2013

Facebook: public space, or private space?

Jacquelyn Burkell
The University of Western Ontario, jburkell@uwo.ca

Alexandre Fortier
Faculty of Information and Media Studies, University of Western Ontario, afortie@uwo.ca

Lorraine Wong
Western University, lola.wong@uwo.ca

Jennifer Lynn Simpson

Information, Communication & Society, 2013
http://dx.doi.org/10.1080/1369118X.2013.870591

Routledge
Taylor & Francis Group

Facebook: public space, or private space?

Jacquelyn Burkell[a]*, Alexandre Fortier[a], Lorraine (Lola) Yeung Cheryl Wong[a] and Jennifer Lynn Simpson[b]

Faculty of Information and Media Studies, The University of Western Ontario, North Campus Building, London, ON N6A 5B7, Canada; Faculty of Law, The University of Western Ontario, 1151 Richmond Street, London, ON N6A 3K7, Canada

(*Received 30 March 2013; final version received 25 November 2013*)

Social networks have become a central feature of everyday life. Most young people are members of at least one online social network, and they naturally provide a great deal of personal information as a condition for participation in the rich online social lives these networks afford. Increasingly, this information is being used as evidence in criminal and even civil legal proceedings. These latter uses, by actors involved in the justice system, are typically justified on the grounds that social network information is essentially public in nature, and thus does not generate a subjective expectation of privacy necessary to support a charter-based privacy protection. This justification, however, is based on the perceptions of individuals who are outside the online social network community, rather than reflecting the norms and privacy practices of participants in online social networks. This project takes a user-centric approach to the question of whether online social spaces are public venues, examining of the information-related practices of social network participants, focusing on how they treat their own information and that of others posted in online social spaces. Our results reveal that online social spaces are indeed loci of public display rather than private revelation: online profiles are structured with the view that 'everyone' could see them, even if the explicitly intended audience is more limited. These social norms are inconsistent with the claim that social media are private spaces; instead, it appears that participants view and treat online social networks as public venues.

Keywords: privacy; social media; Facebook

'If you are a young adult or teenager, you can't live without Facebook'. (Tsjeng, 2010)

This headline, appearing in the online version of the *Guardian* on 21 March 2010, pretty much reflects the status of social networking in the lives of many teenagers and young adults. According to the author, and consistent with other reports (Vaughan-Nichols, 2013), Facebook, the most widely used among social networking sites, is the first site that users go to when they turn on their computer, serving as (among other things) a social calendar (and event manager), communications channel (allowing users to keep in touch with friends and family), and shareable photo album. The large majority of teens and young adults maintain social network profiles: recent American data, for example, indicate that 87% of youth and young adults aged 18–29 use social networking sites (Rainie, Lenhart, & Smith, 2012). Users perform a variety of social

*Corresponding author. Email: jburkell@uwo.ca

functions on networking sites, including maintaining and updating their online profiles, sending directed messages (to individuals or groups), posting semi-public comments to friends' walls (visible to anyone with access to the profile), commenting on photographs, and joining social groups (Joinson, 2008).

Online social networks are all about the sharing of personal information, so it is not surprising that participants reveal a great deal about themselves in their online profiles (see, e.g. Gross & Acquisti, 2005). This information sharing occurs in the context of online social networks that are typically much more extensive than their offline counterparts, including large numbers of 'weak ties' (in the context of Facebook these are colloquially termed 'Facebook friends') with whom the participants neither have nor anticipate extensive interaction in the face-to-face world (Lewis & West, 2009). The apparently profligate self-revelation of online social network participants might suggest that they are unconcerned about privacy in these social environments. At the same time, however, participants in social networks report deploying different site features or aspects to tailor the visibility of their online actions and productions (Thelwall & Wilkinson, 2010; see also Carey and Burkell, 2009 for privacy protecting strategies used in the online environment), and members of various social networking sites indicate that they employ privacy settings to limit access to their profiles (Lange, 2007; Patchin & Hinduja, 2010).

