

Winter 3-30-2013

# The View From Here: User-Centered Perspectives on Social Network Privacy

Jacquelyn A. Burkell

*Faculty of Information and Media Studies, UWO, jburkell@uwo.ca*

Alexandre Fortier

*Western University, afortie2@uwo.ca*

Lorraine Wong

*Western University, lola.wong@uwo.ca*

Jennifer Lynn Simpson

*Western University, jsimps4@uwo.ca*

Follow this and additional works at: <https://ir.lib.uwo.ca/fimspub>

---

## Citation of this paper:

Burkell, Jacquelyn A.; Fortier, Alexandre; Wong, Lorraine; and Simpson, Jennifer Lynn, "The View From Here: User-Centered Perspectives on Social Network Privacy" (2013). *FIMS Publications*. 25.

<https://ir.lib.uwo.ca/fimspub/25>

# **The View From Here: User-Centered Perspectives on Social Network Privacy**

Final report to the Office of the Privacy Commissioner of Canada, Contributions  
Program 2011-2012

Jacquelyn Burkell, The University of Western Ontario

## **Research Team:**

**Alexandre Fortier**

**Lola Wong**

**Jennifer Simpson**

**Craig Butosi**

**March 31, 2013**

## Table of Contents

Abstract	1
Introduction	2
Background	6
Privacy Expectations in Online Social Networks: Results from Interviews and Focus Groups	8
Participants	9
Profile Information	12
Audience	16
Sharing	18
Competing Interests	21
Discussion	23
Investigating Subjectivities: Q Methodology	25
Methodological Background	27
Characterizing Facebook: The Q-sample	29
Method	29
Participants	31
Results	32
Consensus Statements	33
Factor 1: Facebook profiles should be controlled by their creator.	34
Factor 2. Facebook profiles are ‘fake’ and everyone knows the rules	35
Factor 3. Facebook profiles are personal spaces.	37
Discussion	38
Limitations and Future Research	40
Recommendations	41
References	48
Appendix 1: Interview and Focus Group Sample Topics	55
Appendix 2: Q Sample Statements	59
Appendix 3: Q Sort Factor Matrix with Defining Sorts	62
Appendix 4: Consensus Statements	64
Appendix 5: Factor 1 Distinguishing Statements	65
Appendix 6: Factor 2 Distinguishing Statements	67



## Abstract

A great deal of personal information is released in online social network profiles, and this information is increasingly being sought as evidence in criminal, administrative and civil legal proceedings. Determination of the admissibility of social network profile information rests in part on the issue of subjective expectations of privacy: to what extent do online social network participants expect privacy in their social network profiles? This question is examined through a combination of interviews and focus groups. The results suggest that Facebook as a whole is characterized as a space where participants construct and display a produced version of the self to a large and indeterminate social network. The common perspective is that information posted on social network profiles is selected for social broadcast, and further dissemination (beyond the online social network to which information is disclosed) is therefore both acceptable and to be expected. Although they would prefer profile access to be restricted to a broadly defined social network of friends and acquaintances, online social network participants do not in general expect to control the audience for their profiles, and they therefore typically include only information that 'everyone' can know in their online profiles. They thus require and exercise control over the content that is associated with their online profiles, and actions that undermine this control run contrary to privacy expectations.

## Introduction

*“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 March 21, 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, 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, and Smith, 2012). Users perform a variety of social 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). Users also have opportunity for less explicit, but no less revealing (see Kosinski, Stillwell, and Graepel, 2013) information sharing, through actions such as ‘liking’ a website, ‘checking in’ at a location, or participating in an online game.

Online social networks are all about the sharing of personal information, so it isn’t surprising that participants reveal in their online profiles a great deal about themselves (see, e.g., Gross and Acquisti, 2005), and much of the information shared explicitly and implicitly supports the inference of even more personal details (Kosinski, Stillwell, and Graepel, 2013). 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’; see Granovetter, 1973, for a discussion of ‘weak ties’) with whom the participants neither have nor anticipate extensive interaction in the face to face world (Lewis and West, 2009). The apparently profligate self-revelation of online social network participants might suggest that users are unconcerned about privacy in these 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 and 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, 2008; Patchin and 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, 2009, for a discussion of how information that is formally public is accessed by 'blurry-edged' networks of interested others). We don't know quite how to think about these technologies and social spaces, we don't know quite how to behave within them, and, critically, we don't understand the social norms regarding disclosure and sharing in these spaces (see Häkkinen and 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).

This issue has heightened urgency because, increasingly, information posted on social networks is entering into the legal process (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 et al., 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 BCSC 1813). Prior decisions on s.8 of the Charter (e.g., *R v. Tessling*, 2004 SCC 67) have made it clear that the standard is *not* merely descriptive, as this approach would involve an inevitable erosion of personal privacy: instead, the reasonable expectation of privacy is viewed as a normative standard that fosters “the underlying values of dignity, integrity and autonomy, protecting a “biographical core of personal information” which would “tend to reveal intimate details of the lifestyle and personal choices of the individual” (*R v. Plant* [1993] 3 S.C.R. 281). 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 turn on the question of whether this information is ‘public’, taking a descriptive stance on the issues, and indeed making assumptions regarding the nature of social network disclosure. 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 size (typically relatively large) of the network within which profile information is explicitly shared, 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] O.J. No. 5511, 67 C.P.C. (6<sup>th</sup>) 245 (OSCJ), Ont SCJ 2007; *Schuster v Royal Sun Alliance*, [2009] O.J. No. 4518, 83 C.P.C. (6<sup>th</sup>) 365 (OSJC); and alluded to in *Sparks v Dubé*, 2011 NBQB 40). This comment in *Frangione v. Vandongen et al.*, 2010 ONSC 2823 is typical of the reasoning applied by the courts:

*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 at least arguably applying standards and norms from the ‘face to face’ world to establish whether there are privacy expectations in



the online environment. It is not clear, however, whether these standards and norms are directly applicable. Indeed, legal scholars have struggled, and continue to struggle, with the question of privacy in the online environment, working to map existing privacy law onto these new domains. Much of this scholarship is based in the US, 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': his is a fundamentally descriptive approach.

These and other legal and policy analyses can and should be strengthened by inquiry into the privacy 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 a factor that diminishes privacy expectations. 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. 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 project 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 developing values and expectations that govern information sharing and use.

## Background

In what is certainly the most well-known legal document on privacy, Warren and Brandeis (1890) highlighted the tension between nascent technology and established law for the protection of individual privacy. The new technology that concerned Warren and Brandeis was the camera, which provided previously unseen possibilities for the capture and subsequent publication of images. The new technologies of today are ubiquitous, deeply woven into every aspect of our everyday lives, and therefore challenging notions of personal privacy in ways that could not until now be anticipated. Online social networks, in particular, have changed the nature and context of much social interaction, with concomitant implications for the privacy of the personal information we choose to share with others in these environments.

Abril (2007) makes the point that the privacy, specifically the public/private distinction, has historically been linked to physical space, and indeed psychological investigations of the notion of privacy have similarly focused in the concept as enacted in the physical environment (e.g., Altman, 1975; Schwartz, 1968). The translation from physical privacy to conceptions of information privacy has been, at best, an uncomfortable one (see, e.g., Friedman, 2000). As with all forms of privacy, informational privacy is not uniformly desirable: there are conditions under which we want informational privacy, conditions under which we are desire or are willing to relinquish it (e.g., for purposes of self-promotion), and conditions under which it could even be considered undesirable (e.g., if lack of information compromises personal safety). The management of information privacy is, therefore, a matter of the *appropriate* flow of information (Nissenbaum, 2010), involving (as Petronio (2002) identifies) the management of a dialectic between privacy and information disclosure. Along with legal scholars such as Dan Solove (2008), these authors stress the importance of a contextualized notion of privacy, and therefore of privacy expectations. Privacy values, practices, and expectations cannot simply be imported from existing situations to new, apparently comparable ones. Instead, we have to treat these new situations as unexplored territory, and approach with an open mind the question of the privacy expectations they support.

Participation in online social networks is clearly of instrumental value. Participants enjoy enhanced social capital (Ellison et al., 2007; Steinfield et al., 2008), and this effect is particularly true for those with lower levels of self-esteem. Social capital benefits of online social network participation include both bridging capital (the development of heterogeneous networks of weak ties) and bonding capital (strong ties to close friends and family). Online social networks provide for young adults a venue for important developmental tasks including the development of strong social skills (Arnett, 2000) with long-term effects on identity and well being (Connolly et al., 2000; Montgomery, 2005). Uses and gratifications research suggests that participation in online social networks provides a form of escape from everyday pressures, and a primary use of Facebook is the exchange of social information (Quan-Haase and Young, 2010). Park et al. (2009) identified the major uses and gratifications of social networking site use to include socializing, entertainment, self-status seeking, and information, and LaRose and Eastin (2004) identified similar factors including information-seeking, entertainment, and social needs. Bumgarner (2007, no page) puts it particularly succinctly: “Facebook appears to operate primarily as a tool for the facilitation of gossip”. Young people in particular appear to value online social network participation for the opportunity to practice identity presentation and management in a relatively risk-free social context (Dunne et al, 2010). Thus, it appears that the exchange of social information is an important, if not *the* important, function of online social networks.

The exchange of so much social information raises the spectre of privacy concerns (see, e.g., Gross and Acquisti, 2005), and social network participants readily express their concerns about online privacy. Nonetheless, one of the salient findings in privacy research is the ‘privacy paradox’, wherein people regularly profess to a greater interest in privacy that their information revelations practices would suggest (typically identified in the online context: see, e.g., Barnes, 2006; Norberg, Horne, and Horne, 2007; Utz and Kramer, 2009). Studies that address online privacy, however, typically document information revelation or pose direct and decontextualized questions about the desire for privacy. Relatively little work has been done to elucidate the privacy norms that operate in these new spaces, and this research seeks to address that gap.

## Privacy Expectations in Online Social Networks: Results from Interviews and Focus Groups

This research focuses on individuals involved in online social networks, who are able to provide an ‘insider’ view on their own privacy expectations and practices. Instead of engaging participants in direct discussion about privacy issues, we examine this general question through a focus on reported privacy-related actions. This was a deliberate decision, taken in light of the well-established ‘privacy paradox’ (Barnes, 2006; Norberg, Horne, and Horne, 2007; Utz and Kramer, 2009), in which people express privacy concerns while at the same time failing to protect their personal information. We reasoned that privacy expectations are best reflected not in the expressed wishes of social network participants, but rather in their practices with respect to the information provided in online social network profiles.

Our particular focus is on the public/private nature of these online spaces, in an attempt to answer a core question: are online social networks *public* spaces, *private* spaces, or something in between? Our interviews and focus groups were conducted with active online social network participants, recruited through advertisements at a large Canadian university. Unstructured interviews and focus group discussions explored a wide variety of issues (a general list of topics is provided in Appendix 1), including but not restricted to:

- whether and to what degree online social networking spaces are ‘private’ spaces;
- whether participants see information posted to online spaces has effectively entered the ‘public’ domain, or to what extent that information remains private;
- whether and under what conditions the personal information of other social network users is examined and shared; and
- how competing interests (including free speech and security) should be balanced against privacy interests;

Each session was transcribed and the data were anonymized. Data analysis proceeded using a grounded theory approach (Glaser and Strauss, 1967; Glaser, 1992; Strauss and Corbin, 1990) to identify emergent themes.

