Interpersonal Surveillance on Social Media

Daniel Trottier
Uppsala University, Sweden

ABSTRACT *This article examines changing rules and regimes of visibility on social media, using Facebook as a case study. Interpersonal social media surveillance warrants a care of the virtual self. Yet this care is complicated by social media's rapid growth, and especially Facebook's cross-contextual information flows that publicize otherwise private information. Drawing from a series of thirty interviews, this article focuses on how users perceive and manage their own visibility and take advantage of the visibility of other users. These experiences are tied to shifting understandings of private and public information, as well as new terms like "stalking" and "creeping" that frame surveillant practices.*

KEYWORDS *Surveillance; Privacy; New media; Social media*

RÉSUMÉ *Cet article examine l'évolution des règles et des régimes de visibilité sur les médias sociaux, en utilisant Facebook comme une étude de cas. La surveillance interpersonnelle sur les médias sociaux nécessite un soin de l'être virtuel. Pourtant, ce soin est compliqué par l'expansion rapide des médias sociaux, et en particulier la nature inter contextuel de Facebook, qui diffuse de l'information privé. Tirant d'une série de trente entrevues, cet article concentre sur la manière dont les utilisateurs perçoivent et gèrent leur proper visibilité sur Facebook ainsi que de profiter de la visibilité des autres. Ces expériences sont liées à l'évolution des conceptions de l'information publique et privée, ainsi que de termes nouveaux comme «harcèlement» et «stalking» qui caractérise la surveillance sur les médias sociaux.*

MOTS CLÉS *Surveillance; La vie privée; Les médias nouveaux; Les médias sociaux*

Introduction

This article addresses one axis of visibility on social media, interpersonal surveillance, using Facebook as a case study. In adopting Facebook as a platform for interpersonal communication, these relations become more surveillant. Users grow comfortable sharing with their peers, but at the same time are troubled by the cumulative exposure to those peers, and others. Interpersonal social media surveillance renders users visible to one another in a way that warrants a care of the virtual self (Whitson & Haggerty, 2008), including both self-scrutiny, and watching over what peers upload, as this may reflect poorly on oneself. Yet even this care is complicated by social media's rapid growth, and especially Facebook's cross-contextual information flows that publicize otherwise private information. Visibility on social media makes this care necessary, but not sufficient.

Daniel Trottier is a postdoctoral fellow in the Department of Informatics and Media at Uppsala University, Sweden. Email: dan.trottier@gmail.com .

Canadian Journal of Communication Vol 37 (2012) 319-332

This article uses ethnographic accounts to describe interpersonal surveillance made possible through Facebook. The findings below present interpersonal surveillance as a matter of users being both the subject and the agent of surveillance. Facebook is an exemplar of social media. Nearly one billion users (FB Statistics, 2011) maintain profiles, upload photographs, and share personal information with each other. Facebook shares some features with other social media, like the pervasive construction of an online presence, populated by personal information, but it stands out from many other services, as this presence exceeds any specific social context. Facebook's users make their lives visible to each other, and this exchange enables unanticipated kinds of visibility.

Literature review

User adoption of social media is a new kind of visibility, wherein everyday interactions more closely resemble surveillance. Surveillance refers to the covert, sustained, and targeted collection of information, often about an individual or group of individuals (Lyon, 2001). Surveillance is more than data collection because it relies on mediated relations, profiling, and asymmetrical relations of visibility. It is the dominant organizational logic of late modernity. Facebook, for instance, organizes relations between peers. Not only are interpersonal social ties mediated on an organizational platform, but interpersonal activity also becomes asynchronous. Users watch over each other, as opposed to communicating directly with one another. Other kinds of surveillance take place through Facebook (Trottier, 2011), but peer relations also become more surveillant in nature.

Users experience interpersonal surveillance as a violation, but also come to see it as a pervasive condition of social media, suggesting a further normalization of surveillance (Murakami Wood & Webster, 2009). The intervisibility (Brighenti, 2010) these individuals exhibit and exploit is an increasing feature of contemporary sociality. Interpersonal surveillance is also mutual on social media, as users are able to watch and be watched. The fact that users can choose to watch others as well as make themselves visible adds an empowering dimension to this surveillance (Koskela, 2004; Albrechtslund, 2008), and our respondents were comfortable with some aspects of this visibility. But intentional visibility cannot be disassociated from unanticipated exposure. One function "creeps" into another, and information "leaks" to new contexts (Lyon, 2001).