What quickly becomes evident is that social networking sites are neither prototypically 'private' nor obviously 'public'. Instead, online social networks appear to be emerging social spaces that occupy a liminal territory between 'open' and 'closed' (e.g. Lee, 2009: boyd (2007) has used the term 'networked publics' to refer to the permeable and somewhat fluid audience for online social profiles) (see also Gelman, 2011, for a discussion of how information that is formally public is accessed by 'blurry-edged' networks of interested others). We do not know quite how to think about these technologies and social spaces, we do not know quite how to behave within them, and, critically, we do not understand the social norms regarding disclosure and sharing in these spaces (see Häkkilä & Chatfield (2005) and Viégas (2005) for research that documents the development of new social norms in various digital environments; see also Grimmelmann, 2009, for a discussion of the importance of understanding social values in these new venues in order to craft appropriate regulatory responses). We have to look to community practices to determine whether social networks are public or private spaces. AQ2

This question has heightened urgency because, increasingly, information posted on social networks is entering into the legal process (e.g. as submissions in criminal proceedings, administrative proceedings, and, in some jurisdictions, civil proceedings). As a result, the courts must determine whether there is a 'reasonable expectation' of privacy with respect to these obviously personal data, requiring a subjective expectation of privacy that is also objectively reasonable: i.e. a subjective expectation of privacy that is consistent with societal values. The relevant considerations are difficult enough in the familiar world of physical bodies, physical objects, and physically defined territories. They become more challenging when the privacy in question refers to entirely new forms of personal and social spaces for which social norms are, at best, developing (see, for example, Barnes, 2006, and Debatin, Lovejoy, Horn, & Hughes, 2009).

Courts are tackling the difficult question of whether and to what extent online profiles (in practice usually Facebook profiles) are discoverable for the purposes of civil action. Section 8 of the *Canadian Charter of Rights and Freedoms*, which protects against 'unreasonable search and seizure', governs the admissibility of social networking profiles in administrative and criminal cases, and the discoverability of these profiles in civil actions is evaluated in light of Charter values (*Park v. Mullin*, 2005). Prior decisions on Section 8 of the Charter (*R. v. Tessling*, 2004) have made it clear that the standard is *not* merely descriptive, as this approach would involve an inevitable erosion of personal privacy: instead, it is viewed as a normative standard that fosters 'the underlying values of dignity, integrity and autonomy', protecting a 'biographical AQ3

core of personal information' which would 'tend to reveal intimate details of the lifestyle and personal choices of the individual' (*R. v. Plant*, 1993). At the same time, 'reasonable expectations' must take account of the 'totality of the circumstances', including (among other factors) whether the individual can regulate access to the information, and whether it is in 'public view'.

In practice, the legal reasoning regarding the admissibility of social network profiles seems to focus on, and indeed make assumptions about, whether posted information is 'public'. In deciding whether a plaintiff can expect privacy in her Facebook content, courts rely on several factors such as the social (and therefore public) nature of Facebook and other networking sites, the number of Facebook friends a user has and the extent to which the user limits access to her profile through her privacy settings, in order to infer the degree of privacy that the user must expect in her profile (see e.g. *Murphy v. Perger*, 2007; *Schuster v. Royal & Sun Alliance Insurance Company of Canada*, 2009; and alluded to in *Sparks v. Dubé*, 2011). In *Frangione v. Vandongen et al.* (2010), for example, the court commented as follows:

> The plaintiff's testimony on discovery was that he maintained privacy over communications with his friends that numbered approximately 200 although only five of them were close friends. In other words, he permits some 200 'friends' to view what he now asserts is private. This is a preposterous assertion especially given his testimony that only five of the 200 are close friends. In my view, there would be little or no invasion of the plaintiff's privacy if the plaintiff were ordered to produce all portions of his Facebook site.

In this and other similar reasoning, the courts are focusing on the relatively large size of online social networks, citing this large size as prima facie evidence that information posted to this network is 'public' in nature. It is entirely possible, however, that participants could nonetheless treat this information as 'private' in the sense that social norms preclude sharing this information outside the original distribution list, or suggest in other ways that the information is 'private' rather than 'public.

Legal scholars have struggled with the issue of privacy in the online environment, working to map existing privacy law onto this new domain. Much of this scholarship is based in the United States, relating to privacy torts. Abril (2007), for example, attempts to recast privacy torts in a 'spaceless world', suggesting that 'instead of physical space, we should think in terms of walls of confidentiality built by technical architecture, agreements, and relational bonds' (p. 47). Grimmelmann (2009) examines whether Facebook (and particularly *privacy* on Facebook) can be 'saved' through a strengthened public-disclosure tort along with enhanced options to opt out of information sharing. Kerr (2010) maps Fourth Amendment principles from physical space to cyberspace, proposing that the 'inside/outside' distinction appropriate for physical space be replaced, in the context of online communications, with a 'content/non-content' distinction, while Crocker (2009), again in the context of US jurisprudence, proposes that online privacy rights be protected through a focus on interpersonal liberty. Strahilevitz (2004) suggests that social network theory offers a 'relatively objective, testable, rigorous, and principled approach' to the determination of whether an online disclosure should be considered to be 'public'.