At this moment in time, online social networking is effectively synonymous with Facebook: a recent PEW Center study, for example, indicated that 67% of Internet users were members of at least one social networking site, and of those 100% used Facebook

(PEW, 2013). Although there are many other available social networking platforms (e.g., Tumblr) and applications that support some social networking functions (e.g., Flickr), our interview and focus group discussions of online social networking inevitably and quickly turned to Facebook; moreover, although different social networking applications provide a slightly different context for discussion, our initial interviews suggested that privacy-related perspectives and issues did not differ widely across these platforms. Consistent with the PEW results, all subjects responding to our call for participants were (or in one case, had been) Facebook users, and although a minority also used other social networking platforms, this additional participation was not universal. Therefore, in order to provide common ground for discussion and in order to allow the largest range of potential participants to contribute to the research, we focused our interviews and focus groups on this specific social networking platform.

It is important to note that the focus group and interview discussions focused on information practices, including practices with respect to posting and practices with respect to sharing. It is well established in the extant literature that social network participants express concerns about privacy, and that they lack a full understanding of the privacy issues associated with online social networks (Debatin et al., 2009). Our focus in this research was not their knowledge (or lack thereof) of the very real privacy issues that face social network participants. The focus group and interview results are presented together, organized around four issues that bear critical relationship to privacy expectations:

- 1) Profile Information: Are social network profiles the locus of private disclosures (i.e., do participants treat them as ‘private’ spaces)?
- 2) Audience: To whom are these disclosures directed (i.e., who is the intended audience, what mechanisms of control are exerted)?
- 3) Sharing: How do participants use social network information, and particularly the information about others that they encounter there?
- 4) Competing Interests: How do participants trade off various interests in the disclosure and use of social network information?

## **Participants**

Participants were primarily recruited via posters placed at various locations on a large university campus in Ontario. An inclusion/exclusion questionnaire, distributed via e-

mail to respondents, determined eligibility. Questions included an indication of their level of educational or professional experience, and age. Suitable participants were those who were a minimum of 18 years of age. Once it was determined that the participants met the eligibility requirement, a mutually convenient time and place for the interview or focus group session were arranged. A compensation of \$20 for participation was offered to interviewees. Food and light refreshments were provided during focus groups.

Sampling was carried out to saturation, at which point no new categories or codes were emerging from interviews. Creswell (1998) and Morse (1994) suggest that in grounded theory research, saturation is typically with a sample of 30-50 respondents. We reached saturation with a sample of 40 participants (10 individual interviews and five focus groups, each with between 4 and 7 participants, for a total of 30 focus group participants).

Ten interviews were conducted from September through November 2011 with a variety of students and working professionals (70% were students attending university or college; 30% were in the workforce). Participants were predominantly female (80% female; 20% male) and tended to be between the ages of 18 and 36 (10% 18-20; 50% 21-29; 40% 31-36). All interview participants were university graduates. Over half (60%) indicated an undergraduate degree as their highest academic certification, while 30% had completed a masters degree, and 10% had completed a doctorate.

A total of 5 focus group sessions held in March of 2012. Each focus group session contained between 5-7 participants, and a total of 30 participants were included in all focus groups. All participants recruited for these focus group sessions were students at the University of Western Ontario. Participants were predominantly female (60% female; 40% male) and tended to be between the ages of 18 and 42 (66.7% 18-20; 30% 21-29; 3.3% 31-42). Education levels of participants ranged from undergraduate (70%) to graduate students (26.7%) to professional school student, such as law or business school (3.3%). Participants largely reported using social media on a daily basis, especially Facebook (43.3% almost always were on Facebook; 46.7% used Facebook multiple times a day; 6.7 used Facebook at least once a day; 3.3% almost never used Facebook). Focus group participants reported their approximate number of Facebook friends, and these values ranged from under 100 to over 1000 (3.3% had less than 100 friends; 10% had between 100-300 friends; 13.3% had between 301-500 friends; 20% had between 501-999 friends; 3.3% had over 1000 friends).

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 30's) and Fern (also in her 30s, both health care professionals, interview participants) are typical of the more conservative social network users who participated in the study. As somewhat older individuals (in their 30s) with professional identities (both are health care 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 20s, 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 choose 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, however, 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.

### Profile Information

One mark of a private space is that the information shared within it is considered private. We began our early focus groups by asking our participants how they would choose to share deeply personal information with family and friends. Their responses were simple and entirely consistent: so much so, in fact, that we soon dropped the question from our protocol. Universally and not surprisingly, participants reported using Facebook only to communicate ‘big news’ of interest to a large audience. For more personal messages, and particularly for sensitive information, they indicated they would use direct forms of communication, in part because social network communication is seen as ‘*impersonal*’.

Focus group and interview participants were asked to discuss the nature of personal and private information. Many spontaneously distinguished between the two, noting that personal information was a much broader category than private information. Information typically identified as ‘private’ included identifying information (name, address, social insurance number, etc.), financial information (credit card information, salary, etc.). Telephone numbers were identified as personal but not necessarily private: this was true particularly for cell phone numbers, which served as ways to facilitate contact without linking to other locating or identifying information (particularly physical address) and were therefore considered more ‘private’ in nature. Most participants indicated that they would *not* share this ‘private’ information in their online profiles. In particular, they were reluctant to share in their online profiles information that provided a physical connection to the real world person, such as address or landline telephone. In some cases, this is motivated by a safety concern:

*One thing I stopped doing on FB is saying when I’m going home because I live alone and it’s obvious that there is no one in my apartment if I’m going there. So I stopped doing things like that...*

Participants report that Facebook profiles are “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 those who post information “just want people to,



like, think they're cool or something." There is a general sense that the Facebook 'self' isn't 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.*

*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.*

*I think what I put on Facebook is just like just what I think is really clever*

Online social profiles appear to be shaped for impression management – to create the 'right kind' of impression for those perusing the profile.

In some sense, online social profiles seem to be constructed with the 'lowest common denominator' (see Hogan, 2010) in mind. Participants regularly remarked that they would not post 'extreme' content:

*What about your pictures? Would you put up some of your crazier party pictures up there?*

*Probably I wouldn't put the super crazy ones. If it was just me holding a drink then that is fine. And I wouldn't put too many, probably just one picture of me.*

*I don't think I have anything too bad about me on FB. Obviously I have pictures of my drinking and partying but nothing so bad. If an employer – drinking I don't think it's that bad. If an employer's not going to hire me because of a picture of my with a beer in my hand – I don't know. I think that is just a bit too much. Obviously if I'm doing something crazy, then that's different and understandable, but I don't have those pictures up. I just have normal ones.*

Instead, they regularly limited accessible content to information that was appropriate for the audience likely to see the content: a broadly construed socially connected network.

Participants rarely reported removing posted information from Facebook, indicating instead that they carefully considered postings *before* they appeared on the site. This isn't 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. In other cases, older information was seen to be embarrassing or irrelevant, and deleted for that reason. Although there was some recognition that deletion might not be an entirely effective way to eliminate information from an online profile, most participants felt that it was sufficient, perhaps because their focus was on removing this information from the view of their intended audience – that is, people to whom they are (perhaps loosely) socially connected:

*Recently on our floor these two people were having a fight over - they took old pictures of each other and tagged everybody so that everybody could see one another and laugh at them about it. And then everybody laughs at them because “Oh you used to look like that?!” And I didn’t want that to happen to me. So I deleted a whole lot of my pictures.*

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. As this participant notes, such information can be problematic:

*I get really annoyed with pictures because people will post pictures of drinking and I don’t want that on my profile. I don’t want people to be able to see – especially future employers or my mom or my mom’s friends or my younger sister’s friends – and I don’t want them to see that because they are younger. It’s just not something you want everybody to know but sometimes you can’t convince people to make it private or you can’t convince them to take off the picture. That really bugs me.*

Participants reported regularly and carefully monitoring their online profiles, including these images posted by others that, through tagging, become part of their online profile.

*I know that anytime I get - on my phone I get things from Facebook - and anytime it says tagged photo I’m at the nearest computer to make sure it’s not something gross looking or its something embarrassing so something I don’t want people to see. Because I have my mom on Facebook and I have aunts and I know for sure they creep. I’ve been at*

*my aunt's house before while she creeped by Facebook because she thinks that it's interesting. So I make sure as soon as I see that notification that I check it.*

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:

*[on being tagged in a photo] That might be bad if it implied I was hooking up with someone. Or doing something like that. I'd probably untag that one, just because when it comes to drinking and stuff my parents know, but hooking up – that's weird.*

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.

Finally, a persistent but subtle theme regarding responsibility ran through the interviews and focus groups. Participants responded negatively to what they saw as bad judgment regarding online content:

*I know a girl, a Facebook friend, a girl who will post pictures of her with her bong. I don't understand why anyone would ever do that. It's an illegal drug. Why would you put that on Facebook?*

*Um, well, I find that on Facebook especially that a lot of people in their "Info" will list their interests like drinking, partying, going to bars. If you're looking for a job or even if you don't want to be seen as that type of person you shouldn't put that information. It makes people see you as just a partier when you could be so many other things as well. So I find that's something that should be kept private even if you want people to know "Oh yeah you're really cool – you drink" but you don't have to put it on Facebook.*

Thus, each individual is responsible for their own online presence, and the consequences of any poor choices:

*On FB I wouldn't put up online anything that I consider to be embarrassing about myself. I wouldn't put anything that I wouldn't willingly tell someone offline about. I wouldn't put anything online that I wouldn't be willing to tell a large group of people offline.*

*I suppose the onus is on the person who put it out there. If you don't want people to know you shouldn't put it online.*

## Audience

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 and 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 explicitly articulate and control the audience for online postings.

Some participants have a very open policy when it comes to Facebook friends. One young student acknowledges 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 could “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. A male 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. None of the interview or focus group participants maintained an ‘open’ profile (one accessible to anyone, and thus without the access control mechanism of a friends list). Moreover, every participant articulated criteria for inclusion on the friends list that included some (though variable) degree of real-life social connection. Friends lists, no matter how large, represented a socially connected network.

Interview and focus group participants spontaneously and regularly referred to the audience for their Facebook postings as ‘big’, comprising ‘everyone’, or ‘the whole world’. According to participants, Facebook postings are appropriate for “bigger audiences” and “unselected” audiences, and a posting on Facebook indicates that “everyone” is to know the information. One participant indicated that he had chosen, for personal reasons, not to maintain a profile on Facebook. He reported 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. The consistent use of broad and encompassing terms to describe the audience seems quite meaningful, and entirely consistent with the sharing practices described below. In particular, participants in online social networks do not presume any obvious limits to their online disclosures. Most importantly, there is no assumption that online disclosures are restricted to the original social network to which they were revealed. As one participant puts it: “Friends have mouths and talk... when I put stuff on Facebook, I assume they’re going to tell people”.