Scholars like Andrejevic (2005) describe a cultural climate that compels individuals to watch over untrustworthy peers. Yet, an increased reliance on surveillance technology, as we will see, furthers the risk of exposure, and the need to be vigilant. As services like Facebook are intimately tied to both identity and communication, they shape how we are perceived and how we interact with others. This warrants what Whitson and Haggerty (2008) call the virtual care of the self, "whereby citizens are encouraged, enticed and occasionally compelled into bringing components of their fractured and dispersed data double into regular patterns of contact, scrutiny and management" (p. 574). New risks emerge as a result of offloading social processes online. Whitson and Haggerty identify practices that mitigate the risk of identity fraud. With Facebook, personal reputation is at stake. The findings below suggest users are sorting out responsible use among themselves, but that this is a complex and occasionally contradictory project.

Lateral surveillance is a product of the domestication of media technology. Domestication literature (Silverstone & Haddon, 1996) recognizes technology as a lived experience, and anticipates a qualitative focus on user reception of social media for interpersonal surveillance. Domestication addresses how information and communication technologies are integrated into everyday life, with a focus on the tensions that emerge in consequence. The struggle between privacy and public exposure is a concern, as is the tension between the familiar and the strange when interpersonal relations are mediated (Silverstone & Haddon, 1996). Social media connect familiar relations to unfamiliar and often unwanted kinds of exposure, as a result of the accumulation of personal information and social ties. Also, following Whitson and Haggerty (2008), reputations on social media are treated as an individual responsibility, while in practice exceeding individual control.

Social media adoption endangers privacy, and this troubles users. But privacy is not clear-cut. In its simplest terms, surveillance is a process, and privacy is a value that is endangered by this process. Loss of privacy means unwanted exposure, an inability to manage one's reputation, and a compromised virtual self. Scholars and users both approach social media surveillance by way of privacy, yet these sites underscore the complexity of understanding and maintaining privacy (Nippert-Eng, 2010). Users reconsider while actively managing their privacy on social media (boyd, 2008; West, Lewis & Currie, 2009). These users were experienced in maintaining a degree of privacy from parents prior to social media, and these experiences inform their use of sites like Facebook. But they do not just hide information from some users; they actively share it with others. Users maintain a trade-off between ensuring privacy and achieving public exposure when placing their personal content on Facebook (Tufekci, 2008; boyd & Hargittai, 2010).

Research questions

Facebook mediates social life, often in a public way. Surveillance on social media is more pervasive than a series of incidents. It is increasingly a lived condition, a product of ubiquitous mobile technology and a rapidly growing user base. In light of these developments, scholarly research needs to interrogate the conditions surrounding peer visibility on sites like Facebook. This research asks: what compels users to engage in Facebook surveillance, how do they perceive these conditions of visibility, and how do they manage their online presence?

Privacy as a value is being reconfigured through users' familiarity with social media. They may experience privacy violations, but these violations are part of a normalization of social media visibility. For this reason, this article not only positions privacy concerns alongside publicity, but also situates these values alongside users' broader experiences with Facebook. Findings in this article are thematically presented along a narrative charting exposure to, use of, and familiarity with Facebook. Joining Facebook appears to be a decision that results from peer pressure and convenience. Users then come to realize surveillance and visibility are at the heart of the interpersonal use of Facebook. They describe these practices through terms like "creeping" and "stalking." These experiences also lead to a reconsideration of privacy and publicity. Users then develop a set of tactics to manage more problematic forms of exposure.

They also regard users as being responsible for caring for their virtual selves, while acknowledging the difficulties involved in this task.