These and other legal and policy analyses can and should be strengthened by inquiry into the privacy-related practices and expectations of the reasonable social network participant (Grimmelmann, 2009). In some sense, the courts seem to consider the social nature of online participation, and thus the shared nature of online profiles, as testament to the public nature of line social profiles. Yet personal, and private, information is shared in a wide variety of contexts without 'crossing over' into the public domain (Strahilevitz, 2004). Privacy is not an 'all or nothing' proposition, and it is at least possible that a reasonable social network participant might still expect privacy in her profile, despite the social nature of the site or the possibility that she has

a large number of Facebook friends who have access to the information that she posts. Alternatively, posting to Facebook might be like going to the bar, providing a social venue for public display of the 'produced' self: a version of the self that is intended precisely for public consumption, and available to a large and undefined public. It is entirely possible that social network participants might *not* perceive information shared in the social networking context as having entered the public domain, and might instead share with others in the same community a set of standards and norms that preclude the disclosure of this information outside of the original network of contacts. The question of whether or to what degree online social spaces are private spaces can really only really be answered by the digital citizens who populate them. This research seeks to fill this gap in the literature by examining the information-related practices of social network participants. Our focus is on how people treat their own information and that of others posted in online social spaces, with particular focus on the question of whether online social environments are public or private spaces.

What does it mean for information to be 'public'? The notion of 'public' is one for which there is no explicit definition, and in practice 'public' is often identified as the antithesis of 'private (Tverdek, 2008). Being 'public' tends to be first and foremost a question of space: something is considered public if it occurs in a space (real or virtual), where there can be no expectation of freedom from observation by others. By choosing to act in a space to which others have a ready access, one surrenders one's claims to privacy with respect to a potential audience. Tverdek (2008) argues also that something can lose its private character, and therefore become public, by virtue of its being revealed to others (whether intentionally or inadvertently). When we share information, we lose control, and our privacy depends on the confidentiality of that person (Petronio, 2002). If online social spaces are private spaces, the social norms should censure sharing of information beyond the original audience, and participants should feel free to post information they consider to be sensitive in nature. By contrast, if these are public spaces, 're-sharing' of posted information should be supported and accepted, and participants should take care to share only that information they intend to be widely shared.

Method

Interviews and focus groups were conducted with active online social network participants, recruited through advertisements at a large Canadian university. Given the pre-eminence of Facebook as the most widely used online social network, discussions naturally focused on this social networking platform, and the report of the results reflects that focus. Unstructured interviews and focus group discussions explored a wide variety of issues related to their practices within social media, including but not restricted to:

- Their expectations of audiences for their social media profiles.
- The content they choose to share on their social media profiles.
- Their practices with respect to the dissemination of the content shared by others.

Each session was transcribed and the data were anonymized. Data analysis proceeded using a grounded theory approach to identify emergent themes.

Subjects

We conducted a total of 10 individual interviews and 5 focus groups, each with between 4 and 7 participants (total of 30 focus group participants). The majority of the participants were female (among the interviewees, 8 females and 2 males; among the focus group participants, 18

females and 12 males). Interview participants ranged in age from late teens to early thirties (exact ages were not provided), and included undergraduate and graduate students as well as individuals employed in the health and retail sectors. All focus group participants were students (including both undergraduate and graduate programs), and they ranged in age from 18 to 42.

Recruitment materials for focus groups and interviews targeted active social network users, and the majority of the participants fit this category. Among the focus group participants, however, there were two who were not currently active in any online social networks, although they had been active users in the past. All other participants classified themselves as active social network users; there were, however, obvious differences in the nature of this participation, perhaps best demonstrated by a short description of individuals who occupied the most extreme positions on what might be interpreted as a continuum between the most conservative and least conservative participants in online social spaces.

