snapchat perpetually destroys. Utz and her colleagues found, through an online survey of users of both Snapchat and Facebook (mean age of 22 years), that users of Snapchat

had fewer number of networked connections than Facebook, which they argue "could also be driven by the more private nature of Snapchat" (Utz et al. 2015:144). However, care should be taken to delineate between *perceptions* of privacy based on assumptions regarding specific affordances of technology.

The question then has gravitated to not whether youth are concerned for online privacy, but the strategies and approaches they use to manage context collapse and preserve their impression management; said another way: "how users, as agentic beings, circumvent architectural affordances" (J. Davis & Jurgenson 2014:476). Although James (2014) identified *privacy as forsaken* in reference to the idea that privacy is not attainable online; that once content is posted, the user no longer has any control over how it is appropriated, a number of strategies to manage online privacy and avoid regret based on shared information are well documented. These strategies include the creation of multiple or fake accounts, 'wall' cleaning on Facebook (referring to reviewing past posts and untagged and/or deleting undesired content), using pseudonyms, lying about age and location, delaying responses, declining or ignoring 'friend' requests, self-censoring, and managing privacy settings (Bailey & Steeves 2015; boyd 2014; James 2014; Raynes-Goldie 2010; Wang et al. 2011).

Some researchers have explored the relationship between privacy concerns, the aforementioned strategies for privacy, and age. Surveying the existing literature, Youn (2005:94) points to "inconsistent findings", with some scholars pointing to no relation between age and privacy concerns (e.g., Phelps, Nowak, & Ferrell 2000) and others, largely focused on consumption practices, showing younger consumers as "more likely to know and use privacy protection strategies than older consumers" (Youn 2005:94; see also Dommeyer & Gross 2003). Some scholars report a statistically significant relationship between age and privacy concerns; for

example, in a study conducted by Paine and colleagues (2007), participants under 20 years of age were less likely to express concerns over privacy online than those over 20. More recently, James (2014:36) found that younger 'tweens' were "naive to the effectiveness of [privacy management] strategies." With the rapidly changing social media landscape over the last decade, including the rise to prominence of Instagram and Snapchat, questions remain regarding how extant privacy mindsets, as well as ostensibly newer adaptations such as 'nothing to hide' are being experienced among youth. In the current study, we sought to understand if these strategies are salient among our participants, and if any new strategies have emerged *across* SNS, particularly newer, popular SNSs such as Snapchat.

CURRENT STUDY

Recognizing attitudes towards privacy are often studied through survey designs that do not tap the reasoning and meanings behind participant responses (see Paine, Reips, Stieger, Joinson, & Buchanan 2007), we use focus groups, a qualitative approach, to generate knowledge that interprets attitudes and opinions within dynamic group interactions (Madriz 2000; Morgan 1997; Stewart, Shamdasani, & Rook 2007). Specifically, we mine "personal meanings" (2003:159), in our exploration of the context and lived experiences of teens towards cyber-risk, through dialogue that captures interpretive details and complements the breadth of current survey-based research on online risk. Often employed by scholars researching sensitive populations, focus groups elicit "a level of frankness that is seldom achieved through survey questionnaires" (Madriz 1997:3). Select international scholars have employed focus groups to research specific cyber-risks such as cyberbullying (e.g., Agatston, Kowalski, & Limber 2007; Pelfrey & Weber 2014) and sexting (Lenhart 2009). Comparable studies, however, are lacking in Canada and the

few emerging in the area focus solely on female experiences online (Bailey & Steeves 2015) or are limited to youth in urban areas (though see Burkell & Saginur 2015; Steeves 2014). In response to these lacunae in knowledge, we held focus group discussions with male and female teens living in urban and rural areas. Our objective was to provide a venue for participants to reflect on how their experiences are shared across others their age and, in so doing, the groups provide a forum for interconnection and mutual empathy. We also contribute to emerging research on youth and the internet that explores similarities and differences across urban and rural regions (see Burkell and Saginur 2015), and discuss our findings with reference to location, gender and age where discernible differences exist.

METHODS

PARTICIPANTS AND RECRUITMENT

Between July 2015 and November 2016, we conducted 35 focus groups with 115 participants aged 13-19 (average age of 15), with an average number of 3.3 participants per group (a minimum of two and maximum of five).[1] Groups of four to six have been found to be optimal to ameliorate the effects of 'over sharing' or domineering participants as well as participants who may feel intimidated and become silent within larger groups (Morgan 1997; Twinn 1998). Although we aimed for groups with no less than four participants, changes in the availability of students reduced the size of some groups to two participants. A total of 67 females and 48 males participated. Most groups were held with youth of the same gender and age/grade levels, a sampling stratification strategy designed to help ensure participants interacted with others that they would not perceive as threatening and with whom their experience may also resonate (Madriz 1997; Morgan 1997). 15 groups were conducted in a mid-sized city in Western Canada,

'Cyber City'; the remaining 20 groups were conducted in rural Atlantic Canada, 'Cyberville'. Discussions lasted from 30 minutes to 120 minutes and were audio recorded to preserve their accuracy. Any quoted excerpts from transcripts included are edited for speech fillers (e.g. 'ums') and readability, but otherwise are reproduced verbatim.

We employed a purposive, snowball sampling design, whereby initial contacts in various sectors, such as schools and universities, helped refer additional participants. Some participants were referred through participating schools in both Cyber City and Cyberville. Public middle and high schools participated in the project. Focus groups were conducted by both authors as well as trained research assistants. Discussions often began with general conversation about social media use and everyday habits engaging with technology, before turning to impressions of risk and harm online. Issues of privacy were most often raised by participants themselves through open-ended questions about what is concerning to them, if anything, about going online. Follow up questions would then be asked to mine deeper into attitudes and strategies related to privacy, which sometimes led to specific discussions over the affordances of particular SNS such as Snapchat and 'Snapstreak', which we highlight in this paper.