Although online social networks are typically large and include many peripheral acquaintances, there is one group that is often actively restricted: family. Some participants simply refused to have their parents as ‘friends’, while others restricted their access to specific content (usually photographs). Parents (and often employers) are identified as belonging to a different social context, and while some participants are worried about the embarrassing things a parent might *do* online (thus reflecting badly on them), more are concerned that parents will see compromising content. The concern seems to be a mixing of “family life with social life”, and participants express a desire to keep the contexts separate. This comment is typical:

*As far as restricting information on my profile goes, I’m fairly open about everything with my friends – absolutely 100 per cent. I have a cousin that is younger than me, so that’s the only person that can’t see my content – and that’s something just to stop my family from seeing the shenanigans that I get up to.*

These restrictions, however, are viewed as having more symbolic than practical value, because

*Yeah but you could have like – it's a small world definitely. I'm from [town] and there is people here that are – they know people from [town]. So there could be an employer that somehow – their daughter knows you somehow so you can still see it that way. Or there is always a way that they can find it.*

The best practice, then, is to assume the widest possible audience and to control content appropriately:

*Even though you have friend list, there are so many holes in the privacy settings. Like you better be ready that people are going to hear that. I post when I am ready for every person in the world to know. It's like, if anyone came up to me and said "Oh, this was you?" I could say "Yes, that was me" and I wouldn't be embarrassed.*

## Sharing

Although access to a Facebook profile is formally controlled by 'friends' lists and the 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., 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 that 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, 20s) 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..... 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 own Facebook practices and the degree to which they treated Facebook as a 'public' medium, 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, 30's). 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, 30s, health professional) has her own profile limited so that only friends can view it. Although she views her own postings as ‘private’ and 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.

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, 20s) 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 20's, 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.

### **Competing Interests**

Our interview and focus group participants were discussing their individual privacy-related practices and expectations. As such, they did not use the language or ‘rights’ in discussing competing interests. They did, however, identify limits to or conditions on the use of social network information, and the relevant perspectives are summarized here.

Although in general participants seemed to view information posted to online social profiles as ‘public’ in nature in that they presumed disclosure to a broad socially connected audience beyond the specifically identified online social network, they identified limits in the ways in which this information could be used. In particular, they were adamant that social network information could not be used in ‘negative’ or ‘malicious’ ways. While it was considered perfectly acceptable to ‘lurk’ online social profiles to satisfy social curiosity and to share the information of others for that same reason, there was general prohibition against seeking or sharing information in order to ‘hurt’ or ‘bully’ someone else. Furthermore, although ‘re-sharing’ of posted information was generally considered acceptable, many respondents reported that they would choose not to pass on information that was evidently highly personal, contentious, or potentially damaging. Thus, for example, online revelations regarding sexual orientation are treated differently than less evidently sensitive information:

*I think you can sort of grasp from some things, like, if they're sort or like a private thing or if they're ok to be shared. Like, if somebody sent me an email and was like 'I'm coming out of the closet. I'm gay.' ... I wouldn't go ahead and tell all my friends and be*

*like 'Oh so and so's gay! So and so's gay!' I'd wait and see what— if they had anything, like, if someone was like 'Oh, did you hear about so and so? I hear they're coming out of the closet,' or something and I'd be like [surprised] 'Oh yeah.'*

This is particularly true if the discloser is a 'real world' friend:

*Let's say someone 'comes out'. Now you maybe know, because you know this person, that certain people wouldn't appreciate hearing that. Does it matter, can you just go up to those people and tell them?*

*I think that would be incredibly – incredibly mean thing to do.*

*But can you? If the information is on Facebook that person decided to put it out to his network?*

*I suppose you can. I can't picture anyone doing that to a friend, you know what I mean? But I don't want to be the guy that says you can do that but you know...*

It appears, therefore, that 'real-world' social considerations derived from norms and relationships overlay and limit the online default of 'publicness'.

With respect to access to their *own* information (and this discussion was often more general than online profiles, extending to others records of online behaviour), respondents were prepared to accept corporate use for personal benefit:

*Yeah, no, doesn't bother me too much. Ummm, I have to admit that there's been a few times that the little Facebook ads have kind of been like 'Ooo! That is something I'd buy!' [laughs] you know what I mean?*

Thus, they would trade their online profile information for incentives (e.g., coupons). In general, they appeared willing to accept what might be termed *intrusions* (e.g., targeted ads), but *not* revelation:

*...associating my image with something that they want to promote and that I'm not sure if I want to promote... that was a no go.*

In general, they were sensitive to information uses or disclosures that contravened the 'contextual integrity' (Nissenbaum, 2010) of the online social network. One respondent indicating that social network profiles should not be accessed by border guards, since "[they] need to know how old I am, that I'm a Canadian citizen, things like that", but "you don't need to see my birthday photos or my friends". At the same time, participants accepted and were even willing to participate in such breeches if safety or security were at issue:

*let's say that my friend is a crack addict...and his mom comes and asks me to see his profile to find out where he is, it's because I know he's going to be harmed— like, something bad's going to happen to him. I'd show it, even though he's going to get in trouble,*

and they are willing to accept external monitoring of an access to their own information for similar purposes.

## Discussion

Based on our focus group and interview results, it appears that participants in online social networks provide personal information with the expectation of, if not hope for, widespread disclosure to a loosely connected social network. They insulate their online disclosures from unconnected strangers through privacy settings, and social practices largely respect this boundary. Many participants report attempts to 'wall in' socially connected adults (typically family members), providing them access to only limited parts of the profile, but they fully anticipate that these attempts will be unsuccessful, given the multiple social pathways that exist between connected individuals. For example, they recognize that even if parents are restricted from seeing online photo albums, they may encounter or even seek out some of these photos through the profiles of others to whom they are connected. Social network participants appear to accept and in fact universally participate in the practice of 'leaking' information posted in online social spaces to other socially connected individuals to whom the information was not specifically directed. Thus, they *expect* their social profile information to be dispersed beyond the group to which they explicitly disclose, and while many hope this audience does not include family members or employers, they recognize and accept the risk that information may reach these groups through social connections.

Although social network participants do not, therefore, appear to expect full control over the audience for their online disclosures, they *do* anticipate control over the *content* of those disclosures. Their first line of privacy defense is obvious and universal: highly personal content that is to be kept private is simply not posted to social network profiles. This makes sense, since social networks are sites of broadcast rather than personal communication. If only a few people should know, they are told directly (though perhaps using mechanisms for direct communication available within the social network platform), and postings to online social profiles are reserved for more widespread disclosures. Participants select and carefully formulate their own posts to create a

produced version of themselves, and while many are comfortable with having online social connections contribute to their profile through mechanisms such as wall posts and tagging in photographs, they expect to be able to decide whether and how that information appears in their profiles. It is here that their privacy expectations can most easily be violated, since the mechanisms used to exercise this control are relatively rudimentary, and do not anticipate technological innovations or changes to platforms policies that can undermine this control.

In some sense, social network participants operate with a ‘what you see is what you get’ model of their own online presence. This is evident in two widespread practices (or in some cases, plans) for content control: deletion and dissociation. While they limit online disclosures to information they currently consider appropriate for ‘public’ display, many participants realize that changing life circumstances (e.g., moving into the job market) may well change their perceptions of ‘appropriate’ content. In this event, they expect to be able to limit the content of their online presence by deleting items or, in extreme cases, entire profiles. Although this may not be technologically sufficient to remove the information from their online social presence, they *expect* it to be enough. Dissociation as a content control strategy is even more commonly discussed. Participants rely on tools that alert them when content posted by others is linked to their profile, and they regularly review this content to ensure that it is appropriate. Although some participants would request offending content to be removed, most suggest that content is owned by the individual who posts it, and such requests would be at best unusual if not actually inappropriate. The more common response to problematic content is simply to ‘untag’ or ‘unlink’ oneself, thereby breaking the link between content and profile. Tools or services that automate such linking (e.g., automated face recognition) limit the effectiveness of this ‘delinking’, and the negative reaction to such tools suggests that they contravene the privacy expectations of social network users (see : <http://www.dailymail.co.uk/news/article-2207098/Facebook-switch-controversial-facial-recognition-feature-following-data-protection-concerns.html>). In general, the invisible ‘vertical’ privacy risks described in Debatin (2011) that involve the “systematic collection, aggregation, and use of data by the networking company” (p. 55) present the greatest challenges to privacy expectations, despite (or perhaps precisely because) they remain largely invisible to the social network user.

It turns out, then, that the courts, and Strahilivetz (2004), have it right: what you tell your 200 closest Facebook friends *is* effectively public, and everyone knows it. The bottom

line is that social network participants are perfectly aware of and comfortable with the widespread social disclosure of the information they post to their online profiles. They may not *like* some of the places it goes, any more than I liked it when I was a teenager and my mother overheard some acquaintances talking about my Saturday night escapades (I was grounded for a month), but they *accept* it as a fact of (social) life, and they govern themselves accordingly. For the rare individual who maintains an online social profile restricted to only the closest of friends and family members, there may exist a viable expectation that online profile information is private: even these individuals, however, are likely to further disclose the information shared with them by others outside of this very small network.

Online social network users also recognize that inferences will be made about them on the basis of the profiles they present (see, eg., Buffardi and Campbell, 2008), especially since they participate in exactly this kind of social sense-making in response to the profiles they encounter. Such inferences, however, are made on the basis of a visible profile, the content of which the user has actively constructed or at least approved. Given the degree to which participants expect to control their online presence, we must assume that datamining activities that tie together numerous sources of information to draw accurate conclusions about undisclosed social and personal information (Bachrach et al., 2012; Kosinski, Stillwell, and Graepel, 2013) will represent an unwelcome intrusion: the typical social network participant would claim that if they wanted everyone to know, they would have posted it themselves. In considering the privacy expectations of online social network participants, therefore, courts should focus on *content* rather than *audience*. Online social network participants expect to control the content of their profile, and this is the subjective expectation that courts should consider when determining the admissibility of social network profiles.

## Investigating Subjectivities: Q Methodology

The results of the focus groups and interviews suggest that Facebook participants allow for and indeed almost expecting sharing of profile information beyond the confines of the

online social network. Participants seem well aware that online profiles constitute *exhibitions* rather than *performances* (see Hogan, 2010), and they view themselves as curators of their personal exhibition spaces. In general, participants in the focus groups and interviews recognize the extended and not strictly bounded audience for online social profiles, and even those who actively limit access to their own information tend to treat the profiles of others as if they are intended for the larger public. The presumed purpose of online information sharing is social display, and our respondents suggest that information is carefully selected with exactly this purpose in mind, and with the recognition that *actual* audiences, and not just declared distribution lists, should be considered when constructing online profiles. The results of the interviews and focus groups suggest, therefore, that the default view of Facebook is of a public space.

The mere existence of a default view does not, however, preclude the possibility of different *subjective* perspectives on Facebook, and indeed some of the focus group and interview participants seem to suggest that they use the platform in ways that are substantially different from what they perceive as being the default, while others describe the use of specific groups (parents being one salient example) as being atypical of what they might consider to be ‘standard’ practice. In particular, we noted that while some participants undoubtedly treated their own profiles as they saw those of others, that is, as produced exhibitions of the self meant for widespread public consumption, others appeared to treat their own Facebook profiles as loci of highly personal communication directed to a select audience of close friends and family members. This apparent variation in individual or personal practice appears to exist within a common perspective of the ‘typical’ Facebook member who uses the platform for public self-promotion.