Harold (in his thirties) and Fern (also in her thirties, both healthcare professionals, interview participants) are typical of the more conservative social network users who participated in the study. As somewhat older individuals (in their thirties) with professional identities (both are healthcare professionals), they demonstrated an acute awareness that their online activities can affect their offline reputations. Both Harold and Fern maintain a small list of online friends, limited to individuals with whom they have an ongoing and active offline connection. They carefully select their online postings and monitor their online presence to ensure that the profile they present is professional, and the information they reveal is not too personal in nature. Crystal and Matt are two younger focus group participants (each in their twenties, focus group participants) who take an entirely different approach. Each has a large and growing friends list, populated not only with 'real world' friends, but also with acquaintances and 'friends of friends' with whom they have at best a tenuous offline connection. Similar to many of the younger participants, Crystal and Matt each recognize that they may in the future chose to further limit their online postings, perhaps even deleting some material that they have added (or allowed to be added by others) to their profiles; they imagine that this might occur, for example, when they are looking for employment after they finish their university degrees. In the meantime, however, their online profiles include a wide variety of information about themselves, their friends, and their social activities, all intentionally shared with a large and growing network of friends and acquaintances, including some with whom they have only a tangential face-to-face connection (e.g. 'friends of friends', or people they have encountered once at a party or at a bar). These participants demonstrate the most extreme of a range of the Facebook-related practices represented in our sample. Unless explicitly reported otherwise, the results discussed below are characteristic of participants across the entire range. Where consistent differences are evident between participants with a more conservative approach (such as Fern and Harold) and those who are less conservative (such as Crystal and Matt) these differences are discussed explicitly in the text.

Results

Each person who has a Facebook profile maintains a 'friends' list, populating that list by asking to 'friend' other users and accepting friend requests in return, and by responding to friend requests initiated by other users. Friends can be deleted ('unfriended') at any time by the user. Users have control, through privacy settings, over the privileges accorded to friends (and, by extension, the online connections of those friends); previous research suggests, however, that changes to these default settings are relatively rare (Gross & Acquisti, 2005). By default, each 'friend' of a user has access to the entire Facebook profile including pictures, wall postings, status messages, and any other information included in the profile; each friend also receives by default automatic updates (news feeds) regarding changes to the profile. The default setting allows 'friends of friends',

connected to the user only through an intermediary who is themselves a Facebook friend, to view the profile. 'Friends' lists are, therefore, an important aspect of privacy control for social network users, and these lists articulate an audience for online postings.

Some participants have a very open policy when it comes to Facebook friends. Maya (18, student), for example, admits that she is 'not very selective' about friends on Facebook. At a recent party, for example, she met three people, friends of someone she already knew. She decided to add them to her Facebook friends so she can 'talk to them later, share with them, even though I've only met them once.' Other participants have more limited friends lists, some including only close real-life friends and family. Sam (male, 18, student) expresses a common and 'middle of the road' criterion when he describes how he 'prunes' his friends list: 'If I think they are people I'm never going to talk to again, people that I'm just not that interested in hearing about, then I'll prune the list.' Friends lists can grow to be very large in number (one participant, whose list was not atypically large, noted that he had reduced his list from 850 to 550 as a result of 'higher standards' for friends); even the largest lists, however, consist of contacts with whom there is some degree of social connection: attendance at the same school, a meeting at a bar, or an acquaintance in common, for example.

Interview and focus group participants spontaneously and regularly referred to the audience for their Facebook postings as 'big', comprising 'everyone', or 'the whole world'. Thus, for example, Manny (male, student, 18) notes that if he wants to share something with a 'bigger audience', he posts on Facebook (as opposed to another site); Maya (female, student 18) posts information as a Facebook status message if she wants 'everyone to know about it'. Dennis (male, student, 18) uses Facebook when he does not have a 'select audience'. Tammy (female, student, 19) uses 'Skype or something' if she is 'really excited about something' and does not want 'everyone to know about it', while Facebook is her preferred venue for sharing if she wants to tell a larger and more general audience. Harold (26) has chosen, for personal reasons, not to maintain a profile on Facebook. He reports that people approach him saying 'oh, I know you're not on Facebook so I should tell you this', giving him details about, for example 'something personal that happened to someone else that I should know'. His impression is that this information is shared because he 'should know it because everyone knows it'. The implication is obvious: if it is posted on Facebook, then 'everyone' does, and should, know about it. In other words, it is public, at least within a large, loosely defined, and peripherally connected social circle.

The 'everyone' included in this audience appears to be large in number, but the group is not entirely undefined. In particular, many participants (particularly the younger ones) were reluctant to add family to their 'friends' list, preferring to maintain a semblance of separation between the social and family spheres. Employers were another important category, and most (but not all) participants indicated that they would not include employers as Facebook friends. Although acquaintances and 'friends of friends' were often included in Facebook networks, 'friend' requests from complete strangers with whom there was no social connection were generally declined. Taking into account these practices and the 'extra-list' sharing discussed above, it appears that the typical Facebook audience is a large and 'burry-edged' network of socially connected individuals that is assumed to branch at least to 'friends of friends', but that may very well include individuals who are even more distantly connected.