DATA ANALYSIS

Data was analyzed using an inductive, comparative approach aided by NVivo qualitative analyses software. Concepts and theories emerged naturally through analyses of the dynamic interaction of participants (Berg 2004; Strauss & Corbin 1990). The initial stages of "widely open inquiry" involved the 'open coding' of the data (Berg 2004:278). Prominent themes developed through the tracking of coding 'nodes' across and within groups. Regular research

meetings between the investigators ensured that thematic development emerged in a consistent manner, and helped to certify a hermeneutically attuned validity of the data (Twinn 1998).

AGE, PERSONAL RESPONSIBILITY AND THE 'NOTHING TO HIDE' MINDSET

Perhaps in an effort to adapt to the demands of authority figures, including parents and educators, older teens in our sample emphasized a felt sense of perpetually debased privacy by declaring one has 'nothing to hide'. This mindset appears most similar to *privacy as forsaken* identified by James (2014), who found that about half of the teen participants in his research, regardless of age, held this mindset. In our own sample of teens, references to 'having nothing to hide' were concentrated among those aged 15 and older (31 references), with only three references made by youth aged 13 and 14. The majority of references were made by females (20), with only three made by males. Overall, 26 references were made by youth in Cyber City, and eight in Cyberville. 'Nothing to hide' references are here concentrated among older, urban-based female teens. Participants' experiences reveal that parenting styles are relevant in helping instill this mindset. For instance, two 17-year-old females from Cyberville, engaged in a discussion of parental monitoring, raised this issue:

> Carolyn: When I was younger, my mom would like …go through [my] Facebook friends, and be like 'how do you know this person?' …but like now we're older, I think she thinks you're responsible enough now to know.
>
> Rebecca: My parents don't have any set rules on me because I don't do anything anyway.

This notion of 'not doing anything anyway' buttresses a sedimented notion of personal responsibility for managing risk online (akin to James' (2014) privacy mindset 'privacy in your own hands') and the notion that parents' role in their children's self-management of risk

becomes increasingly reduced as youth age. As one participant, rather strikingly, suggests, "I feel it's probably like a 90 [%] individual, 10% parents should also be involved in it" (Helen, 16, Cyber City). Similar remarks were made across our focus group discussions as a whole, such as this exchange between two 19-year-old male students from Cyberville:

> RESEARCHER: When you think of online messages and safety and all that kind of stuff, do you think it's up to you guys to monitor it?
>
> David: Yes, it is.
>
> Donald: Yeah.
>
> David: It's our choice to do what we gotta do to make our news and our things that we put on social media.

This exchange alludes to the general emphasis on personal responsibility that appears hegemonically ingrained in individuals by the time they reach their 20s. Said another way, there appears to be a clear individualization of and internalization of responsibility for each youth's online profile.

More strikingly, some youth alluded to an *expectation* of debased privacy. Victoria, a 17-year-old female from Cyber City, expressed this 'privacy as forsaken' mentality most explicitly:

> RESEARCHER: What do you think about these [risks], are you constantly checking old posts, kind of managing your online [presentation]?
>
> Victoria: I mean I used to, I used to go back and be like 'I need to delete this', but I think I've cleaned it up enough that I don't have to worry about it, but also as I [have] gotten older and more experienced with the internet I guess, I kind of realized, *I don't have any expectation of privacy when I'm posting things*, and I find myself kind of using it less and less, and I kind of stick to more personal social media like Snapchat, and just individually

> texting people, I don't really post anything on Facebook or Instagram. *…you shouldn't really expect to have privacy in general …generally if you play it safe it's not a big deal*. [added emphasis]

In sum, participants generally felt that by high school, "it was just assumed you knew" how to manage oneself regarding youth engagement online (Yasmin, 18, Cyber City).

These statements represent a different dynamic than previous studies examining privacy mindsets (e.g., Acquisti & Gross 2006; Altheide 2000; Youn 2005). With the rapidly changing social media landscape over the last decade, we turn to discussions over newer SNS such as Snapchat, which continued to raise the theme of 'nothing to hide', but nevertheless alongside impression management strategies to mitigate context collapse.

MOVING BEYOND FACEBOOK: IT'S ABOUT PRIVACY MANAGEMENT

The teens in our focus groups, in line with previous research, brought up a number of strategies they actively use to manage their online privacy. By only a slight margin, the most frequently identified strategy employed is blocking users perceived as threatening or undesirable, followed closely by deleting negative comments, and adjusting privacy settings. The majority of those who made reference to such strategies are aged 13-14 and female (no discernable trends are identified by location of residence). Our findings are consistent with Acquisti & Gross (2006), who found statistically significant higher average concerns for privacy among females compared with males, and Youn (2005:105), whose sample of US teens revealed that "girls perceived more risk from information disclosure, whereas boys perceived more benefits from information disclosure and were willing to provide more information to a Web site." Our own discussions demonstrated the saliency of privacy management strategies for younger teens, with a gravitation

towards espousing ‘not doing anything wrong’ and therefore having, in different terms, no discreditable or hidden stigma waiting to be exposed as they age (Goffman 1963).