Methodology

I conducted semi-structured, in-depth interviews to consider how users coped with peer-to-peer surveillance. A convenience sample of thirty undergraduate students who use Facebook were selected for study. Participants were all enrolled at the same mid-sized Canadian university at the time. These students were selected from all faculties at this university and were recruited through a series of posters on campus, as well as notices sent by email to undergraduate mailing lists. Of the thirty students interviewed, twenty-three were women and seven were men. As women are both more likely to use socal media in Canada (Dewing, 2010) and to participate in studies (Sax, Gilmartin, & Bryant, 2003), this was expected. Seven respondents were in the first year of their studies, eight were in their second year, five were in their third year, seven were in their fourth year, and three were in their fifth year. Twenty-six students were in the faculty of arts and sciences, three were in health sciences, and one student was in the faculty of education. Twenty-seven students checked their Facebook account at least once a day. The three that did not perform daily checks instead received email notifications from Facebook. Interviews focused on a set of themes, including describing respondents' Facebook usage over time, the types of personal information made available to others and the reasons for doing so, the types of personal information acquired from others through Facebook and the reasons for doing so, and the perceptions of information exchange on Facebook. When quoted, respondents are identified by their program, year of study, and gender. Interviews were recorded as MP3 audio files, manually transcribed, and coded based on interview questions as well as additional themes that emerged during the interviews.

The interviews are with one population at a specific period of Facebook's growth; yet, these findings can be generalized, as the conditions of visibility that respondents describe are common to all users. This research focuses on undergraduate students because they were the first population to embrace Facebook. Many respondents report being users since it first became available. Although it has since grown to a more mainstream status, these students belong to the population most familiar with the service. Users have a broad and extended presence on social media, and they are committed to this presence. Their attitudes and behaviours are guided by a care of the virtual self-compelling them to manage their reputation online. Many students use Facebook to maintain social relations with friends and family elsewhere, as well as foster new relations with other students. At the same time, they are also entering adulthood and either the job market or postgraduate studies, and thus are increasingly concerned with their public exposure.

Ties that bind: Peer pressure and convenience

Many respondents felt compelled to join Facebook due to peer pressure, either from new friends at university or high school classmates. Peer pressure went beyond recommendation or prescription. Some respondents had friends who constructed profiles on their behalf, and then transferred control of this nascent profile to them. In more

extreme cases, non-users learned that Facebook contained photos and other content about them. This perplexed people who were not familiar with the kinds of visibility in which they were implicated:

> I was like, "How can pictures of me be on the Internet?" They would show me and they'd show a picture of me with other people and they'd show comments that other people had made and, like, "How are people making comments on this photo of me and I don't even know it's there? I should be involved in this. I should know what's going on." (Artsci2W)

Many respondents realized they already had a presence on Facebook, even if they never intended to join the site. This presence was only manageable by becoming a Facebook user.

Though respondents often joined Facebook because of peer pressure, they stuck around because of its social convenience. Facebook was often used for on-campus coordination, like broadcasting one's presence in the library, or requesting class notes. In other cases, it was used for a more spectacular kind of visibility, such as uploading photographs from a recent vacation. Facebook was a mix of memorable events coupled with mundane details, and was recognized as a resource for sociality. By allowing users to upload content for no explicit audience, Facebook enabled a visibility between users that extended beyond what they would typically know about each other. This provided peers with "a general feeling of how your life is going" (Artsci3W). As submitting personal information was a more pervasive activity, Facebook produced a visibility akin to a "general feeling" of individuals. This is the familiar side of visibility on domestic technologies; it is mundane and consensual, without seeming deliberate.

Many respondents actively disliked Facebook, going so far as to deactivate their profiles. These students invariably returned to Facebook, though their absence only strengthened their criticism of the site. Their return to a service they dislike is fuelled by the perceived need to stay online. Not being on Facebook is equated with being cut off from peers and social events. Nobody directly prevented them from leaving, but there are clear costs associated with leaving:

> It's my damn friends, man. Like, there's Homecoming and there's a bunch of people coming up to Homecoming and [for] a lot of my friends, Facebook is the only reliable way to get a hold of them. Which is annoying. It's really annoying. Because I don't really want to be on it and I probably—like, after university's done, I probably won't be. But I don't know, right now it's just—it's almost too convenient not to have it. (Artsci4M)

Staying on Facebook was seen as too convenient, and leaving it was too costly (Chang & Chen, 2008). Even when some visibility was desirable, these ties posed risks on an everyday basis and required heightened vigilance vis-à-vis offline sociality. What makes social media convenient, namely the way they diffuse information, also makes them risky.