When asked how they would convey deeply personal information, such as a significant illness, participants were unanimous in their rejection of Facebook postings as a means of communication. Even those with the most limited 'friends' lists indicated that they would share truly private information through other means: email, telephone, face-to-face conversations, or, in some cases, private messages on Facebook.

Information that is posted on Facebook appears to be tailored for this broad social audience. Ben (male, 18, student) does not get into 'sensitive' issues on Facebook; another participant (Yves, male, 28, student) notes that what you post on Facebook is instead 'tied to the public image you want to project'. Denise (female, 18, student) feels that on Facebook 'you can change it to make people view you in a certain way', and posters 'just want people to, like, think they're cool or something.' There is a general sense that the Facebook 'self' is not the real self, but instead Facebook is used to present and even craft a persona:

> Yeah, um, that basically like people feel like if, um, if their Facebook looks more exciting and stuff then they themselves feel more exciting. Then people reciprocate that like their friends and whoever else that they have on their Friend's List. (Julie, female 18)
>
> On Facebook she looks happy, she changes her profile picture, like, five time a day, changes here status fives times a day. And, she's fake. She's fake on Facebook. So I don't think people are honest. (Ben, male, 18, student)

Participants rarely reported removing posted information from Facebook, indicating instead that they carefully considered postings *before* they appeared on the site. This is not to say their decisions are always objectively wise, or consistent (in the case of younger participants) with what a more mature self would choose: among younger participants, for example, images of drinking and partying (if not *too* excessive) are essentially *de rigueur*, although older participants choose not to post such images and even those who *do* post such images indicate that they might choose to delete them in the future. One issue that prompted considerable discussion was the posting and tagging of pictures by *other* people. There was general agreement (though not universal support for the practice) that pictures would be taken at any social event, posted to Facebook, and 'tagged' to identify the individuals who appear and to connect the picture to the online profile of those individuals. Participants reported regularly and carefully monitoring their online profiles, including these images posted by others that, through tagging, become part of their online profile. Undesirable images (typically images in which the user 'looks bad', but sometimes images that depict problematic activities) are typically 'untagged', thereby breaking the association between the profile and the image. Rarely, however, is there a request to remove the image entirely, since such images are generally viewed as 'belonging' to the person who posts them, generally granting that individual control over the distribution of the image. This presentation of a 'best' self, or a self that meets norms for sociability, interests, and attractiveness makes sense, especially given that many Facebook users report using the social network to get to know *new* people, rather than simply maintaining existing connections (Joinson, 2008).

Although access to a Facebook profile is formally controlled by 'friends' lists and associated privacy settings, participants report a number of other practices that extend the audience to whom online profile information is available. A relatively small number of participants indicated that they share their Facebook password with others, thereby providing access to all the profiles in their 'friends' list to someone who might not otherwise be able to see these profiles. This practice was limited to younger participants with a less conservative approach to Facebook, and passwords were shared with close friends or partners. Other participants acknowledged accessing profiles of interest (e.g. that of an ex-boyfriend) by using, with permission and under supervision, the accounts of friends who were Facebook users, and participants reported offering similar access to their own friends and acquaintances. Participants also acknowledged 'over the shoulder' access, in which they browsed with another person or actively watched while someone else browsed profiles in their Facebook network. More rarely, participants discussed surreptitious or furtive access, using a Facebook account that was inadvertently left open by the owner to browse associated content, or reading profiles browsed by others without acknowledging the

activity. There was also recognition that Facebook content could and is stored and shared on other platforms.

Among these activities, only password sharing and surreptitious access were subject to direct approbation, and many participants explicitly noted the audience for a posting was not in practice limited as described by friends lists and privacy settings. The following comments are typical:

> Well I feel like on Facebook the privacy settings – when you're doing that you're thinking like 'Oh no one can see this' but at the same time all of your friends that you have can see it and who knows who is with them. … because you never know who's around or where they left their Facebook up or something. (Denise, female, 18)

> So I think people have to realize that anything they post on Facebook, people can take a 'print screen' – it can be eventually shared with a very large audience that it wasn't intended to be shared with (Manny, male, 18)

The practice of 'over the shoulder' browsing was acknowledged by a number of participants, and appeared to engender little if any negative reaction. When asked whether she has ever tried to get access to a profile that was closed to her, Belinda (female, employed, twenties) replied:

> Oh, yeah. All us girls do it all the time. Like, our groups of friends … I think somebody got married, and we're like 'Ohhh, wedding photos!' And we were trying to find them but … only one of us had them as a friend so we just went on their Facebook and looked at all the wedding photos … they posted it amongst all their friends, so they should be comfortable with a friend of a friend being able to see it. … . if you're beside the person and they're on Facebook, and they're just clicking through pictures, you're not going to stand there and look the opposite way. You're going to be talking with them and looking at stuff. You sorta have to understand that's going to happen.