A prominent theme among our participants is the gravitation away from Facebook, in preference for newer SNS platforms, although Facebook did still remains central in the online lives of rural and urban participants. However, both academic and popular sources have observed Facebook’s decline of popularity amongst teens (Lang February 21, 2015; Marwick & boyd 2014). A central explanation is that as wider adult sectors of the population—especially parents and relatives—join Facebook, they encroach on what was perhaps once a uniquely youth-dominated space. boyd (2014), for instance, found teens who were early adopters of Twitter, Tumblr and Instagram explained their preference for these newer SNS based on parental ignorance of their existence (see boyd 2014:59). Our focus group discussions revealed how much of this transition—the move away from Facebook as the most prominently used SNS—involves concerns over privacy and online impression management (Livingstone 2008; Marwick & boyd 2011). This is presciently recognized by Vickery (2015:289), who argues “the use of different platforms is a deliberate privacy strategy intended to resist the ways social media industries attempt to converge identities, practices, and audiences.” Our participants pinpoint who makes up these audiences. A representative summary comes from Christine, a 19-year-old undergraduate student from Cyber City:

> …my Facebook is for family and how I want to present myself professionally, and then my Instagram is like, I guess how I want to present myself to friends and then, but my Snapchat is like where I present myself, like *my real self* I guess, is where like they see me doing stupid things… [added emphasis]

As expressed by Christine, youth use social media to manage a variety of impressions to different audiences. Some of our participants spoke about a sense of authenticity felt on Snapchat, while the self is strained in its inauthentic articulations on older and more established SNS like Facebook, which is more prone to the risk of context collapse (cf. Goffman 1959). Participants identified several alternative SNS to Facebook, usually Twitter, Instagram, and Snapchat. Often, they preferred these sites due to their more focused features and the perceived simplicity of use (e.g., sharing pictures and videos). However, our discussions revealed an important underlying draw: the newer SNS enabled a stronger sense of agency, and thus independence, among participants in terms of their ability to manage privacy and their audiences. For instance, 17-year-old Zoey from Cyberville stated "Twitter you can block people easily, you just hit it, hit your settings, block, then they're gone, but Facebook and stuff it's harder." Christine recollects that initially her Facebook included only "very intimate friends" but has now grown to about 800 people which she admits to not frequently interacting with. She compares this with Snapchat, which "is usually connected to your contacts on your phone," which enables her to

> pick who I don't want to see my stories so it's very like, these are the people who I'm like, like I *trust the most* and that's why the privacy settings… [if] I don't want them to see my story, I can block them from my story or I can …like delete them. [added emphasis]

Yet, the practice of "deleting" someone or, more notably, being "deleted" also generated concern. Some participants, for example, worried that blocking others or not using certain SNS would lead to their social exclusion and losing control of their 'definition of the situation' online (see Thomas and Thomas, 1928). If central to the social process of going online is 'writing

oneself into being' (Sundén 2003), then teens lose the ability to control how others write about their identities if they are not also carefully monitoring what is being posted—a time consuming and worry inducing activity. For instance, blocking was debated in a focus group with four females aged 14 and 15 from Cyber City:

> Nancy: like you can block it …but a lot of the problem is, nobody really wants to block [unwanted contact from school friends] because when you block them, then you're outside the circle, with, where everybody else knows all the information, and you just block them so you don't know anything.

Ashima adds "and you only use that [blocking] if you don't know the person, and they're like trying to get your information; 'Okay you're blocked, I don't want to talk to you." Blocking thus works as a privacy management strategy for strangers but not for those more personal peer networks in school. For teens, the possible emotional turmoil tied to social exclusion and isolation (i.e., the fear of missing out) may supersede the benefits of blocking. *Not* blocking, in sum, works to *control* definitions of the situation and prevent context collapse; it helps address a fear of missing out and being kept 'out of the loop' (James, 2014;). In sum, blocking works on SNS like Facebook, especially with strangers, in order to avoid a 'collision of contexts' (Marwick & boyd 2011), but blocking or other privacy management strategies may become counterproductive on sites like Snapchat and Instagram, given their more intimate peer networks. When discussing newer alternatives such as Instagram and, especially, Snapchat–the most popular actively used SNS amongst our participants–strategies, such as blocking, were less salient given a sense of better security. As with existing studies (boyd 2014; J. Davis & Jurgenson 2014; Utz et al. 2015), for our participants, audiences on Snapchat were usually much smaller and intimate, leading to a sense of greater control over impression management. Lucy, a

17-year-old female from Cyber City, stated that Snapchat is a "more direct" way to communicate with well-known persons. Other groups often strongly agreed when asked if Snapchat was more private than Facebook, arguing that Snapchat is geared for "personal pictures" (David), where the user feels they have control over who has access to them. From Cyber City, 19-year-old Eleanor provided a representative view: "I post more personal stuff on Snapchat, and nothing personal on Tumblr because I have strangers following me and stuff, so I gotta keep it private" (for a different view on Tumblr see Bailey 2015). In a different group Bethany, a 19-year-old female from Cyber City, reflects that she uses Snapchat "for my closest friends and then I can choose who it goes to and who sees it." These statements mimic of Hargittai and Marwick's (2016:3749) young adults who identify sharing content with more "targeted" audiences.

An interesting dynamic emerged, however, during focus group discussions centered on Snapchat. While some participants referred to Snapchat's ostensible security and ephemerality, this was quickly challenged by others. For instance, a group of three 13-year-old females from Cyberville were asked whether they were aware of any "sexting" on Snapchat. Valerie quickly responds "oh my god yeah! …Snapchat's definitely the worst for that!" Others agree. Valerie elaborates:

> because it's like, you only see the pictures for 10 seconds or you can set them for 1, up to 10 seconds, so I guess if someone asks, you can easily just send it, and it'll be on for like 1 second and I guess they don't really have time to screenshot, cuz you can screenshot the picture.