Our goal in this portion of the research was to articulate the different subjective perspectives on social networks and social network use that characterize participants in these online networks. We employ a methodology particularly suited to this endeavour – Q methodology – in order to achieve this goal. Based on the interview and focus group results, we anticipate that social network participants will vary along two dimensions: first, whether they consider Facebook (or other online social networks) to be a venue for personal communication or social display; second, whether they view content of and audience for Facebook profiles as something to be tightly controlled or left relatively open. The combination of these two dimensions can be considered to produce four ‘types’ of social network users: personal communication/controlled users who see Facebook as a space for connecting with family and friends; social display/controlled

users who see Facebook as a site for display of a controlled image to a designated audience; social display/open users who view Facebook as a place for broad social connection and less controlled social display; and personal communication/open users who view Facebook as a place to disclose highly personal information to a broad and undefined audience (this last group we assume will be difficult to find, since this constitute a somewhat deviant mode of interaction). In order to test whether these different profiles can be identified in a group of typical Facebook users, we asked users to examine a set of statements about Facebook, based on interviews and focus groups, and to identify the degree to which they agreed with each statement. The resulting ‘sorts’ were subjected to an analysis (described below) that identified participants holding similar attitudes; these ‘factors’ constitute subgroups within the sample who hold different opinions on the nature and use of Facebook.

### **Methodological Background**

Q methodology provides a complete, distinctive and systematic approach for the quantitative analysis of human subjectivity (McKeown and Thomas 1988, 11–12). Subjectivity—or a person’s point of view on any matter of personal or social importance—is anchored in a person’s “internal” frame of reference. Drawing from their experience, individuals express opinions, and the purpose of Q methodology is to reach understandings of such experience. Q-studies, adhering to the methodological axiom that “subjectivity is always self-referent”, preserve respondents’ frame of reference by enabling them to model their own viewpoints through the rank-ordering (Q-sort) of a sample of statements (Q-sample) (McKeown and Thomas 1988, 12). By doing so, respondents express their “subjectivity operantly” (Stephenson 1968, 501), i.e. without the influence of an external frame of reference brought by an investigator or by other subjects in the context of a focus group discussion.

A Q-sample is a purposively sampled set of stimulus items on a specific domain of subjectivity, which was termed by Stephenson (1978) as a “communication concourse”. The collection of statements in a Q-sample can be assembled in a number of ways, and McKeown and Thomas (1988, 25–30) suggest two axes to classify Q-samples. The first axis represents the sources from which the statements are taken: naturalistic Q-samples are based on the respondents’ own communications (both oral and written) and ready-made Q-samples use statements derived from sources outside of the study. Neither type of source is considered to be superior to the other, and the choice of one Q-sample type depends on the context of the study (McKeown and Thomas (1988, 25). The second axis

represents the process of selecting statements to be included in a Q-sample. Statements can either be selected for their presumed relevance without ensuring coverage of all possible sub-issues (unstructured sampling), or they can be tested through a factorial experimentation (inductive or deductive) whereby they are assigned to conditions defined by the researcher (structured sampling). The latter reduces the risk of introducing a bias in the sample (McKeown and Thomas 1988, 28–30).

Through Q-sorting, each participant models his or her own point of view by rank-ordering Q-sample stimuli along a continuum defined by the researcher. Q-sorting can be based on a simple request for agreement or on operationalization of theoretical constructs. Multiple scenarios (i.e. Q-sorting under various conditions with the assumptions that participants will behave differently) can act as surrogates for behavioural hypotheses (McKeown and Thomas (1988, 30–31).

In Q methodology, Q-sorts are the variables and data analysis carried out through three sets of statistical procedures: correlation, factor analysis and computation of factor scores. As opposed to R methodology where tests and traits are correlated, Q methodology focuses on the correlation between and factoring of persons. Factor analysis, which uses a mathematical process that is virtually identical to the one used in R, is the core of Q methodology, as it comprises the statistical means by which subjects are grouped. The factors represent clusters of participants who express similar opinions as represented by similar Q sorts. The loadings of participants on factors identify their degree of association with the factor: loadings vary between -1 and +1, with loadings toward either end of the scale representing a stronger (positive or negative) association with the factor. Factors are interpreted by examining the relationship between *statements* and the factors, and a composite or idealized sort of the statements can be identified for each factor, representing the way in which a hypothetical respondent who *perfectly* matched the factor would sort the statements. Comparisons between the idealized sorts for the various factors can be used to identify the *consensus* statements (which do not differ between factors or viewpoints) and the *distinguishing* statements, which characterize the difference between factors.

Sample sizes in Q methodology are typically small, usually 30-50 participants, and the focus of the methodology is to articulate the different subjective positions, rather than to make any claims about their relative frequency (McKeown and Thomas (1988, 36).



## Characterizing Facebook: The Q-sample

To examine the privacy expectations within social media, a sample of statements and opinions were drawn from the interviews and focus groups. As the results of the interviews and focus groups were analysed, it became apparent that Facebook could be characterized in two ways: as a social space or as a personal space. In discussing privacy and information disclosure/management in online social networks, participants discussed six general categories of issues: access to content posted, persona management, social norms surrounding content posted, audience management, privacy management, and lurking behaviours. A sample of 60 statements was developed that reflected the various combinations of the two general orientations (social space/personal space) and the six issues.

Q-sample items include:

- When I post something on Facebook, I am making a public announcement. (public space, access to content)
- When I post something on Facebook, it is only intended for my “friends” list. (personal space, access to content)
- Everyone should know that at a social event photos will be taken and posted on Facebook. (public space, social norms)
- People should check with others before tagging them in photos or posts. (personal space, social norms)

The complete Q-sample can be found in Appendix 2.

## Method

Participants rank-ordered the 60 statements by sorting them on an 11-point scale ranging from -5 (most *unlike* my point of view) to +5 (most *like* my point of view). Participants were given a sorting diagram that indicated the number of items to be placed in each category (see Figure 1). They began by reading through the statements and dividing them into three groups: those with which they agreed, those with which they disagreed, and those about which they were neutral, ambivalent or uncertain. Each participant then chose the three statements with which they agreed the most and the three with which they disagreed the most, and placed these into the +5 and -5 columns respectively. They were then asked to choose from the remaining items the four items with which they most strongly agreed and the four with which they most strongly disagreed: these were placed in the +4 and -4 columns. They continued in this manner (selecting the number of items

for each column as identified in Figure 1) until they had 10 statements left. These were put into the 0 or neutral column.

**Figure 1: Distribution of statements in Q sort**

Most unlike my point of view					Neutral		Most like my point of view			
-5	-4	-3	-2	-1	0	+1	+2	+3	+4	+5
3 items	4 items	4 items	7 items	7 items	10 items	7 items	7 items	4 items	4 items	3 items
item	item	item	item	item	item	item	item	item	item	item
item	item	item	item	item	item	item	item	item	item	item
item	item	item	item	item	item	item	item	item	item	item
	item	item	item	item	item	item	item	item	item	
			item	item	item	item	item	item		
			item	item	item	item	item	item		
			item	item	item	item	item	item		
					item					
					item					
					item					

## Participants

In addition to the Q-sort, participants completed a questionnaire soliciting information regarding their gender, age, level and field of study, frequency of Facebook use, number of years using Facebook and number of Facebook friends. Over three quarters of the participants (78%) were female ( $n = 32$ ) and 22 percent were male ( $n = 9$ ). They ranged in age from 18 to 51 years ( $Mdn = 21$ ). Eighty-three percent ( $n = 34$ ) were students and 17 percent ( $n = 7$ ) were non-students. Among participants who were students, 71 percent ( $n = 24$ ) were undergraduate students, 26 percent ( $n = 9$ ) were graduate students and 3 percent ( $n = 1$ ) were professional students. They were distributed among disciplines as follows: 41 percent ( $n = 14$ ) from humanities and social sciences, 38 percent ( $n = 13$ ) from natural sciences and engineering, and 21 percent ( $n = 7$ ) from health sciences. Among participants who were not students, 43 percent ( $n = 3$ ) reported having high school education, 43 percent ( $n = 3$ ) reported having an undergraduate degree and 14 percent ( $n = 1$ ) reported having a graduate degree.

Participants reported being Facebook users for 7 months to 7 years ( $M = 5$  years,  $SD = 1.28$ ). Participants also indicated their frequency of Facebook use by choosing from the following categories:

- I'm almost always online: 9.8 percent ( $n = 4$ );
- Multiple times per day: 46.3 percent ( $n = 19$ );
- At least once day: 14.6 percent ( $n = 6$ );
- Multiple times during the week, but less than once a day: 12.2 percent ( $n = 5$ );
- About once a week: 4.9 percent ( $n = 2$ );
- Once every few weeks: 2.4 percent ( $n = 1$ );
- Once a month: 0 percent;
- Almost never: 9.8 percent ( $n = 4$ ).

Finally, 14.6 percent ( $n = 6$ ) had less than 100 Facebook friends, 29.3 percent ( $n = 12$ ) had between 100 and 300 friends, 39 percent ( $n = 16$ ) had between 301 and 500 friends, 14.6 percent ( $n = 6$ ) had between 501 and 999 friends and 2.4 % ( $n = 1$ ) had more than 1000 friends.

## Results

The 41 Q-sorts were correlated then factor analyzed, using the principal components method with a varimax rotation, to discover the groupings of opinions expressed among the participants. Three solutions were considered: a 2-factor solution, a 3-factor solution, and a 4-factor solution. The three-factor solution was deemed most adequate, as the results were most interpretable and subjects showed the strongest tendency in this solution to load on a single factor. Table 1 provides details on the subjects defining each factor (i.e., those with a loading on the factor of over .65 along with loadings on the other two factors of less than .4); the bolded loading for each subject indicates the factor with which they are primarily associated. The complete factor matrix can be found in Appendix 3. The interpretation of these three factors uses the ‘factor scores’ for the statements on each factor. These factor scores are the weighted z-scores for each statement reconverted to an array of scores corresponding to the +5 to –5 values used in the Q-sorting. Thus, the statement factor scores can be interpreted as an idealized Q sort for each factor, and examination of this idealized sort allows interpretation of the meaning of the different factors.

As is typical and indeed appropriate for Q method studies, the number of subjects is small, and in fact insufficient to allow statistical testing of the differences between subject profiles. It appears, nonetheless, that subjects loading on the first factor are less frequent users of Facebook, and this group appears also to have members with the greatest range of ages.

**Table 1: Factor Matrix for Selected Subject in Privacy Expectations within Social Media (highest loading in bold)**

Subject	Factor loading			Gender	Age	Frequency of FB use	Number of FB friends
	1	2	3				
Q10	<b>0.7617</b>	0.2886	0.2841	F	25	Multiple times per day	180
Q33	<b>0.6951</b>	0.3747	0.1125	F	31	Almost never	300
Q99	<b>0.6699</b>	0.3906	0.1516	F	29	Multiple times per week	10
Q05	<b>0.6694</b>	0.1561	0.0694	F	21	Almost never	15

Q03	<b>0.6595</b>	0.1609	0.3683	F	40	Multiple times per day	301
Q17	0.0995	<b>0.8133</b>	0.1050	M	18	Multiple times per day	560
Q30	0.2767	<b>0.7036</b>	0.1410	F	28	Multiple times per day	330
Q13	0.2913	<b>0.6974</b>	0.1932	F	18	Multiple times per day	346
Q40	0.2965	<b>0.6595</b>	0.0510	F	18	Multiple times per day	400
Q37	0.2287	0.0203	<b>0.6512</b>	F	20	Multiple times per day	150

### Consensus Statements

Before turning to examination of the differences between the factors identified in the Q sort, it is important first to note the ‘consensus statements’, that is, the statements that did not distinguish between the groups. This set of statements, and the ratings that are associated with each factor, represent a perspective that is common across all groups.