These comments reflect both common practice and common understanding: friends share stuff with friends, and that sharing includes the social network profiles of people they are connected to.

Although our interview and focus group participants differed in their practices with respect to their own online networks and online profiles, they were generally consistent regarding the information posted by others, claiming 'they should expect that people will talk about it', and remarking that if 'you have three hundred friends … the chances of them passing some information on to someone about you, even in casual conversation – are probably pretty high' (Penny, female, thirties). Thus, there is a general presumption that information shared by others on Facebook is 'public' unless there is clear evidence or strong social expectation to the contrary.

Fern, for example (female, thirties, health professional), has her own profile limited so that only friends can view it. Although she views her own postings as 'private' an does not want them shared beyond her network of Facebook friends, she has a different perspective on the postings of others in her online social network. In particular, she has an agreement with her aunts and uncles that she will monitor the Facebook profiles of younger cousins, reporting problematic material to them:

> I have a deal with my aunts and uncles that if I see something … like my cousin for example talking about blow jobs when she was fourteen … that I would bring it up to their parents and be like 'By the way, this is what's on Facebook'.

She reasons that this is appropriate because:

> If they want to hide it from mom and dad, it's one thing. But if they want to post it for the entire world to see, thinking that they're still hiding it from mom and dad, you know, that's a different situation.

Fern could be accused of having a double standard, expecting her own privacy to be respected while compromising the privacy of others. But another interpretation is equally valid: Fern assumes by default that Facebook is a public space. She knows that, contrary to regular practice, she intends her *own* information to be private and not shared beyond the specific network of friends who have access to her profile, but she has no such signal about the information posted by others, including the younger cousins to whom she is linked online.

Although it appears that the default is 'public' for Facebook information, users describe being sensitive and responsive to signals (usually explicit) to the contrary. Thus, it is possible to create exceptions to this general rule. For example, Belinda (female, employed, twenties) describes a situation in which she happened to view information was posted to and then deleted from the profile of a friend. In this circumstance:

> Even though it was posted on Facebook, the fact that they deleted it and didn't want anyone to see it sort of told me that was supposed to be a private fight or a personal fight that they didn't want anyone to know about. But I just happened to be awake and saw it as it happened.

Respecting this signal, she chose not to talk about the information, even to the individual who had posted it. Later on in the interview, she is explicit about her position:

> I think if they've posted it and they've put that information out there, then it's OK if you tell somebody … [but] if they put it in a private thing, or if they asked me not to tell anybody, I wouldn't tell anybody.

There are some people (typically parents and employers) with whom information sharing is more circumspect, and evidently sensitive information posted on Facebook is more likely to be held in confidence. Thus, Janet, a young woman in her early twenties, remarks:

> People can share very sensitive information on their profiles sometimes, and it has to be up to our discretion to share, with whom, and in what format. If I find out that a friend had a miscarriage through Facebook, I would not go posting about it on someone else's profile.

Even in this case, however, Janet might 'send a mutual friend a message asking if they saw it' – so sharing is limited by the evident sensitivity of a topic, but not entirely eliminated.

Conclusion

Boyd (2007) characterizes online social spaces as 'networked publics', consisting of digitally interconnected audiences with indistinct boundaries (see also Gelman, 2011). The social practices and expectations described by our research participants are consistent with this concept, in that their online profiles are produced for and most participate as members of exactly such large and loosely linked social groups. In particular, online profiles are structured with the view that 'everyone' (at least the members of a broad and socially coherent group with what might be described as 'blurry' or 'leaky' boundaries) could see them, even if the explicitly intended audience is more limited, and participants generally treat information posted by and about others in the same vein, treating Facebook posting as tantamount to public disclosure that allows discussion both within and beyond the online social connections to whom it is explicitly disclosed. These social norms are inconsistent with the claim that Facebook is a private space; instead, it appears that participants view and treat online social networks as public venues.

It is important to note that our discussions did not explicitly focus on privacy and privacy concerns: instead, we engaged our participants in a dialogue about information sharing practices.