Facebook visibility as surveillance

Respondents were fully aware of why Facebook would be used for surveillance. They described the site as a vast and accessible resource for personal information. Respon-

dents described interpersonal surveillance on Facebook in terms of being watched by others. In addition to former and current romantic partners, respondents were concerned with parental scrutiny. Parental access to profiles led to a convergence between social contexts that respondents wanted to avoid (boyd 2008). Facebook also provided a distorted representation of the person. One user described how Facebook misrepresented him to his father:

> My dad is on Facebook. He knows what I'm up to. He knows the shenanigans that happen. But at the same time, he doesn't see that I put in like twenty hours a week at the library along with fifteen hours a week of classes. He doesn't see that I'm working every weekend on essays and stuff. He sees the guy holding the red plastic beer cup. (Artsci1W)

Facebook all too easily gives other users' access to personal information that is misrepresentative. It also publicizes information respondents would simply prefer to keep to themselves. For these reasons respondents were ambivalent about their presence on the site.

Interpersonal surveillance on Facebook is also mutual, as watching and being watched both feature prominently. Respondents turned to Facebook to discover more about people who were of interest in their romantic lives. This is justified by the availability of relevant information on profiles, including sexual orientation, relationship status, the kind of relationships the user wishes to pursue, and potential topics of conversation. Respondents described their own exposure as a distinct concern from watching their peers. They held different standards between what they wanted to expose about themselves and what they wanted to find out about others. Yet when considering their own visibility, their ability to access their peers' personal information was the most accessible yardstick:

> I find it kind of weird that I have such insight into her life and I can, like, basically judge her, like I don't know, it's really weird to me. That's why I don't really use it that much, because I feel like all these people can do the same thing. (Artsci4W)

Peer visibility lead respondents to guard their own information. Knowing they were being watched and knowing the extent to which they could watch others compelled respondents to monitor their online presence for content that they believed others would find objectionable. This kind of self-scrutiny triggered the strategies for impression management detailed later in this article.

"Creeping" and "stalking" on Facebook

Two terms associated with peer surveillance on Facebook warrant exploration: "stalking" and "creeping." Both describe problematic ways of getting information on Facebook. Creeping was seen as a milder version of stalking, which in turn was meant to reflect more negatively on the user: "It's all a matter of degree. I mean, if you were looking to assign either Facebook stalking or Facebook creeping to one person's activities, I'd think you would have to do it on a case-by-case basis" (Health3M). Creeping was a more involved and targeted way of using Facebook, though respondents treated this as a matter of circumstance. Creeping involves perusing content: a few pages of

wall posts, or a photo album. It is a function of using Facebook, as using the site in the way it was intended leads to the prolonged scrutiny of others' information. Creeping can also be brought on due to boredom, or simply because content on the user's news feed—the content that first greets people when they sign on—caught their attention.

> I guess most people would define the stalking one as more, like, actively searching, but I guess creeping would be if you're just bored and you're just looking at people's profiles and you don't have an active interest or motive to look at it. (Artsci4W)

Stalking resembles creeping, although it is "a little bit more aggressive" (Artsci4W). If a user consistently returned to a particular user's profile, this would be framed in terms of stalking. As Facebook stalking is not restricted to actual stalkers, respondents suggested the site facilitates this kind of behaviour from its users. Much as Shirky (2008) claims emergent media lower the threshold on group activity, social media facilitate surveillance by virtue of how they organize interpersonal exchanges.

Some terms, like creeping and stalking, imply that some forms of exposure on Facebook are more troubling than others. Yet users generally grew accustomed to this range of visibility, illustrating a tension between accepted and unwanted kinds of interpersonal surveillance on social media. One respondent stated that having his personal information accessible to a network of peers had consequences he was only beginning to realize and accept:

> I've had like a few people phone me and I'd say, "How'd you get my phone number?" "Oh, yeah I got it from Facebook, sorry." "Okay, yeah, no that's totally fine." Because I put it up there, right? I put it up there for a reason. (Artsci2M)

Experiences with creeping and stalking showed respondents what kind of visibility to expect from the site. These incidents lead to greater self-scrutiny and management of their presence, but also to a level of comfort with their exposure. Creeping and stalking were not necessarily seen negatively, as users did it themselves. Visibility between users ranges from casually discovering what a close friend did over the weekend, to the targeted and prolonged monitoring of strangers. This range of practices is unique, as they emerge seamlessly from the everyday use of domestic media. For this reason, many respondents suspected Facebook was designed specifically for activities like "stalking" and "creeping." As a domesticated surveillance technology, Facebook itself creeps from the familiar to the objectionable.