With respect to content, there is general disagreement with the statement that ‘What I see on Facebook reflects what is going on in real life’ (-3, -4, and -5 respectively for the three groups). All groups also tend to disagree with the statement that ‘For me, Facebook is all about parties and having a good time’ (-2, -3 and -4 respectively) and, to a lesser degree, with the statement that “Content posted on Facebook should not be boring” (-2, -1, and -1). It is notable that there is an almost entirely neutral response across all three groups to the statement “People can post good and bad stuff about themselves on Facebook” (0, 0, and 0): we had anticipated that some people, particularly those whose use of Facebook is primarily as a space for self-exhibition, would have a strongly negative evaluation of this statement. The consensus on Facebook content, therefore, seems to be that Facebook content represents a ‘staged’ version of life; at the same time (and somewhat contrary to the opinions expressed in focus groups and interviews) there do not appear to be requirements for posted content to be interesting or exciting, or to demonstrate social engagement.

In general, all participants disagree that it is ‘important to have a large number of Facebook friends’ (scores of -4, -5, and -4 for the three groups). Response is largely neutral, with little if any difference between the groups, to the statement ‘I use Facebook friendships as a way to get to know new people’ (-1, -1, and 0). Thus, there is consensus that the size of the Facebook network is not of primary importance, and Facebook is not strongly identified as a tool for expanding social networks. These consensus statements

suggest that social network participation is not, among the participants we studied, a way of assembling and demonstrating a large group of online friends and acquaintances.

Finally, there is consensus with respect to a number of statements related to information control and/or profile access. Thus, participants are generally reluctant to share their Facebook passwords with people they trust (-4, -3, and -3). There is no strong feeling one way or the other with respect to the efficacy of privacy settings to “limit people’s ability to find out about each other”, and this neutrality is consistent across all three factors (-1, -1, and 0). There is general agreement, not significantly different in degree across the three factors, with the statement “If I’m uncomfortable with it, I can always “untag” myself from a photograph (2, 4, and 2). The complete list of consensus statements is available in Appendix 4.

#### **Factor 1: Facebook profiles should be controlled by their creator.**

This view acknowledges that content posted on Facebook is meant to be shared, but the factor is defined by the importance of respecting one’s desired persona and intended audience on Facebook. Participants consider that, when it comes to what is posted on their own profile, they should be in control (scores in parenthesis for Factor 1, 2 and 3, respectively; negatively rated statements in italics). They agree strongly with the statement that

- I should be the one to decide what is posted about me on Facebook. (4, 0, 1), and disagree that
- *Other people can post the content they want about me on Facebook. (-5, -1, -4).*

Their view that the profile owner should be in control appears to extend to the profile of others, especially with respect to photographs. Members of this group feel that

- Before posting photos on Facebook, people should get permission first (4, 0, 1)
- People should check with others before tagging them in photos or posts. (2, -1, 1), while they disagree with the statement that
- *It’s ok to tag others in photos or posts without checking with them first—they can always “untag” themselves. (-3, 1, -1).*

These notions of control also relate to profile access: members of this group tend to respond negatively to any statement concerning ‘unauthorized’ profile access (e.g., ‘friend of friend’ access to profiles), suggesting that they may feel more strongly than participants who load on other factors that the ‘friends’ list should be an access control mechanism:

- I wouldn't share information by letting others look at profile through my Facebook account. (2, -2, -2)
- *It's ok to let my real world friends look at profiles through my Facebook account* (-2, 1, 2)
- *I would ask others to help me view profiles I can't access.* (-4, -2, 0).

Although their perspective is not extreme, they appear in general less likely than members of other groups to share information posted on Facebook beyond the original group to which it was posted.

- Information posted on Facebook is meant only for that person's online network (1, -2, -1)
- I keep information I find on Facebook to myself (0, -2, -3)
- *I can share information I find on Facebook with friends and family* (-1, 1, 1).

At the same time, and somewhat surprisingly, members of this group appear to put the onus on the profile owner to identify information that is *not* meant to be more widely shared:

- If someone wants to keep something on Facebook "private", he or she should make sure people know about it. (3, 1, -2).

Although they do not express strong opinions on the issue (i.e., they tend to provide neutral ratings of these items), they are less likely than members of others groups to use Facebook to 'lurk' profiles to learn about other people:

- Just because I look at others' profiles doesn't mean I want to friend them. (0, 3, 3)
- I only look at Facebook photos of people I know well. (0, -3, -2)
- I use Facebook to lurk friends' profiles. (-2, 0, 0).

Members of this opinion group feel most strongly about content control, providing the most extreme (positive or negative) ratings of statements that reflect this issue.

Specifically, they feel that the profile owner should control *what* is posted to a profile. Although they also endorse profile owner control of information dissemination, their feelings on this issue are less strong, and content control is definitely their focus. The complete list of distinguishing statements for Factor 1 is available in Appendix 5.

## **Factor 2. Facebook profiles are 'fake' and everyone knows the rules**

While participants who define Factor 1 focus on *who* controls profile content and access, those who define Factor 2 are more Participants who characterize Factor 2 focus instead

on the on the *kind* of content that is shared in social Facebook profiles. Although their general perspective is consistent with that of members of other groups, their opinions on content-related statements tend to be the most extreme, consistently supporting the interpretation that they see Facebook as a space in which participants present an ‘unreal’ or ‘produced’ version of the self. They tend, therefore, to agree with statements that identify Facebook profiles as divorced from ‘real life’, and *disagree* most strongly with statements that suggest that Facebook profiles are ‘real’ or ‘private’ in nature:

- What I see on Facebook isn’t necessarily representative of real life. (4, **5**, 2)
- I don’t post identifying information such as addresses, phone numbers and birthdays on Facebook. (3, **5**, -2)
- *My Facebook profile represents my true self.* (-2, **-4**, 1)
- *For me, Facebook is a place to post private thoughts and moments* (-5, **-5**, -5)<sup>1</sup>

Participants who share this view also tend, more than members of other groups, to trust social norms for regulating the content that people post about *others* on Facebook. Instead of focusing on profile owner control of content, they tend to endorse statements that reflect community standards or norms for Facebook content, and disagree least strongly with statements that focus on profile owner control of that content:

- There are rules about what is ok (and what is not ok) to put on Facebook. (1, **3**, -1)
- People should consider what their friends would want before posting content about them on Facebook. (4, **2**, 4)
- It’s ok to tag others in photos or posts without checking with them first—they can always “untag” themselves. (-3, **1**, -1)
- *People should check with others before tagging them in photos or posts.* (2, **-1**, 1)
- *Other people can post the content they want about me on Facebook* (-5, **-1**, -4)

Finally, although they do not feel strongly on the issue, participants who share this view are more likely than members of other groups to acknowledge Facebook as a place where ‘lurking’ is expected and appropriate:

- I use Facebook as a way to connect with lots of new people outside my close circle of friends and family. (-1, **1**, 0)
- I regularly look at Facebook photo albums of people I don’t know. (-3, **-1**, -3)
- *Facebook is for connecting with people, not for lurking.* (2, **-1**, 1)

---

<sup>1</sup> Note that although all groups have a -5 ranking for this statement, members of group 2 (i.e., those loading on Factor 2) show the *strongest* negative evaluation of this statement, as reflected in the z-scores (standardized scores) of -1.8, -2.3 and -1.5 for the three groups.



As with Factor 1, members of this group are focused on profile content. However, rather than suggesting that owners should be in control of the content that is posted about them, individuals who define Factor 2 appear to view profiles as appropriately co-constructed by members of the extended online social network, and they tend to rely on social norms to limit posted content. The complete list of distinguishing statements for Factor 2 is available in Appendix 6.

### **Factor 3. Facebook profiles are personal spaces.**

For participants who share this view, content on Facebook profiles is intended for one's restricted social network that reflects the real-world ties that exist between members. Members of this opinion group appear focused on the nature of the online social network, and they, more than members of other groups, tend to restrict their online social network to close friends and family:

- When I post something on Facebook, it is only intended for my “friends” list (2, 1, 5)
- It is the quality not the quantity of Facebook friends that matters. (2, 2, 5)
- I use Facebook mainly to keep in touch with friends and family (1, 2, 4).

It is likely the relatively restricted nature of their online social networks that leads members of this group to be *least* opposed to sharing Facebook passwords:

- I would never share my Facebook password. (5, 5, 2).

Participants who share this view tend to respond most *negatively* to statements that suggest that posting on Facebook is essentially a public announcement, and they are most likely to view Facebook information as something that is *not* to be shared widely:

- *If someone wants to keep something on Facebook “private”, he or she should make sure people know about it. (3, 1, -2)*
- *When I post something on Facebook, I am making a public announcement (1, 2, -1)*
- *Information posted on Facebook is meant to be shared widely. (-2, 1, -4).*

It is interesting to note, therefore, that they also *disagree* with the following statement:

- *I keep information I find on Facebook to myself. (0, -2, -3).*

Their relatively strong disagreement with this statement may reflect the nature both of their online networks and the types of disclosures they expect within them. In particular, since they are participating within networks of close friends and family, they may in fact be quite likely to discuss online disclosures within that defined group.

Members of this group indicate, more than members of other groups, that Facebook profiles are likely to represent their 'true' selves:

- My Facebook profile represents my true self. (-2, -4, **1**), and they are less strongly opposed to the posting of identifying information:
- *I am fine with posting identifying information such as addresses, phone numbers and birthdays on Facebook. (-5, -5, -1).*

Finally, although their opinions on these issues are not extreme, members of this group tend to feel that individuals should be in control of their own online profile. In general, their opinions on these issues are consistent with, but not as strong as, those of the participants defining Factor 1:

- People should check with others before tagging them in photo (2, -1, **1**)
- It's ok to post any cool, fun content about friends on Facebook. (-1, 0, **-2**)
- *Other people can post the content they want about me on Facebook. (-5, -1, -4).*

The complete list of distinguishing statements for Factor 3 is available in Appendix 7.

## Discussion

Based on the focus group and interview results, we anticipated that this investigation of subjective perspectives on Facebook would identify different perspectives that varied along two dimensions: first, whether they consider to be a venue for personal communication or social display; second, whether they view content of and audience for Facebook profiles as something to be tightly controlled or left relatively open. Our results are largely consistent with this expectation, in that we identified three factors, or opinion clusters, that fit into three of the four quadrants anticipated by the interaction of these two dimensions.

It is important to note that, consistent with the interview and focus group results, *none* of the groups identify Facebook as a locus of deeply personal exposure. Thus, while this investigation of different subjective positions vis a vis Facebook reveals a variety of 'opinion profiles' that are distinguished by expectations of who should control the online profile and the audience to which it is revealed, none of the groups suggest that social network disclosures are of the sort that would threaten personal dignity were they to be revealed.