Although the information posted in online profiles is clearly personal in nature, in that it reveals aspects of the self, profile owners typically anticipate further disclosure, and profile viewers tend to believe further disclosure is appropriate: thus, there appears to be a general expectation that the information posted on social network profiles is public. This should not be taken to imply that there are no privacy considerations with respect to Facebook profiles: there are very real and well-documented privacy risks associated with the revelation of personal information on social networking sites (see, for example, Rosenblum, 2007). Instead, our results suggest that social network participants enter into online social spaces with the assumption that the information posted there is available to a broad and ill-defined audience with no clear boundaries. As such, it appears that online social information is treated as 'public' as opposed to 'private'. Even though most of our participants acknowledged creating boundaries around their Facebook profile through a friends list (only one had a totally open profile), they all tailored their Facebook profile to appeal to a much larger audience, as their practices indicate. Indeed, easily accepting new friends is a common practice, as is sharing information found on Facebook with one's friends outside of the explicitly identified audience. In very limited circumstances, information found on Facebook is considered too personal to be shared, but such boundaries appear to be exceptions to a general rule that Facebook is a public space.

If we concede (as these data suggest we must) that online social networks are indeed viewed and treated by participants as 'public' spaces, does it necessarily follow that there can be no privacy expectations with respect to the information revealed in online social network profiles? Although at first blush 'private' and 'public' might seem to be polar opposites, legal scholars, philosophers, and those involved with information technologies have explored the possibility of 'privacy in public'. This work suggests that, in at least some circumstances with respect to some information, people can maintain a privacy interest in information they reveal in a public domain. Greenfield (2011), for example, explores the privacy implications of sensors deployed in public spaces. His focus is on devices that record and act upon public behaviour (e.g. walking across a public street or looking at a publicly displayed advertisement), and he concludes that while some systems are innocuous (e.g. motion-triggered lights that signal the presence of a pedestrian in a crosswalk) others present significant privacy risks and indeed challenge privacy expectations (e.g. 'bi-directional' video billboards that unobtrusively capture and analyse viewer images to determine characteristics such as sex, age, and ethnicity). His convincing and persuasive analysis suggests strongly that some 'public' behaviours (or implications drawn from those behaviours) are in some sense viewed as 'private' by those performing them. Moreham (2006) provides a legal analysis on the question of whether a person might have a reasonable expectation of privacy with respect to actions taken or information revealed in a public place. Although her analysis is restricted to cases in the English courts, she demonstrates clearly that the courts have been willing to extend privacy protection to publicly revealed information, given consideration of location, the nature of the activity, the way in which the information was obtained, and the extent to which the individual is the specific focus of any further disclosure. Nissenbaum (1998) argues for a right to privacy that extends to public spaces. She bases her argument in a notion of 'contextual privacy' that suggests that information is revealed for particular purposes in particular contexts, and that privacy violations occur when that information is used for other purposes or in other contexts. According to Nissenbaum, the notion of contextual integrity applies even in public, and privacy violations can occur if publicly revealed information is used for unintended purposes by unanticipated parties. Finally, Cheung (2009) argues that public privacy is becoming increasingly important in the Internet era, given the ease and speed with which revealed content can be captured and disseminated to an extremely broad audience. Further analysis is required to determine whether the principles outlined by these authors provide motivation for a privacy interest in social network profile information;

the notion of 'privacy in public', however, clearly offers an interesting lens through which to view the issue of privacy in online social spaces, and offers potential for the extension of a privacy protection to information revealed in these spaces. AQ5

Acknowledgements

The authors thank the Office of the Privacy Commissioner of Canada for support for this research through their Contributions Program.

References

Abril, P. S. (2007). Recasting privacy torts in a spaceless world. *Harvard Journal of Law and Technology*, *21* (1), 1–47. Retrieved from http://jolt.law.harvard.edu/articles/pdf/v21/21HarvJLTech001.pdf

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). Retrieved from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/1394/1312%23note4

boyd, d. (2007). 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: MIT Press.

Carey, R., & Burkell, J. (2009). A heuristics approach to understanding privacy-protecting behaviors in digital social environments. In I. Kerr, V. Steeves, & C. Lucock (Eds.), *Lessons from the identity trail* (pp. 65–82). New York, NY: Oxford University Press.

Cheung, A. S. Y. (2009). Rethinking public privacy in the Internet era: A study of virtual persecution by the Internet crowd. *Journal of Media Law*, *2*, 191–217. Retrieved from http://ssrn.com/abstract=1683422

Crocker, T. P. (2009). From privacy to liberty: The fourth amendment after *Lawrence*. *UCLA Law Review*, *1*, 1–69.

Debatin, B., Lovejoy, J., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*, 83–108. doi:10.1111/j.1083-6101.2009.01494.x

Frangione v. Vandongen et al., ONSC 2823 (May 18, 2005) (2010).