Making sense of the private/public distinction

The terms private and public came up frequently when discussing Facebook with student respondents. Not only was a public/private binary insufficient to describe Facebook, but Facebook was also a catalyst to reconsider these values. Facebook represents a kind of blurring of private and public, at least as they were generally understood in North America prior to the advent of social media. In addition, the term "personal" crosscuts these discussions, such that personal information appears in public spaces, private spaces, or both.

Facebook is a public space where users are ostensibly comfortable sharing personal details with friends that they have wilfully chosen. Some respondents, especially

those in their first year of studies, drew parallels between their exposure on Facebook and the kind of publicity sought by reality TV stars. Clearly one of the key motivations for using Facebook was to share specific information with a somewhat amorphous (though occasionally specific) audience.

> It's pretty much all about attention, as far as pictures; taking pictures, things like that – because everyone can see that. … It's almost as if we're in a world where we watch a lot of reality TV and there's TV shows like *The Hills* and things like that, Facebook is our own little form of entertainment where we can get a glimpse of everyone's life. (Artsci3M)

Other respondents approached Facebook publicity with trepidation, making comparisons to real-life exposure to underscore the difficulty of adjusting to the service. One respondent likened the circulation of photos on Facebook as if they "had a photo album at my house and somebody came and copied it and then put it in their photo album" (Artsci4M). Another claimed the wall was modelled after the whiteboard on students' doors in residence, making it a kind of public space. Students also drew comparisons between putting content on Facebook and being visible outdoors. The implications of this imagery, however, were not unanimous. While some believed being outside legitimated scrutiny, others believed they still had reasonable expectations against creeping and stalking. These tensions are a product of domestication, and force a reconsideration of privacy and publicity.

Privacy also mattered to respondents, especially when personal information leaked in unanticipated or undesirable ways. One respondent who described Facebook as private referred to its extensive privacy controls, yet also acknowledged a public element insofar as the site is open to all:

> I'd say it's private in the sense that like your own profile is like, your own profile and you can control what's on it because even if somebody writes on your wall, you can make it invisible kind of thing. So, it's totally private because you can have as much information as you want or as little information as you want, but then it's public in the sense that anyone can use it. (Health1W)

Although some respondents valued privacy more than others, most respondents managed their privacy and publicity simultaneously. One respondent referred to Facebook as "a completely public expression of private and personal matters" (Artsci4W). This statement suggests not only that competing values coexist on the site, but also that using Facebook is contradictory. By default, users are putting information in a context that is more public than desired. The fact that this is a deliberate and wilful act perplexed respondents:

> It's supposed to be personal information but Facebook makes it very public and you're supposed to be, I guess, with every post you make, keeping in mind the fact that everyone can see this and that this is a public sphere for, I guess, private communication. (Artsci4W)

While conversations about the public and private on Facebook are messy, there is no boundary separating the private from the public, even though some spaces are designated as more private than others. Private information may become public in conse-

quence later. Respondents treated social media as a kind of public where users balance consensual visibility against unwanted exposure.

Managing online presences

Although social media like Facebook offer new opportunities for public exposure, respondents had a range of tactics at their disposal to manage their presence. Caring for the virtual self (Whitson & Haggerty, 2008) involves restricting information flows, and exceeds the range of privacy features offered by Facebook. In general student users made extensive use of privacy settings. They did this to restrict information from a general public, but also for more targeted purposes like hiding a particular photo album from specific individuals. The majority of respondents were familiar with privacy settings. Others found them confusing, but maintained a commitment to mastering these settings. Based on prior experiences, respondents periodically returned to their settings to ensure they were still in order. Upon joining his school's academic network, one respondent noticed his personal information had leaked to an extent he had not anticipated. Following this incident, he appraised his privacy settings "every so often … to make sure that only my friends can see my profile" (Artsci3M). One respondent set her privacy such that other users could not seek her out. In effect, she had to initiate contact with others.