Kimberly then responds: "but then …say I sent a picture to Valerie and then she like screenshots it, I would get the notification that she screen-shotted it." Here Kimberly refers to knowledge regarding how privacy is secured through Snapchat. Despite images that self-destruct, capturing a screen shot of an image on the receiver's phone may be one way to preserve the image being

sent. However, Snapchat's affordances include sending a notification to the distributor of the picture that the receiver has attempted to 'screenshot' the picture. Interestingly, Valerie responds to Kimberly's confidence in the screenshot notification feature of Snapchat:

> Yeah, but there's also an app you can get called Snapsave, and whatever Snapchats you get, it saves onto that, so I've heard of boys who have those apps and they get like pictures from girls and she'll be like, 'I'm sending you so don't screenshot it', and they'll have the app and they're like 'no, of course I won't screenshot it, you can trust me and stuff.'

Valerie here refers to a separate application, Snapsave, that can be used to capture and preserve content sent through Snapchat and avoid notifying the sender of doing so. Other groups also made reference to Snapsave as an app that can be used to compromise privacy, especially related to female users engaging in digital sexual expression. In one such group Emily, a 19-year-old undergraduate student from Cyber City, was caught by surprise by the existence of Snapsave, mentioned by another participant: "that's sneaky, I never knew about [Snapsave], *cuz I have nothing to hide*, if I screenshot it and they know, like why did you screenshot that" [added emphasis]. Emily was not alone in suggesting that privacy concerns (here related to 'sexting') are less relevant if one has "nothing to hide".

Navigating the various labyrinthine permutations of privacy management through applications such as Snapchat involves monumental tenacity and vigilance, not to mention a solid technical knowledge of information communication technologies. The 'nothing to hide' mindset, then, appears to be a generalized adaptation which ultimately points to a pragmatic self-responsibilization. That this responsibility ultimately rests on individual youth (or that they feel this is the case) is problematic. Yet it is also related to what appears to be a conformity to

socially accepted performances (Cooley 1902; Mead 1962 [1934]). The range of acceptable presentations of self is narrowed by the intense social pressures teens face (i.e., from each other and from adult society), exacerbated through the widening of audience online and the difficulties inherent in controlling context collapse.

DISCUSSION

In this paper we explored an apparent incongruence between impression management strategies used by teens to maintain privacy across SNS, as well as a salient privacy mindset of 'having nothing to hide' regarding online activities. The incongruity centers on the question of why impression management strategies are relevant with such a mindset; i.e., why take so much care in managing impressions when one is supposedly not concerned for the content they post? SNS problematize context, leading users to grapple with how to manage contextual integrity given the affordances of SNS, including persistence, searchability, and anonymity (boyd 2008a; Nissenbaum 2011). That our participants adapt in sophisticated ways to manage privacy and simultaneously hold a 'nothing to hide' mindset is not hypocritical – it is at heart a pragmatic adaptation to the present definition of the situation. The cyber-based generalized other today is one where young people feel less like they have lost privacy and more that they "never had it to begin with" (Hargittai & Marwick 2016:3751). Indeed, "I have nothing to hide" may usefully be considered less a mindset than a shift at the level of the generalized other, where youth have learned that online there is no real privacy. This cyber-based generalized other, the broader moral expectation to wider society that the self internalizes, exists alongside the various persistent attempts to manage privacy, but also serves to *pre-empt* context collapse, stigma and victimization (especially in relation to violations such as 'sexting'). These twin aspects, then,

what we argue to be the contemporary adaptation of the privacy paradox, do not merely coexist, they are mutually reinforcing aspects of the "I" and "Me".

Overall, our research builds on knowledge of teen SNS use and their attitudes and actions towards privacy and managing risk online. Similar to extant research, we also find teens express concerns over breaches of their privacy online and are active in their consideration of privacy. However, we highlight strategies involving impression management *across* SNS, especially newer sites such as Snapchat, felt to be more secure by some of our participants. Managing privacy across SNS enhances teens' ability "to exert control over how information flows, who has access to it, and in what context" (Vickery 2015:282; see also Nissenbaum 2011). As Livingstone (2008:408) notes, teens are "found to work with a subtle classification of 'friends', graded in terms of intimacy, which is poorly matched by the notion of 'public' and 'private' designed into social networking sites." The more intricate gradations and subtleties related to affordances match with this more fine-grained view of friends and impression management.

We also highlight the presence of a 'nothing to hide' mindset that appears to grow in salience as teens age, buttressed by the mindset of privacy being 'in your own hands' (James 2014). The latter may be linked to a "broader ethos of individualism" which James (2014:37) found "prevalent in American culture." In Canada, Raynes-Goldie (2010) revealed a shift towards privacy pragmatism as opposed to being unconcerned about privacy, finding the position of 'privacy pragmatism' was most salient among Canadian teens - mirroring other findings in the U.S. at the time. This mindset refers to "people who are concerned about their privacy but are willing to trade some of it for something beneficial." While privacy pragmatism remained salient for our own participants, for older teens the expressions of unconcern became more pronounced. The 'nothing to hide' mindset suggests a fourth typology complementing those identified by

James (2014) highlighted above. This seems to build upon the 'privacy as forsaken' mindset, but differs since it shuns the notion that privacy is relevant if one is not 'doing anything wrong'. Academic focus on the theme of having nothing to hide in relation to privacy management has only recently emerged (e.g., Solove 2007, 2011), arguably due to the saliency of this mindset in relation to online sociality. Our findings suggest that this mindset may sediment as youth reach late adolescence, but this question remains for future research to determine as our sample is relatively small and assumptions regarding maturation effects should not be made here.