Gelman, L. A. (2009). Privacy, free speech, and 'blurry-edged' social networks. *Boston College Law Review*, *50*, 1315–1344. Retrieved from http://ssrn.com/abstract=1520111 AQ6

Grimmelmann, J. (2009). Saving Facebook. *Iowa Law Review*, *94*, 1139–1206. Retrieved from http://ssrn.com/abstract=1262822

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

Häkkilä, J., & Chatfield, C. (2005). 'It's like if you opened someone else's letter': User perceived privacy and social practices with SMS communication. *Proceedings of the 7th international conference on Human Computer Interaction with Mobile Devices and Services* (pp. 219–222).

Joinson, A. (2008). Looking at, looking up or keeping up with people? Motives and uses of Facebook. *Proceedings of the twenty-sixth annual SIGCHI conference on Human Factors in Computing Systems* (pp. 1027–1036). doi:10.1145/1357054.1357213

Kerr, O. S. (2010). Applying the fourth amendment to the Internet: A general approach. *Stanford Law Review*, *62*, 1004–1049. Retrieved from http://ssrn.com/abstract=1348322

Lange, P. (2007). Publicly private and privately public: Social networking and YouTube. *Journal of Computer-Mediated Communication*, *13*(1). Retrieved from http://jcmc.indiana.edu/vol13/issue1/lange.html

Lee, D. H. (2009). Mobile snapshots and public-private boundaries. *Knowledge, Technology and Policy*, *22* (3), 161–171.

Lewis, J., & West, A. (2009). 'Friending': London-based undergraduates' experience of Facebook. *New Media and Society*, *11*(7), 1209–1229. doi:10.1177/1461444809342058

Moreham, N. A. (2006). Privacy in public places. *Cambridge Law Journal*, *65*(3), 606–635. doi:10.1017/S0008197306007240

Murphy v Perger, O.J. No. 5511, 67 C.P.C. (6th) 245 (OSCJ), Ont SCJ 2007 (2007).

Nissenbaum, H. F. (1998). Protecting privacy in and information age: The problem of privacy in public. *Law and Philosophy*, *17*, 559–596. Retrieved from http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf

Park v. Mullin, BCSC 1813 (2005).

Patchin, J. W., & Hinduja, S. (2010). Trends in online social networking: Adolescent use of Myspace over time. *New Media and Society*, *12*(2), 197–216. doi:10.1177/1461444809341857

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. Albany: State University of New York Press.

R. v. Plant, 3 S.C.R. 281 (1993).

R. v. Tessling, 3 S.C.R. 432 (2004).

Rainie, L., Lenhart, A., & Smith, A. (2012). *The tone of life on social networking sites*. Pew Research Center's Internet and American Life Project. Retrieved from http://pewinternet.org/Reports/2012/Social-networking-climate.aspx

Rosenblum, D. (2007). What anyone can know: The privacy risks of social networking sites. *Security and Privacy*, *5*(30), 40–49. doi:10.1109/MSP.2007.75

Schuster v. Royal & Sun Alliance Insurance Company of Canada, CanLII 58971 (ON SC) (2009).

Sparks v. Dubé, NBQB 40 (2011).

Strahilevitz, L. J. (2004). *A social networks theory of privacy.* John M. Olin Law and Economics Working Paper No. 230 (2D Series). University of Chicago. doi:10.2139/ssrn.629283

Thelwall, M., & Wilkinson, D. (2010). Public dialogs in social networks: What is their purpose? *Journal of the American Society for Information Science and Technology*, *61*(2), 392–404. doi:10.1002/asi.21241

Tsjeng, Z. (2010, March 21). Facebook: Why we can't live without it. Guardian.co.uk. Retrieved from http://www.guardian.co.uk/technology/2010/mar/21/facebook-cant-live-without-it

Tverdek, E. (2008). What makes information 'public'? *Public Affairs Quarterly*, *22*(1), 63–77. Retrieved from http://www.jstor.org/stable/40441479

Vaughan-Nichols, S. (2013, May 14). Facebook remains top social network, Google+, YouTube battle for second. ZDNet.com. Retrieved from http://www.zdnet.com/facebook-remains-top-social-network-google-youtube-battle-for-second-7000015303/

Viégas, F. B. (2005). Bloggers' expectations of privacy and accountability: An initial survey. *Journal of Computer-Mediated communication*, *10*(3), Article 12. Retrieved from http://jcmc.indiana.edu/vol10/issue3/viegas.html