Another tactic employed by respondents was to maintain dynamic and contextual privacy settings. Many respondents stated their intention to revise their settings, with one respondent doing this mid-interview. Respondents augmented their privacy during job searches, such that potential employers could not locate their personal content. One person went so far as to cancel his Facebook account temporarily in recognition of how his position as a political leader could be compromised by his online presence:

> I cancelled Facebook for a little while; it was for quite a long period of time. It was because I was vice-president of the [youth political group]. … I had that leadership position too and, that's when I realized that you know, this is my personal life but, it's publicly ... like my public personal life, that could reflect negatively on the [youth political group]. (Artsci1M)

Other respondents logged onto their friends' accounts to see the extent to which they were visible. By looking at their presence from another user's perspective, they had a better sense of how their presence was perceived. Facebook later integrated this feature into their privacy settings, an acknowledgment that peer visibility matters to users.

Respondents also cared for their virtual self by choosing not to upload certain information. This self-censorship is described along common-sense lines, as respondents simply did not share content that may harm their reputation:

> Anything I put out there on the Internet—if I'm afraid of it ever coming back to haunt me, I won't put it out there. And I consciously make that decision for every piece of information that I put out. So I'm not really worried about stalking or creeping because anything out there on me is kind of what I've already put out. (Artsci3W)

> Anything that you wouldn't want your parents to know isn't something that should be on the Internet. (Artsci4W)

Respondents cared for their virtual self by omitting or removing damaging content. Parents and stalkers were invoked as justification. Self-censorship included not uploading information, but as well as not behaving in a way that could be photographed or otherwise documented:

> For me to be caught on photo doing something stupid, I had to be doing something stupid in the first place. And if I avoid that, which I have been hit or miss about in the past, then it's a non-issue. They can't post photos of me that didn't happen. (Health3M)

Many respondents monitored the content their friends post about them. These respondents objected to some wall posts and photos authored by friends, deleted these posts, and scrutinized their friends. They recognized that these friends shaped their online reputation. In extreme cases respondents also pruned their social network by removing users from their friend lists who posted problematic content on their profile. Yet, some respondents also suggested that they did not know the full details of their virtual self on social media, that their efforts to manage their reputation were insufficient. This is a tension of domestication: familiar interactions lead to an accumulation of content and social ties that are difficult to manage.

Responsibility and futility

Respondents felt responsible for their exposure on social media and extended this responsibility to others. In the event of privacy violations or other unwanted consequences, respondents believed users only had themselves to blame. This suggests a perceived locus of control when users upload information to Facebook: "you can exercise so much control over what's visible, it's boggling to me, honestly. If I didn't want people to see my profile, I'd make it private, and that would be that" (Health3M). Because of this sense of agency, the idea of users encountering trouble with their profile was met with little sympathy. Respondents claimed that by uploading information onto their profiles, users were "inviting people to look into their life" (Artsci3M). Here users were seen as deliberately uploading information about themselves in a public setting and then complaining about consequences they clearly should have anticipated. Respondents did treat their own creeping and stalking as problematic, but self-judgement was tempered by the perception that users are responsible for the care of their virtual self. As a result, they justified their lateral surveillance of others by citing the other user's decision to upload this information, or their failure to use more stringent privacy settings: "If I'm looking at it, I feel like if she has it public, then I can just look at it and I don't feel bad" (Artsci4W).

Respondents felt responsible for managing their online visibility; yet, they also acknowledged that this was challenging. Attempts to manage privacy are often case-based; that is, to stop specific information at a specific point in time. Many respondents believed information would still leak beyond an intended audience. The sheer volume of information and social ties complicates an online presence. Respondents claimed that simply having information on a profile, whether public or private, left users open to considerable risk because of the growing number of people who would have access to that information: "I guess we all tend to forget is that what we put on Facebook

isn't personal or private in any means because of the hundreds and sometimes thousands of people that you allow to see your profile" (Artsci4W). This respondent compared this unexpected exposure to the "reply all" button on email interfaces, where users accidentally send a message meant for one person to an entire community. Respondents also described the non-friend friend (a Facebook friend but a stranger otherwise) as a potential vulnerability:

> I think just the people who you kind of add, maybe two or three years ago, who you've kind of forgotten about. They're still on your friends list but you may not actually be friends with them in real life and you may not see them ever or talk to them ever, but you still have access to their profile and they still have access to yours. (Artsci4W)

The quantity of seemingly trusted friends prevents a user from managing their entire audience. Even when respondents placed the locus of control—and blame—on individual users, they acknowledged that Facebook is primarily a public domain, and that attempts to limit exposure are futile. Social media are domestic technologies that creep and leak in unanticipated directions. Respondents were aware that proper conduct on Facebook is based on a contradiction: individual users are expected to be vigilant, but this vigilance will not offset all potential risk. Safe use is necessary, but not sufficient on social media.