Our discussions revealed patterns according to age, more so than gender and location (i.e., urban Western vs. rural Atlantic Canada). However, that more references to feeling a lack of control online and having nothing to hide were made among female participants in Cyber City suggests that societal messages regarding cyber-risk management may be concentrated on females more than males (see Bailey & Steeves 2015; Karaian 2014) but also to those in urban environments moreso than rural ones (see also [Authors] Forthcoming 2019). Further research is warranted, as other studies have not found the relationship between gender and privacy concern to be statistically significant (Lawler & Molluzzo 2010; Paine et al. 2007). Perhaps teens in rural areas have more close-knit connections that undercut the emphasis on the individual to rely on him or herself. Indeed, 13 of our groups, many from rural Cyberville, made references to having close community ties and familiarity in rural regions, including a few participants who had moved from smaller rural areas to larger urban ones. Future researchers should explore this contrast, mining experiences more specifically related to urban and rural social dynamics.

Youth today are growing up immersed in the expectation of the ephemerality of privacy online, and often express that effectively managing it is impossible. Opting out of social networks may secure privacy, but this is an untenable option for youth for whom electing what information to

share through such networks is in itself a form of control over privacy (Bailey and Steeves 2015; Hargittai and Marwick 2016; Livingstone 2008; Marwick and boyd 2011). Moreover, opting out debases youth agency insofar as they are not able to monitor and respond to the digital postings of others, especially as it relates to their sense of identity, and results in a variation of exclusion and isolation from social engagement. The need to control impressions and context also explains why our participants abjured the strategy of 'blocking' other users. This undercuts their ability to control definitions of the situation tied to their reputation among offline peer groups.

Nonetheless, what emerges alongside these discussions is a sidelining of wider concerns related to cyber-bullying, sexting and so forth as germane to deviant 'others', not the participants themselves. In other words, as teens grow older, it is only problematic others who take unnecessary risks; if one has something to hide it is assumed to be illicit (O'Reilly, Karim, Taylor, & Dogra 2011; Solove 2007). What is fundamentally absent is understanding of the personal troubles tied to privacy management. Declaring that one has nothing to hide and is therefore indifferent to monitoring sidelines consideration of situations where one's digital profile can be usurped and privacy breached; for example, through hacking and engaging in 'revenge porn' (Stroud 2014). Such a declaration also sidelines the significance of privacy in any number of scenarios youth may wish to engage in, such as digital activism (Wilson & Hayhurst 2009), consenting digital sexual expression (Koskela 2006) and managing discreditable stigma (Goffman 1963). Moreover, atomistic conceptions of risk and privacy obfuscate critical attention to the corporate collection of data and the alignment of social media platforms and 'big data' with corporate surveillance and targeted advertising (Marx & Steeves 2010; Steeves 2012; see also Anthony et al. 2017). As Livingstone (2008:56) here too notes, "unlike privacy advocates and more politically conscious adults, teens aren't typically concerned with governments and

corporations. Instead, they're trying to avoid surveillance from parents, teachers, and other immediate authority figures in their lives." Indeed, our participants demonstrated concerns for what can be considered horizontal privacy (i.e., privacy from offline peer groups), and not so much vertical privacy (i.e., privacy from authorities and institutions). In sum, the problem with the question 'if you've got nothing to hide, what do you have to fear?' lies in the question itself (Solove 2007).

Our study and ones like it, which draws from a micro-Goffmanian analysis of attitudes and perceptions, offers important advances in the broader sociology of surveillance (e.g. Anthony et al. 2017; Lyon, 2007). Zureik (2010b), for instance, argues that privacy has two aspects: a Goffmanian focus on role playing geared to manage and protect personal privacy, and "our having to safeguard against state and private-sector incursions into the private domain" (p. 6). Zureik (2010b) is explicit that her edited collection focuses on the latter. Broader sociological implications regarding how surveillance aligns with systems of social control and debased privacy, social cohesion and structural inequalities are significant areas of ongoing research (Anthony et al. 2017). Anthony et al. (2017) argue that most research on privacy centers on "micro-level outcomes" such as "individual concerns, relationships, and disadvantages." However, they also put forth that,

> Changes in privacy …also affect the kinds of information people receive about government and other significant institutions, and thus have implications for trust and institutional legitimacy. Information flows also affect the relationships that underlie at least some forms of collective action and challenges to authority. (p. 258)

As such, research, according Anthony and colleagues, should expand on exploring "implications of shifts in network structures across social contexts" (p. 258) in order to elicit wider patterns

related to social capital, cohesion and social order. Ignorance of the importance of privacy and a broader sociological imagination connecting personal privacy troubles to such public issues (Mills 1959; see also Phillips and Curry 2003) only serves to reinforce emerging systems of power connected to the broader classification (i.e., social sorting) and profiling of society (Lyon, 2003). Given a lack of focus in sociological research, part of the challenge in researching privacy comes from pulling from differing paradigms such as law, geography and communication studies (e.g, Petronio 2002). As Lyon (2003) argues,

> Surveillance studies today is marked by an urgent quest for new explanatory concepts and theories. The most fruitful and exciting ones are emerging from transdisciplinary work, involving, among others, sociology, political economy, history, and geography. (p. 27).

An eclectic approach that draws from cross-cultural research is especially warranted. This is evident when considering the international Globalization of Personal Data (GPD) survey (i.e., The Surveillance Project) conducted by researchers at Queen's University (see Chan et al. 2008). Grenville (2010) usefully contextualizes Canada's findings in comparison with seven other countries. His analysis of the GPD data reveals that Canadians and Americans are more resistant to surveillance of personal data, especially in relation to businesses (e.g., refusing to give personal information deemed superfluous to a business that requests it, or purposefully giving incorrect information to a marketer (see Grenville 2010:72). Additionally, Canadian survey respondents expressed a marked lack of control over their information online (see Grenville 2010:75). Overall, across countries, three main groups are identified: informed resisters (26%), those satisfied with the 'status quo' (i.e., existing practices online and experiences of being surveilled (41%) and alienated skeptics (33%) (Grenville 2010:76). Alienated skeptics appear

most similar to the youth in our sample: they have a sense of powerlessness, lack a sense of control over their information, and lack knowledge of surveillance technologies and related laws governing privacy (Grenville 2010:76-77). Yet the alienated skeptics are also dissimilar insofar as they are "the most upset about what they see as invasions of their privacy" (Grenville 2010:78).