Participants who share the view identified in Factor 3 express relatively strong privacy expectations with respect to the information they post. They restrict their online social network to people with whom they have close ties, and the content they post is intended only for these individuals. They do not widely share Facebook information, yet do not keep Facebook information ‘to themselves’. Future research is needed to provide insight into the nature of this information sharing, but it seems likely that individuals who endorse this perspective are likely to discuss information shared online with other members of their close social network. This view seems consistent with the perspective of some interview and focus group participants who identified themselves as having small and closeknit online social networks consisting of family and friends.

Participants who share the view identified in Factor 1 also have strong privacy expectations, but not as strong as those shared by Factor 3 participants, as they acknowledge that content posted on Facebook is meant to be shared beyond one’s network of close friends and family. They, however, believe that the owner of a Facebook profile should control who has access to his or her profile; they also express relatively strong beliefs that the profile owner should control the content that is posted.

Lastly, participants who share the view identified in Factor 2 express the least privacy expectations of all participants. They believe that content posted is meant to be shared and strongly disagree that it is a place for content of private nature. For them, the purpose of Facebook is to offer a staged display of themselves at which people are free to look — their Facebook profile is a place where people are allowed, if not expected, to lurk. This opinion profile appears to closely match the default view of social network participants identified in the interview and focus group results, suggesting that this default view is an accurate construction of some but not all social network participants.

Further research is needed to determine whether these opinion profiles are applicable to other social networking platforms, or restricted to Facebook. Furthermore, while this study demonstrates the *existence* of this variety of opinion profiles, it does not address questions of relative frequency, nor does it address the question of whether these perspectives are stable over time. In-depth interviews with individuals who define each of the profiles will provide a more nuanced understanding of these perspectives, providing insight into the genesis and implications of these social networking ‘types’.

## Limitations and Future Research

One of the obvious limitations of this research also represents a significant strength: the fact that participants were limited largely to active participants in online social networks. Our goal was to illuminate developing privacy norms and practices in these online spaces, and therefore a focus on active participants was deemed most appropriate. We acknowledge, however, that those less active in online social environments may hold different perspectives, and we encourage the extension of this exploration of privacy-related norms and behaviours to less involved members of these social communities. Our sample is also restricted with respect to both age and cultural background. The first we consider appropriate, since adults aged 18-29 are most likely to be social network site users (PEW, 2013). The geographic restriction of our sample has greater implications for the transferability of the results, particularly since research has demonstrated cultural differences in motivations for using social network sites (Kim et al., 2011), and we encourage the extension of this study to include participants from different cultural backgrounds. We focus our discussion on a single social network application: Facebook. In the current climate, it is impossible to talk about online social networking without talking about Facebook (PEW, 2013), and the focus on this platform is a natural reflection of this social reality.

The results of this research suggest important avenues for further work. The results of the interviews and focus groups suggest that online social network participants have little expectation of privacy with respect to the audience for their profiles; the control of profile content, however, seems to be very important. Further research should explore content control preferences and mechanisms with the goal of identifying tools and policies that will assist participants to exert the control they need and desire over their online presence.

The second phase of the research illuminated important and systematic differences in the subjective perspective of Facebook users. We identified three ‘opinion profiles’ that characterize different Facebook users, and suspect the existence of a fourth group. The perspectives we identified include: Facebook profiles should be controlled by their creators; Facebook is fake and everyone knows the rules; and Facebook profiles are personal spaces. Further research should examine the prevalence of these various perspectives and explore in detail the differing privacy practices and expectations of these groups.

## Recommendations

Boyd (2007) characterizes online social spaces as ‘networked publics’, consisting of digitally interconnected audiences with indistinct boundaries (see also Gelman, 2009). The social practices and expectations described by our research participants are consistent with this concept, in that their online profiles are produced for and many seem to participate as members of exactly such large and loosely linked social groups. In particular, online profiles are generally 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. Moreover, participants generally treat information posted by and about others in the same way, 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.

In light of this anticipated broad disclosure, online social network users exercise careful control over the content of their online profiles. Our results are consistent with those of Hogan (2010), who suggest that users take the “lowest common denominator” approach, generally restricting content to that which is appropriate for all network members. Much if not all information that they consider to be ‘private’ in nature is excluded, and participants report carefully consideration before posting information to their online profiles. They exercise similar care with information (including photos and comments) posted by others that can be linked to their profiles. Although at least some members of online social networks suggest that social norms effectively control this information, review of these additions is an important practice to social network participants. Online social network participants also recognize that their own standards for ‘appropriate’ material can change over time, and that occasionally they will need to remove material that was earlier deemed non-problematic. In these cases, content is controlled through two strategies: deletion and dissociation. Operating on a ‘what you see is what you get’ model of their own online presence, social network participants expect deletion and delinking to effectively remove information from their online profiles.

We began this research with a view to determining whether online social networks have the character of ‘public’ or ‘private’ spaces, and to articulate the social norms that govern participation in these spaces. The results are complex, and the answers to our original

questions are not entirely straightforward. Nonetheless, we can identify some general patterns.

Most centrally, online social networks do not appear to be spaces for the disclosure of highly personal information to a delimited audience. Social network profiles present a produced version of the self, constructed for social purposes: they appear to be a form of personal exhibit (Hogan, 2010) constructed with an eye to impression management (Leary and Kowalski, 1990). Social network profiles are regularly used for exactly the purpose of learning more about others. They are often the first place someone goes when (or even before) making a new acquaintance. There is general agreement that they present a ‘best version’ of the self – a starting place for getting to know someone. And since ‘getting to know’ or ‘learning more about’ someone is exactly the purpose of visiting online profiles, those profiles tend to be made available (both directly and indirectly) to a large audience. Control over *access to* online profiles does not, for most participants, appear to be a central focus.

While participants accept and even anticipate disclosure, therefore, to a social network that includes both articulated (in friends’ lists) and unarticulated (though further social sharing) members, there is some level of discomfort with disclosures that cross boundaries or mix different contexts (Nissenbaum, 2010). In particular, there is often a preference that family members be restricted from some information, and employers also regularly fall into this category. This does not, however, seem fundamentally different from offline considerations: if you go out to the bar and get falling down drunk, your mother or your employer just might hear about it – online or offline, you run that risk.

The difference with online social profiles, of course, is that the information is *displayed* and therefore available for examination and sharing. There is, therefore, a universally expressed desire to control the *content* of online profiles. Participants are concerned with how they will be seen or viewed by others on the basis of their profile information (raising issues of *dignity*, see Levin and Abril, 2009). They carefully select information for inclusion in their online profile, typically limiting content to that deemed appropriate for the broadest possible audience (Hogan, 2010). Failure to do so (i.e., the posting of content that is deemed ‘inappropriate’) meets with social approbation, and thus social network participants are viewed as responsible for controlling and maintaining their own online image. *Deletion* and *dissociation* are two critical strategies for content management, and participants rely on these strategies to control their online presence.

The fact that online social network participants know their information could (and probably will) be shared with a very wide audience and therefore carefully control content should not be taken to imply that there are no privacy considerations with respect to Facebook profiles: there are very real and well documents privacy risks associated with the revelation of personal information on social networking sites (see, for example, Rosenblum, 2007). Instead, these results support the perspective of Grimmelmann (2009, p. 1206):

*Users want and need to socialize, and they act in privacy-risking ways because of it. We cannot and should not beat these social urges out of people; we cannot and should not stop people from acting on them. We can and should help them understand the consequences of their socializing, make available safer ways to do it, and protect them from sociality hijackers.*

Grimmelmann is advocating a policy response that takes into account a norm of ‘sociality’ on Facebook: this paper documents that norm, demonstrating that participants view Facebook as a space for social disclosure to a broad and largely undefined audience. Policy responses that attempt to protect participants from the consequences of these disclosures must take this perspective into account.

In view of our results, we advocate three levels of response to protect the privacy interests of online social network participants:

- 1) Media literacy education
- 2) Tools for content management
- 3) Policy responses

#### *Media Literacy Education*

Media literacy, or an understanding of how the media operate and how they affect us, has long been considered a critical life skill (see, e.g., Potter, 2012). Educators have responded by including media literacy in school curricula (see, e.g., the Ontario Grade 1-8 curriculum:

<http://www.edu.gov.on.ca/eng/curriculum/elementary/language18currb.pdf>), and educators ensure that students understand how to interpret media messages. These interventions have not typically, however, focused on the *management* of one’s media presence. Online social networks are only one example of the opportunities for

individuals to *contribute to* as well as *consume* media, and as these opportunities increase so increase the challenges of online representation. Monitoring and managing one's online presence is becoming, therefore, a critical life skill (see, e.g., Hobbs, 2010), and 'digital citizens' require a much deeper understanding of online reputation management (Emler, 1990).

Facebook users, and indeed users of all online social media, may be unaware of the degree to which they reveal themselves in their online presentations (Back et al., 2010, Kosinski, Stillwell, and Graepel, 2013), and their perceptions of the 'image' projected by their Facebook productions may also be inaccurate (Barach et al, 2007). In light of these and other concerns, some have argued that we need to support individuals to become capable and thoughtful 'citizen archivists' (Cox, 2009). This gives rise to a new form of digital literacy: Papacharissi and Gibson (2011) identify the need for an "advanced form of digital literacy [that] can enable individuals to *redact* performances of the self online so as to navigate public and private boundaries fluently" (p. 76). Explorations of the history of 'personal media assemblages' can help us to identify some of the required skills (Good, 2012). Media literacy educators such as MediaSmarts (<http://mediasmarts.ca>) already include privacy issues in their media education materials; specific intervention with respect to reputation management skills and risks is both necessary and appropriate.

### *Tools for Content Management*

Our research documents that online social network participants rely on their ability to manage the online personae through tools such as deletion and delinking. While users should be aware that both social and organizational practices limit the effectiveness of these practices (see, e.g., Friedman (2000)), privacy expectations would be supported by tools that helped users to maintain this type of control over their information. Gelman (2009) suggests that users be provided with tools "to express and exercise privacy preferences over uploaded content" (p 1342). This tool would allow users to make 'granular' privacy decisions that would be communicated to others who access the information. The tool would provide "immediate visual feedback to third parties about the content owner's preferences and link to a website that provides more detailed guidance about how the content may be used or shared" (p 1342). She suggests that this tool should be couple with changes in the law that would allow for the enforcement of these expressed preferences.



Useful tools have to be simple, since online social network participants are unlikely to devote significant amounts of time to privacy management. The tools should also comport with the privacy strategies that users actually *employ*. In particular, online social network participants need tools that do a ‘good enough’ job of deleting content from profiles. Online social networks could, for example, be encouraged to develop tools that allow users to place ‘expiry dates’ on material (Backes et al., 2012). Such tools could heighten both the capacity for excising profile information, and the awareness that such choices are important. At the same time, it is important to limit the development and deployment of tools that allow the automated enhancement of online profiles. One prominent example is face recognition on Facebook: this development was met with outcry from Facebook users ([http://news.cnet.com/8301-1023\\_3-57468247-93/facebook-shuts-down-face.com-apis-klik-app/](http://news.cnet.com/8301-1023_3-57468247-93/facebook-shuts-down-face.com-apis-klik-app/)), and appropriately shut down by the company. Participants in online social networks want to be in control of their own presence, and they require an online environment that enhances, rather than undermines, that control.