The above suggests an acknowledgement of partial futility: if information is uploaded it will most likely leak. Facebook surveillance is a product of information convergence, as so many people are using it. The challenges for visibility and exposure posed by Facebook are augmented as more people join it, and as it takes on a greater presence in different social contexts:

> Like, Facebook is so new, like, we don't know what kind of social implications it's going to have. And it's becoming such a momentous force that I don't think, like, it's like people jumped on board before they knew where it was going. (Artsci4M)

Much as interpersonal surveillance is rooted in the everyday use of social media, mitigating the risks of unwanted exposure is embedded in mundane practices like untagging photos and choosing not to upload damaging content. As these risks are tied to information flows between previously distinct contexts, respondents used privacy settings extensively to ensure these leaks are kept to a minimum. Some respondents were overwhelmed by Facebook's opportunities for public exposure, and cited this as a reason to not be diligent:

> I'm pretty sure all my private information is already long gone. There's no sense of privacy in this modern world and because everything I do is basically online these days, I feel like there's little or no safety and, therefore, I don't need to curb what I'm doing on Facebook. (Artsci4W)

This respondent was ambivalent about her comfort with Facebook. She grew accustomed to being visible, but this was in response to the overwhelming exposure on the site. She actively participated in her visibility, but this was not necessarily the kind of social media she wanted. In considering the negative outcomes associated

with Facebook, respondents described a mix of outrage from undue risks, coupled with an acceptance of these vulnerabilities based on individual responsibility and agency. The accumulation of social ties on Facebook means there will be unexpected and undesirable forms of visibility.

Discussion

Respondents have a growing familiarity with interpersonal surveillance on Facebook, but this familiarity is mixed with uncertainties and tensions. Users join at the behest of their friends, and maintain visibility to communicate with these friends. The kind of visibility required for surveillance from Facebook is borne out of everyday practice, with users maintaining relations with their colleagues. Peer pressure notwithstanding, users willingly supply information about themselves to this platform, making it suitable for interpersonal scrutiny. An ever-growing friendship network means unanticipated risks occur, but choice and responsibility are placed on users themselves, despite this complexity. Tensions between individual control and greater complexity on social media, much like tensions between private life and public exposure, are indicative of the further growth and domestication of social media (Silverstone & Haddon, 1996). As an increasingly central feature of everyday life, social media surveillance between users is framed not so much as a violation than a condition that users need to manage. Visibility and exposure on Facebook is normalized. Exposure is not limited to any specific instance, but rather is a pervasive condition of social life on social media.

Users express some ambivalence in their responses. They grow accustomed to Facebook visibility, yet its effects remain chilling. These developments complicate efforts to manage their online presence. Users feel responsible for their presence, but are aware that managing this presence is beyond their control. They perceive their online reputation as being a personal responsibility, even while acknowledging that caring for the virtual self by way of vigilant self-scrutiny is not enough. Student users are aware that different audiences and social contexts intersect on the site, but they still construct a visible profile for close friends. This is emblematic of interpersonal visibility on Facebook: an online presence is built from mundane contributions by users and their friends. Users join because their peers are online, and they build a presence to remain visible to these friends. No single act seems risky or malicious, but when taken together over time, maintaining an online presence can can have damaging consequences. Moreover, Facebook's continued growth—in terms of audience, contexts, and features—increasingling adds importance to the content on the site. This is especially true at a time when Facebook's user population is sharply increasing, with a concomitant increase of the contributors to any user's visibility, audiences of that visibility, and social contexts in which that visibility will have consequences. A photograph that was uploaded when there were a million Facebook users becomes all the more important when its potential audience reaches one billion users.