The GPD offers the first international survey of surveillance and privacy; its findings will no doubt continue to inform our broader comparative understanding of surveillance in sociological context. However, it is unclear from Grenville's analysis how youth differ from adults both within Canada and across countries. Such international comparisons, of course, suffer from epistemological and methodological challenges related to what is being measured and how the comparisons are being interpreted (see Zureik 2010a). Perhaps the categorizations explicated by Grenville (2010) are best understood as ideal types requiring further attention to the hermeneutic nuances of participant understandings and practices. For instance, our participant focus group discussions reveals practices of resistance and simultaneous espousals of acquiescence, taking on aspects of both resistance and skepticism. Broader sociological analyses, we argue, should thus be complemented by further ethnographic work seeking to unpack both attitudes and perceptions alongside actual behaviors in situated contexts (cf. Livingstone and Sefton-Green 2016).

Our Goffmanian framework also helps provide important context and interpretive details to wider national and international samples. We thus agree with Haggerty's (2006:42) observation that research on contemporary forms and contexts of surveillance, often presuming top-down forms of governance, inadvertently exclude the "actual experiences of people being subjected to different governmental regimes," and that "modestly realist projects" are required "that analyze the politics of surveillance on the experiences of the subjects of surveillance" (p. 42).

Marx (2003) observed that a person's ability to refuse and ignore surveillance was not a very common response among research participants. This trend may well be reversing for teens growing up with today's SNS. Consider Nissenbaum's (2011:45) observation "if people expect to be monitored, if they anticipate that their recorded views will be shared with particular third parties for money or favors, they are likely to be more watchful, circumspect, or uncooperative." This adjustment to the expectation of surveillance may not be as relevant to teens today given some appear to have internalized the mindset of having nothing to hide; or knowing that they cannot hide anything online. Curiously, while fewer in number, some of our younger participants (i.e., 13 years of age) seem to have at their disposal the same social vocabulary of motive regarding personal responsibility as older teens. This too behooves further research to clarify the question of whether children and 'tweens' entering adolescence are qualitatively different than the 'digital natives' (Prensky 2001) who grew up immersed in technology before them. In this context, we also had a few older participants refer to their younger siblings in contrasting ways: either as more irresponsible online or as more mature. What are the factors that shape these differences, and is more than just age at play? What is certain, however, is that in the rapidly changing technological landscape, it is not clear whether youth are growing up more critically engaged with issues of privacy and cyber-risk. Thus, developing teens' skills is crucial, not only related to privacy management, but a broader sociological imagination regarding their self in relation to society and citizenship.

ACKNOWLEGMENTS

Thanks to the Social Sciences and Humanities Research Council of Canada for funding this research. The authors would like to thank the reviewers of this paper for their time and efficiency during an exemplary peer review process, especially editors Depelteau and Adams.

ENDNOTES

1 – We draw from the World Health Organization's definition of adolescents as those between 10 and 19 years of age, as opposed to 'youth' more widely, defined by the United Nations as those 15-24 years of age.

See http://apps.who.int/adolescent/second-decade/section2/page1/recognizing-adolescence.html

REFERENCES

Acquisti, A., and R. Gross. 2006. *Imagined communities: Awareness, information sharing, and privacy on the Facebook.* Paper presented at the International workshop on privacy enhancing technologies.

Agatston, P., R. Kowalski, and S. Limber. 2007. Students' Perspectives on Cyber Bullying. *Journal of Adolescent Health* 41(6):S59-S60.

Anthony, D., C. Campos-Castillo, and C. Horne. 2017. Toward a Sociology of Privacy. *Annual Review of Sociology* 43:249-269.

Altheide, D. 2000. Identity and the Definition of the Situation in a Mass-Mediated Context. *Symbolic Interaction* 23(1):1-27.

Bailey, J. 2015. A Perfect Storm: How the Online Environment, Social Norms, and Law Shape Girls' Lives. In J. Bailey & V. Steeves (Eds.), *eGirls, eCitizens* (pp. 22-46). Ottawa: University of Ottawa Press.

Bailey, J., and V. Steeves. (Eds.). 2015. *eGirls, eCitizens*. Ottawa: University of Ottawa Press.

Barnes, S. 2006. A Privacy Paradox: Social Networking in the United States. *First Monday* 11(9-4): http://firstmonday.org/article/view/1394/1312. Accessed Mar 2018.

Berg, B. 2004. *Qualitative Research Methods for the Social Sciences* (5th ed.). Long Beach: Pearson.

boyd, d. 2002. *Faceted ID/entity: Managing representation in a digital world.* (MA), Massachusettes Institute of Technology, Cambridge, MA.

boyd, d. 2008a. *Taken Out of Context: American Teen Sociality in Networked Publics.* University of California, Berkeley.

boyd, d. 2008b. Why Youth ♥ Social Network Sites: The Role of Networked Publics in Teenage Social Life. In D. Buckingham (Ed.), *Youth, Identity, and Digital Media* (pp. 119–142). Cambridge, MA: The MIT Press.

boyd, d. 2014. *It's Complicated: The social lives of networked teens*. London: Yale University Press.

Brandimarte, L., A. Acquisti, and G. Loewenstein. 2013. Misplaced confidences: Privacy and the control paradox. *Social Psychological and Personality Science* 4(3):340-347.