### *Policy responses*

One of the most significant risks associated with online social network participation arises from the coupling of implicit or covert data collection coupled with powerful data mining techniques. Numerous studies have attested to the possibilities and associated risks of data reidentification (Zimmer, 2010). More recently, data mining has been used to infer personal characteristics that might not be explicitly revealed by social network participants (see Kosinski, Stillwell, and Graepel, 2013). These practices run exactly counter to the ‘what you see is what you get’ approach that participants use for online persona management, and the results contravene the expectation that participants in online social networks will control and limit their own online disclosures. The power of these analytic techniques increases with the amount of data available. Increasingly, social network participants are being offered opportunity for implicit sharing of personal information in the course of online activities such as ‘liking’. Although we have come to accept the use of such data for the purposes of targeted marketing, social inferences based on such information present an entirely new level of intrusion. Policy makers should understand that informational control is a central privacy consideration, and consent to the collection and use of discrete pieces of information (e.g., Facebook ‘likes’) should not be taken as consent to the aggregation and analysis of that information to infer undisclosed social facts.

A second issue is the ‘right to be forgotten’ included in the 2012 European Commission proposal for a data regulation. While there are difficult and potentially insurmountable challenges to implementing such a policy (see, for example, Rosen, 2007), this ability to delete online profile information is an important aspect of image or reputation control. It is particularly relevant given the increasingly long timeline of social network information, and the reality that changing values and life circumstances will alter what is considered to be appropriate self-disclosure. In particular, adolescents (who are increasingly participating in online social networks) now carry forward online representations of their younger selves as they move into adulthood. In many other circumstances, we protect young people from themselves by imposing an embargo on information about earlier actions (e.g., sealing juvenile court records). Thus, the right to be forgotten ‘has special relevance when the individual made data available while as a child’ (Costa and Pouillet, 2012, p. 257), and would allow the individual to demand that the controller of the data (e.g., the social network provider) delete that personal information which are no longer necessary for the purposes under which they were collected. In their relations with social network providers, participants should have the right to delete information from their online profile: this amounts to no more than reputation control, or a right to represent oneself as one chooses.

*Finally, a very personal note on ‘lessons learned’. I entered this research with the strong intuition that the ‘view from here’ expressed by social network participants would be very different from that assumed by outsiders. In particular, I fully expected that users would identify a strong sense of community with their online social network, accompanied by a clear distinction between ‘us’ and ‘them’, and clear social norms that ‘what is posted online stays online’. My close reading of these data, however, suggests to me that these intuitions were almost exactly wrong. In particular, I found nothing to suggest that young people are retreating to online social networks to live out the private and intimate parts of their lives: instead, to use a metaphor that dates me completely, going online (in a social network) is more like going to the mall than shutting the bedroom door. I’ve come to understand that online social profiles are public displays, and that everyone knows it. Obviously, however, there are privacy issues associated with the type of permanent online display constructed in an online social profile that don’t arise with ephemeral public performance: in your online profile, you can be watched in precise detail, watched repeatedly, watched retrospectively, and watched over an extended period. What worries me, then, is what doesn’t worry them: the vertical dimension of invisible privacy risks, borne of widespread data collection, data*

*aggregation, and analysis (Debatin, 2011). Paradoxically, it was comforting to think that the problem was one of preventing access to what participants considered to be private information. Instead, I find myself contemplating a much more challenging, and arguably more critical, first step: how do we make people aware of the invisible privacy risks they face?*

## References

- Abril, P.S. (2007), Recasting privacy torts in a spaceless world. *Harvard Journal of Law and Technology*, 21(1), 1-47.
- Altman, I. (1975) *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey, CA: Brooks/Cole Publishing Company.
- Arnett, J.J. (2000). Emerging adulthood: A theory of development from late teens through the twenties. *American Psychologist*, 55, 573-590.
- Back, M.D., Stopfer, J.M, Vazire, Z., Gaddis, S., Schmukle, S.C., Egloff, B., and Gosling, S.D. (2010). Facebook profiles reflect actual personality, not self-idealization. *Psychological Science*, 2(3), 372-374.
- Backes, J., Backes, M., Durmuth, M., Gerling, S., and Lorenz, S. (2012). X-Pire! – A digital expiration date for images in social networks. Available online at <http://arxiv.org/pdf/1112.2649v1.pdf>.
- Bachrach, Y., Kosinski, M., Graepel, T., Kohli, P., and Stillwell, D. (2012). Personality and patterns of Facebook usage. *WebSci'12 Proceedings of the 3<sup>rd</sup> Annual ACM Web Science Conference*, 24-32.
- Barash, V., Duchenaus, N., Isaacs, E., and Bellotti, V. (2007) Faceplant: impression (mis)management in Facebook status updates. In: *Proceedings of the Fourth International AAAI Conference on Weblogs and Social Media*. Palo Alto, CA: AAAI Press, pp. 207–210.
- Barnes, S.B. (2006). A privacy paradox: social networking in the United States. *First Monday*, 11(9), 4 September 2006, available online at <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. D. Buckingham (Ed.), *Youth, Identity, and Digital Media*, pp.119-142. The John D. and Catherine T. MacArthur Foundation Series in Digital Media and Learning, Cambridge, MA: The MIT Press.
- Buffardi, L.E., and Campbell, W.K. (2008). Narcissism and social networking web sites. *Personality and Social Psychology Bulletin*, 34(1), 1303-1314.

- Bumgarner, B.A. (2007). You have been poked: Exploring the uses and gratifications of Facebook among emerging adults. *First Monday*, 12(11), <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2026/1897>
- Carey, R. and Burkell, J. (2009). A heuristics approach to understanding privacy-protecting behaviors in digital social environments. In I. Kerr, V. Steeves and C. Lucock (eds.), *Lessons From the Identity Trail*, pp. 65-82. Oxford University Press, New York.
- Connolly, J., Furman, W., and Konarski, R. (2000). The roles of peers in the emergence of heterosexual romantic relationships in adolescence. *Child Development*, 17, 395-1408.
- Costa, L. and Poulet, Y. (2012). Privacy and the regulation of 2012. *Computer Law and Security Review*, 28(3), 254-262.
- Cox R.J. (2009) Digital curation and the citizen archivist. In: *Proceedings of DigCCur2009*. Available at: <http://sils.unc.edu/news/2009/DigCcurrConference>.
- Creswell, J. (1998). *Qualitative Inquiry and Research Design: Choosing Among Five Traditions*. Thousand Oaks, CA: Sage.
- Crocker, T.P. (2009). From privacy to liberty: The Fourth Amendment after Lawrence. *UCLA Law Review*, 1, 1-69.
- Debatin, B. (2011). Ethics, privacy, and self-restraint in social networking. In S. Trepte & L. Reinecke (Eds.) *Privacy Online: Perspectives on Privacy and Self-disclosure in the Social Web*. Heidelberg: Springer.
- Debatin, B., Lovejoy, J., Horn, A.K., and Hughes, B.N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15, 83-108.
- Dunne, A., Lawlor, M.-A., and Rowley, J. (2010). Young people's use of online social networking sites – a uses and gratifications perspective. *Journal of Research in Interactive Marketing*, 4(1), 46-58.
- Ellison, N.B., Steinfield, C., and Lampe, C. (2007). The benefits of Facebook “friends”: social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication*, 12(4), 1143-1168.

- Emler, N. (1990). A social psychology of reputation. *European Review of Social Psychology, 1(1)*, 171-193.
- Friedman, D. (2000). Privacy and technology. *Social Philosophy and Policy, 17(2)*, 186-192.
- Gelman, L.A. (2009). Privacy, free speech, and 'blurry-edged' social networks. *Boston College Law Review, 50(5)*, 1315-1344.
- Glaser, B.G. (1992). *Emergence vs. Forcing: Basics of Grounded Theory Analysis*. Mill Valley, CA: Sociology Press.
- Glaser, B.G., and Strauss, A. (1967). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago, IL: Aldine Publishing Co.
- Good, K.D. (2012). From scrapbook to Facebook: A history of personal media assemblage and archives. *New Media and Society*, published online 30 September 2012, available at <http://nms.sagepub.com/content/early/2012/09/24/1461444812458432>.
- Granovetter, M.S. (1973). The strength of weak ties. *American Journal of Sociology, 78(6)*, 1360-1380.
- Grimmelmann, J. (2009). Saving Facebook. *Iowa Law Review, 94*, 1139-1206.
- Gross, R., and Acquisti, A. (2005). Information revelation and privacy in online social networks. *Proceedings of the 2005 ACM workshop on Privacy in the Electronic Society*, 71-80.
- Häkkinilä, J. and 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 7<sup>th</sup> International Conference on Human Computer Interaction with Mobile Devices and Services*, 219-222.
- Hancock, J.T., Toma, C., and Ellison, N. (2007). The truth about lying in online dating profiles. *CHI 2007 Proceedings*, pp. 449-452, April 28-May 3, 2007, San Jose, CA, USA.
- Hoadley, C.M., Xu, H., Lee, J.J., and Rosson, M.B. (2009). Privacy as information access and illusory control: The case of the Facebook news feed privacy outcry. *Electronic commerce research and applications, 9(1)*, 50-60.

- Hobbs, R. (2010). Digital and media literacy: A plan of action. The Aspen Institute: Communications and Society .
- Joinson, S. (2008). Looking at, looking up or keeping up with people? Motives and uses of Facebook. *CHI'08 Proceedings of the twenty-sixth annual SIGCHI conference on Human Factors in Computing Systems* (pp 1027-1036). ACM: New York, NY.
- Kerr, O.S. (2010) Applying the Fourth Amendment to the Internet: A general approach. *Stanford Law Review*, 62, 1004-1049.
- Kim Y., Sohn, D., Sejung, M.C., (2011). Cultural differences in motivations for using social network sites: A comparative study of American and Korean college students. *Computers in Human Behavior*, 27(1), 365-372.
- Kosinski, M. , Stillwell, D., and Graepel, T. (2013). Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences of the United States of America*, early edition, available online at <http://www.pnas.org/content/early/2013/03/06/1218772110.short>.
- Lange, P (2008). Publicly private and privately public: Social networking and Youtube. *Journal of Computer-Mediated Communication*, 13, 361-380.
- LaRose, R., and Eastin, M.S. (2004). A social cognitive theory of internet uses and gratifications: Toward a new model of media attendance. *Journal of Broadcasting and Electronic Media*, 48(3), 358-377.
- Leary, M.R., and Kowalski, R.M. (1990). Impression management: A literature review and two-component model. *Psychological Bulletin*, 107(1), 34-47.
- Lee, DH. (2009). Mobile snapshots and public-private boundaries. *Knowledge, Technology and Policy*, 22(3), 161-171.
- Levin. A. ,and Abril, P.S (2009). Two notions of privacy online. *Vanderbilt Journal of Entertainment and Technology Law*, 11, 1001-0151.
- Lewis, J., and West, A. (2009). 'Friending': London-based undergraduates' experience of Facebook. *New Media and Society*, 11(7), 1209-1229.
- Livingstone, S. (2008). Taking risky opportunities in online content creation: teenagers use of social networking sites for intimacy, privacy, and self-expression. *New Media and Society*, 10(3), 393-411.