This article has focused exclusively on interpersonal social media surveillance. Surveillance concerns for users are primarily individualistic. They report and anticipate surveillant relations with family, friends, romantic interests, and classmates. They are generally concerned with situated and immediate forms of surveillance. They want to maintain boundaries that separate different social contexts. From their perspective

these concerns eclipse other kinds of scrutiny conducted through Facebook. Subsequent research should consider these other kinds of surveillance through social media. As law enforcement branches, marketers, employers, and governments take a continued interest in sites like Facebook, the visibility produced by interpersonal social media surveillance will undoubtedly augment the scope and capacity of other kinds of social media surveillance. This research is also limited to digital youth in a university environment. While this provides specific context for user concerns, subsequent research should focus on how a more diverse population is settling into Facebook, as well as the population's conditions of inter-visibility.

Acknowledgment

This research has been funded by a Doctoral Fellowship from the Social Sciences and Humanities Research Council.

References

Albrecthslund, Anders. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3). URL: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949 [August 16, 2011].

Andrejevic, Mark. (2005). The work of watching one another: Lateral surveillance, risk, and governance. *Surveillance & Society,* 2(4), 479-497.

boyd, danah. (2008). Facebook's privacy trainwreck: Exposure, invasion, and social convergence. *Convergence: The International Journal of Research into New Media Technologies*, *14*(1), 13-20.

boyd, danah, & Hargittai, Eszter. (2010). Facebook privacy settings: Who cares? *First Monday*, *15*(8). URL: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589 [August 16, 2011].

Brighenti, Andrea. M. (2010). *Visibility in social theory and social research*. Hampshire: Palgrave Macmillan.

Chang, Hsin Hsin, & Chen, Su Wen. (2008). The impact of customer interface quality, satisfaction and switching costs on e-loyalty: Internet experience as a moderator. *Computers in Human Behavior*, *24*: 2927-2944.

Dewing, Michael. (2010). Social media: 2. Who uses them? Parliamenty information and research service. URL: http://www.parl.gc.ca/Content/LOP/ResearchPublications/2010-05-e.htm [March 4, 2012].

FB Statistics. (2011). *Statistics*. URL: http://www.facebook.com/press/info.php?statistics [August 16, 2011].

Koskela, Hille. (2004). Webcams, TV shows and mobile phones: Empowering exhibitionism. *Surveillance & Society*, *2*(2/3), 199-215.

Lyon, David. (2001). *Surveillance society: Monitoring everyday life*. Buckingham: Open University Press.

Murakami Wood, David, & Webster, C. William R. (2009). Living in surveillance societies: The normalisation of surveillance in Europe and the threat of Britain's bad example. *Journal of Contemporary European Research*, *5*(2), 259-273.

Nippert-Eng, Christena. (2010). *Islands of privacy*. Chicago, IL: University of Chicago Press.

Sax, Linda J., Gilmartin, Shannon K., & Bryant, Alyssa N.. (2003). Assessing response rates and nonresponse bias in web and paper surveys. *Research in Higher Education*, *44*(4), 409-432.

Shirky, Clay. (2008). *Here comes everybody: The power of organizing without organizations*. New York, NY: The Penguin Press.

Silverstone, Roger, & Haddon, Leslie. (1996). Design and the domestication of information and communication technologies: Technical change and everyday life. In R. Silverstone and R. Mansell (Eds.), *Communication by design: The politics of information and communication technologies* (pp. 44-74). Oxford: Oxford University Press.

Trottier, Daniel. (2011). A research agenda for social media surveillance. *Fast Capitalism*, *8*(1). URL: http://www.uta.edu/huma/agger/fastcapitalism/8_1/trottier8_1.html [March 3, 2012].

Tufekci, Zeynep. (2008). Grooming, gossip, facebook and myspace: What can we learn about these sites from those who won't assimilate? *Information, Communication, and Society*, *11*(4), 544-564.

West, Anne, Lewis, Jane, & Currie, Peter. (2009). Students' Facebook 'friends': Public and private spheres. *Journal of Youth Studies*, 12(6), 615-627.

Whitson, Jennifer, & Haggerty, Kevin. (2008). Identity theft and the care of the virtual self. *Economy and Society*, *37*(4), 572-594.