Burkell, J., & M. Saginur. 2015. "She's Just a Small Town Girl, Living in an Online World": Differences and Similarities between Urban and Rural Girls' Use of and Views about Online Social Networking. In J. Bailey & V. Steeves (Eds.), *eGirls, eCitizens* (pp. 129-152). Ottawa: University of Ottawa Press.

Chan, Y., L.L.H. Stalker, D. Lyon, A. Pavlov, J. Sharpe, E. Smith, D. Trottier, and E. Zureik. 2008. *The Globalization of Personal Data Project: An International Survey on Privacy and Surveillance. Summary of findings November 2008*. Kingston: Queen's University.

Cooley, C. 1902. *Human Nature and the Social Order*. New York: Scribners.

Davis, J., and N. Jurgenson. 2014. Context collapse: theorizing context collusions and collisions. *Information, Communication & Society* 17(4):476-485.

Davis, K. 2012. Tensions of identity in a networked era: Young people's perspectives on the risks and rewards of online self-expression. *New Media & Society* 14(4):634-651.

Dommeyer, C., & B. Gross. 2003. What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing*, 17(2):34-51.

Erickson, R.J. 1995. The Importance of Authenticity for Self and Society. *Symbolic Interaction* 18(2):121-144.

Fisk, N. 2016. *Framing Internet Safety: The Governance of Youth Online*. Cambridge: The MIT Press.

Goffman, E. 1955. On face-work. *Psychiatry* 18(3):213-231.

Goffman, E. 1959. *The presentation of self in everyday life*. Garden City, N.Y.: Doubleday.

Goffman, E. 1963. *Stigma*. New Jersey: Prentice-Hall.

Grenville, A. 2010. Shunning surveillance or welcoming the watcher? Exploring how people traverse the path of resistance. In E. Zureik, L. H. Stalker, & E. Smith (Eds.), *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons* (pp. 70-83). Montreal: McGill-Queen's Press.

Haggerty, K. 2006. Tear down the walls: on demolishing the panopticon. In D. Lyon (Ed.), *Theorizing Surveillance: The panopticon and beyond* (pp. 23-45). Mill Street, Uffculme: Willan Publishing.

Hampton, K. 2016. Persistent and pervasive community: New communication technologies and the future of community. *American Behavioral Scientist*, 60(1):101-124.

Hargittai, E., and A. Marwick. 2016. "What Can I Really Do?" Explaining the Privacy Paradox with Online Apathy. *International Journal of Communication* 10:3737–3757.

James, C. 2014. *Disconnected: Youth, New Media, and the Ethics Gap*. Cambridge: The MIT Press.

Karaian, L. 2012. Lolita Speaks: 'Sexting', Teenage Girls and the Law. *Crime Media Culture* 8(1):57-73.

Karaian, L. 2014. Policing 'sexting': Responsibilization, respectability and sexual subjectivity in child protection/crime prevention responses to teenagers' digital sexual expression. *Theoretical Criminology* 18(3):282-299.

Keeler, M. 2006. *Nothing to Hide: Privacy in the 21st Century*. Lincoln, NE: iUniverse.

Koskela, H. 2006. 'The other side of surveillance': webcams, power and agency. In D. Lyon (Ed.), *Theorizing Surveillance: The panopticon and beyond* (pp. 163-181). Collumpton, Devon: Willan Publishing.

Lang, N. February 21, 2015. Why teens are leaving Facebook: It's 'meaningless'. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-intersect/wp/2015/02/21/why-teens-are-leaving-facebook-its-meaningless/?utm_term=.4e93fc7dd067, Accessed March 2018.

Lawler, J., and J. Molluzzo. 2010. A Study of the Perceptions of Students on Privacy and Security on Social Networking Sites (SNS) on the Internet. *Journal of Information Systems Applied Research* 3(12):1-18. http://jisar.org/13/12/.

Lenhart, A. 2009. *Teens and Sexting: How and why minor teens are sending sexually suggestive nude or nearly nude images via text messaging*. Retrieved from Washington, D.C.: http://www.pewinternet.org/Reports/2009/Teens-and-Sexting.aspx

Livingstone, S. 2003. Children's use of the internet: reflections on the emerging research agenda. *New Media & Society* 5(2):147–166.

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.

Livingstone, S. 2009. *Children and the Internet: Great expectations, challenging realities*. Malden, MA: Polity Press.

Livingstone, S., and J. Sefton-Green. 2016. *The Class: Living and Learning in the Digital Age*. New York: New York University Press.
Lyon, D. 2003. Surveillance as social sorting: Computer codes and mobile bodies. In D. Lyon (Ed.), *Surveillance as Social Sorting: Privacy, risk, and digital discrimination* (pp. 13-30). London: Routledge.
Lyon, D. 2007. *Surveillance studies: An overview*. Cambridge: Polity Press.
Madriz, E. 1997. *Nothing Bad Happens to Good Girls: Fear of Crime in Women's Lives*. Berkeley: University of California Press.
Madriz, E. 2000. Focus Groups in Feminist Research. In N. Denzin & Y. Lincoln (Eds.), *Handbook of Qualitative Research* (2nd ed., pp. 835-850). Thousand Oaks: Sage.
Marker, B. 2011. *Sexting as Moral Panic: An Exploratory Study into the Media's Construction of Sexting.* (Masters of Science), Eastern Kentucky University, Richmond, Kentucky.
Marwick, A., & d. boyd. 2011. I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New Media & Society* 13(1):114-133.
Marwick, A., & d. boyd. 2014. 'It's just drama': Teen perspectives on conflict and aggression in a networked era. *Journal of Youth Studies* 17(9):1187-1204.
Marx, G. 2003. A Tack in the Shoe: Neutralizing and Resisting the New Surveillance. *Journal of Social Issues* 59(2):369-390.
Marx, G., and V. Steeves. 2010. From the beginning: Children as subjects and agents of surveillance. *Surveillance & Society* 7(3/4):192-230.
Mead, G.H. 1962 [1934]. *Mind, Self, and Society: From the Standpoint of a Social Behaviorist*. Chicago: University of Chicago Press.
Mills, C.W. 1959. *The Sociological Imagination*. Harmondsworth: Penguin.
Morgan, D. 1997. *Focus Groups as Qualitative Research* (2nd ed.). California: Sage.
Nissenbaum, H. 2004. Privacy as contextual integrity. *Washington Law Review* 79:119-158.
Nissenbaum, H. 2011. A contextual approach to privacy online. *Daedalus* 140(4):32-48.
Nussbaum, E. Feb 12, 2007. Kids, the internet, and the end of privacy: The greatest generation gap since rock and roll. *New York Magazine*. Retrieved from http://nymag.com/news/features/27341/. Accessed March 2018.
O'Reilly, M., K. Karim, H. Taylor, and N. Dogra. 2011. Parent and child views on anonymity: 'I've got nothing to hide'. *International Journal of Social Research Methodology* 15(3):211-223.
Paine, C., U.-D. Reips, S. Stieger, A. Joinson, and T. Buchanan. 2007. Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies* 65(6):526–536.
Pelfrey, W., and N. Weber. 2014. Talking smack and the telephone game: Conceptualizing cyberbullying with middle and high school youth. *Journal of Youth Studies* 17(3):397-414.
Petronio, S. 2002) *Boundaries of privacy: Dialectics of disclosure*. Albany: State University of New York Press.
Phelps, J., G. Nowak, and E. Ferrell. 2000. Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing* 19(1):27-41.
Phillips, D. and M. Curry. 2003. Privacy and the phenetic urge: Geodemographics and the changing spatiality of local practice. In D. Lyon (Ed.), *Surveillance as social sorting: Privacy, risk and digital discrimination* (pp. 137-152). London: Routledge.

Prensky, M. 2001. Digital Natives, Digital Immigrants Part 1. *On the Horizon* 9(5):1-6. http://dx.doi.org/10.1108/10748120110424816 (accessed March 2018).

Raynes-Goldie, K. 2010. Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday* 15(1-4), Available at: http://firstmonday.org/ojs/index.php/fm/article/viewArticle/2775/2432. Accessed March 2018.

Regan, P., and V. Steeves. 2010. Kids R Us: Online Social Networking and the Potential for Empowerment. *Surveillance & Society* 8(2):151-165.

Robinson, L. 2007. The cyberself: the self-ing project goes online, symbolic interaction in the digital age. *New Media & Society* 9(1):93-110.

Shackford, S. June 12, 2013. 3 Reasons the 'Nothing to Hide' Crowd Should Be Worried About Government Surveillance. Retrieved from http://reason.com/archives/2013/06/12/three-reasons-the-nothing-to-hide-crowd. Accessed March 2018.

Solove, D. 2007. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review* 44:745-772.

Solove, D. 2011. *Nothing to hide: The false tradeoff between privacy and security*. New Haven: Yale University Press.

Steeves, V. 2012. Hide and Seek: Surveillance of Young People on the Internet. In D. Lyon, K. Haggerty, & K. Ball (Eds.), *The Routledge Handbook of Surveillance Studies* (pp. 352-359). New York: Routledge.

Steeves, V. 2014. *Young Canadians in a Wired World, Phase III: Life Online*. Ottawa: MediaSmarts.

Stewart, D., P. Shamdasani, and D. Rook. 2007. *Focus Groups, Theory and Practice* (2nd ed.). London: Sage.

Strauss, A., and J. Corbin. 1990. *Basics of qualitative research: Grounded theory procedures and techniques*. Newbury Park: Sage.

Stroud, S. 2014. The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn. *Journal of Mass Media Ethics* 29(3):168–183.

Sundén, J. 2003. *Material Virtualities: Approaching Online Textual Embodiment*. New York: Peter Lang.

Thomas, W.I. and D.S. Thomas. 1928. *The Child in America*. New York: Alfred A. Knopf.

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.

Twinn, S. 1998. An analysis of the effectiveness of focus groups as a method of qualitative data collection with Chinese populations in nursing research. *Journal of Advanced Nursing* 28(3):654-661.

Tynes, B. 2007. Internet safety gone wild? Sacrificing the educational and psychosocial benefits of online social environments. *Journal of Adolescent Research* 22(6):575-584.

Utz, S., N. Muscanell, and C. Khalid. 2015. Snapchat elicits more jealousy than Facebook: a comparison of Snapchat and Facebook use. *Cyberpsychology, Behavior, and Social Networking* 18(3):141-146.

Vickery, J. 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.

Wang, Y., G. Norcie, S. Komanduri, A. Acquisti, P. Leon, and L. Cranor. 2011. I regretted the minute I pressed share: A qualitative study of regrets on Facebook. *Proceedings of the seventh symposium on usable privacy and security*:1-16.

Wilson, B., & L. Hayhurst. 2009. Digital Activism: Neoliberalism, the Internet, and Sport for Youth Development. *Sociology of Sport Journal* 26(1):155-181.

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.

Zhao, S. 2005. The Digital Self: Through the Looking Glass of Telecopresent Others. *Symbolic Interaction* 28(3):387-405.

Zureik, E. 2010a. Cross-cultural study of surveillance and privacy: Theoretical and empirical observations. In E. Zureik, L. H. Stalker, & E. Smith (Eds.), *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons* (pp. 348-359). Montreal: McGill-Queen's Press.

Zureik, E. 2010b. Introduction: Methodological considerations. In E. Zureik, L. H. Stalker, & E. Smith (Eds.), *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons* (pp. 5-7). Montreal: McGill-Queen's Press.