- Liu, Y., Gummadi, K.P., Krishnamurthy, B., and Mislove, A. (2011). Analyzing Facebook privacy settings: User expectations vs. reality. *IMC'11 Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement*, pp. 61-70.
- McCown, F., and Nelson, M.L. (2009). What happens when Facebook is gone? *JCDL'09*, June 15-19, 2009, Austin, Texas, USA.
- McKeown, Bruce and Dan Thomas. 1988. *Q methodology*. Newbury Park, Calif.: Sage.
- Montgomery, M.J. (2005). Psychosocial intimacy and identity: From early adolescence to emerging adulthood. *Journal of Adolescent Research*, 20, 346-374.
- Morse, J.M. (1994). Designing funded qualitative research. In K. Norman and Y.S. Lincoln (Eds.), *Handbook of Qualitative Research (2<sup>nd</sup> Edition)*, pp. 220-235. Thousand Oaks, CA: Sage.
- Nissenbaum, H.F. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford Law Books.
- Norberg, P.A., Horne, D.R., and Horne, D.A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviours. *Journal of Consumer Affairs*, 41(1), 100-126.
- Paparachissi, Z., and Gibson, P.L. (2011). Chapter 7: Fifteen minutes of privacy: Privacy, sociality and publicity on social network sites. In S. Trepte and L. Reineckie (Eds.), *Privacy Online*, pp. 75-90, Springer-Verlag: Berlin Heidelberg.
- Park, N., Kee, K., and Valenzuela, S. (2009). Being immersed in social networking environment: Facebook groups, uses and gratifications, and social outcomes. *CyberPsychology & Behavior*, 12(6), 729-733.
- Patchin, J.W., and Hinduja, S. (2010). Trends in online social networking: Adolescent use of Myspace over time. *New Media and Society*, 12(2), 197-216.
- Petronio, Sandra. *Boundaries of Privacy: Dialectics of Disclosure*. Albany, NY: State University of New York Press, 2002.
- PEW (2013). The demographics of social media users. Available online at [http://pewinternet.org/~media/Files/Reports/2013/PIP\\_SocialMediaUsers.pdf](http://pewinternet.org/~media/Files/Reports/2013/PIP_SocialMediaUsers.pdf), accessed February 21, 2013.
- Potter, W.J. (2012). *Media Literacy*. Sage Publications: Thousand Oaks, CA.



- Quan-Haase, A., and Young, A.L. (2010). Uses and gratifications of social media: A comparison of Facebook and instant messaging. *Bulletin of Science, Technology, and Society*, 30, 350-361.
- Rainie, L, Lenhart, A., & Smith, A. (2012, February 9). 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.
- Schwartz, B. (1968) The social psychology of privacy. *American Journal of Sociology*, 73(6), 741-752.
- Solove, Daniel J. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.
- SteinField, C., Ellison, N.B., and Lampe, C. (2008). Social capital, self-esteem, and use of online social network sites: A longitudinal analysis. *Journal of Developmental Psychology*, 29, 434-445.
- Stephenson, William. 1968. Perspectives in psychology: consciousness out—subjectivity in. *Psychological Record* 18 (1): 499–501.
- Stephenson, William. 1978. Concourse theory of communication. *Communication* 3: 21–40.
- Strahilevitz, L.J. (2004). A social networks theory of privacy. *John M. Olin Law and Economics Working Paper No. 230 (2D Series)*. The Law School. The University of Chicago.
- Strauss, A., and Corbin, J. (1990). *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Newbury Park, CA: Sage Publications.
- Thelwall, M, and 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.
- Tsjeng, Z. (2010). Facebook: Why we can't live without it. *Guardian.co.uk*, March 21, 2010, available online at

<http://www.guardian.co.uk/technology/2010/mar/21/facebook-cant-live-without-it>.

- Tufekci, Z. (2008). Grooming, gossip, Facebook and Myspace. *Information, Communication, and Society*, 11(4), 544-564.
- Utz., S, and Kramer, N.C. (2009). The privacy paradox on social network sites revisited: The role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 3(2), article 1.
- Viégas, F.B. (2005). Bloggers' expectations of privacy and accountability: An initial survey. *Journal of Computer-Mediated communication*, 10(3), Article 12. Available online at <http://jcmc.indiana.edu/vol10/issue3/viegas.html>.
- Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5 (1890): 193-220.
- Zimmer, M. (2010). "But the data is already public": on the ethics of research in Facebook. *Ethics and Information Technology*, 12, 313-325.

## Appendix 1: Interview and Focus Group Sample Topics

**NOTE that these topics are illustrative only. Specific discussions (focus group or interviews) were structured in response to issues that were raised by participants.**

### I. General perception of personal information and privacy

- **When you have information you want to share with friends, how do you do that? When you have information you want to share with family do you use the same methods?**
  - How might you share information online?
  - How might you share information offline?
  - How does the content of the message change how you share information?
    - Does context matter?
  
- **Are some things ‘private’ in some contexts and not in others?**
  - Online vs. Offline?
    - (e.g. Is there a difference between providing your postal code or phone number for a web site versus in a mall at a cashier till?)
  - Between online social networks?
    - (e.g. Is there something you would post on Facebook, but not on Twitter?)
  - Between work and social environments?
  
- **Do you feel the information that other people post about you or related to you should be private?**
  - e.g. How do you feel about being tagged in a photo on Facebook put up by someone else?
  - What if the photo is not of you, but someone/something related to you i.e. your child or your mother, your pet?
  - What if someone posts details about a party you attended on their wall?

## II. Managing personal or private information

*[Formerly: Privacy boundaries in social networking applications/Information seeking & sharing boundaries]*

### Managing information I present:

- **What kinds of information that you choose not to post or put online?**
  - Is there information you feel you **have** to post or keep online?
  - How 'open' is your profile?
    - Can you tell me a time when you were surprised about how much someone knew about you?
  - What kinds of stuff might you remove and when?
    - E.g. after you graduate and are looking for a job, would you remove it then?
  - Would you feel uncomfortable if someone Googled you?
- **Is there information you feel, because of your social group, that you *have* to put up online?**
  - What information can you post about other people?
- **If someone puts information in their social profile, is it OK for their contacts (or anyone) to share it with others?**
  - Do you need *permission* to share something?
  - Is it OK to take information to another context – e.g., offline?
  - Would it be OK for their contacts to share the information with THEIR friends who don't know the person who posted the information?
- **If you wanted a certain group of friends or people to know one thing but others not, how do you go about sharing something?**
  - If you were ill, and you wanted a group of your friends to know, how would you tell them?
  - If you were in a relationship, and you wanted some of your friends to know, how would you tell them?

### Managing Friend's lists: Who makes it onto your list and why?

- **Who is NOT on your friend's list? Why?**
  - Did they do something?
  - Do you consider the privacy of your information before accepting someone as a friend? Have you ever changed your privacy settings

when accepting a friend? Have you ever not accepted someone because of privacy concerns?

- Would they potentially get back onto your friends list?
- Have you kicked/taken someone off your friend's list? Why?
  - "What needs to happen to make you remove someone off your friends list?"
  - "Would you unsubscribe from their feed before un-friending them?" **[levels of removal]**

### **Managing information I consume:**

- **Have you ever lurked on someone else's account?**
  - When is it **not** OK to 'lurk'?
- **Do you consider all information available on Facebook public?**
  - What does that mean to you that the information is public?
  - Is there anything that you can't do with information you find out about people on Facebook whether you know them or not?
  - If all information is public then why do you keep a friend's list? What is the function of this?
    - Is a friend's list a way to keep information private?
      - [IF YES] Then if friend's lists are ways to keep information private, then is all information on Facebook public?
- **Have you searched online for information about someone?**
  - (e.g. a friend, friend of a friend, someone who you were dating, a future employer/employee)
  - Is it OK to look at the online profiles of people you don't know?
  - Did you feel uncomfortable searching for someone's information?
  - Have you been in a situation where you wanted to find something out and knew it was on someone else's page but you didn't have **direct access**... how do you go about finding it out?
- **If a friend asked you to get information from one of your Facebook friend's page, but who isn't their friend on Facebook, would you give it to them?**
  - What can they do with that information?
  - What information online (that you learn about someone you know) can you absolutely not tell others?

- **Have you ever been surprised about what you could find out about people online?**
  - Would you look in multiple locations to get more information?
  - Have you ever learned something about another person through their online profile that you thought you **shouldn't** know?

**Social network specific questions:**

- When you sign on to Facebook what are the first things you do?
- When you sign on to Twitter, what are the first things you do?
- What is the **worst** social network (Facebook, MSN, Twitter, YouTube) experience you've ever had?

## Appendix 2: Q Sample Statements

Q-Sample for Privacy expectations within social media				
	Facebook is a social space		Facebook is personal space	
1. Access	When I post something on Facebook, I am making a public announcement.		When I post something on Facebook, it is only intended for my “friends” list.	
	I would share my Facebook password with people I trust.		I would never share my Facebook password.	
	Information posted on Facebook is meant to be shared widely.		Information posted on Facebook is meant only for that person’s friends.	
	I can share information I find on Facebook with friends and acquaintances.		I keep information I find on Facebook to myself.	
	It’s ok to let my real world friends look at profiles through my Facebook account.		I wouldn’t share information by letting others look at profile through my Facebook account.	
2. Real or produced persona	Content posted on Facebook shouldn’t be boring.		Facebook is a good place to post everyday details about life.	
	Content posted on Facebook should be positive.		People can post good and bad stuff about themselves on Facebook.	
	I post pictures and information on Facebook that make me look good.		My Facebook profile represents my true self.	
	For me, Facebook is all about parties and having a good time with other people.		For me, Facebook is a place to post private thoughts and moments.	
	What I see on Facebook necessarily representative of real life.		What I see on Facebook reflects what’s going on in real life.	
3. Social norms	I can use information I find on Facebook in any way I want.		I shouldn’t use information I find on Facebook in a malicious way.	
	It’s ok to post any cool, fun content about friends on Facebook.		People should consider what their friends would want before posting content about them on Facebook.	
	It’s ok to tag others in photos or posts without checking with them first—they can always “untag” themselves.		People should check with others before tagging them in photos or posts.	
	If I’m uncomfortable with it, I can always “untag” myself from content		If I ask for content about me posted on Facebook to be removed, it	

	posted by others.		should be done.	
	Everyone should know that at a social event photos will be taken and posted on Facebook.		Before posting photos on Facebook, people should get permission from anyone who appears in them.	
4. Friends list	Main question:			
	It's important to me to have a large number of Facebook friends.		It is the quality not the quantity of Facebook friends that matters.	
	I need a good reason to refuse a friend request on Facebook.		I only accept people who are close to me in real life to be my Facebook friend.	
	Once someone is a Facebook friend, he or she is a Facebook for life.		Relationships change and sometimes a Facebook friend needs to be deleted.	
	I use Facebook friendships as a way to get to know new people.		People I friend on Facebook are people I already know.	
	I use Facebook as a way to connect with lots of new people outside my close circle of friends and family.		I use Facebook to keep in touch with friends and family.	
5. Privacy settings control	Other people can post the content they want about me on Facebook.		I should be the one to decide what is posted about me on Facebook.	
	Privacy settings limit people's ability to find out about each other.		Privacy settings are a good tool to manage personal information.	
	There are rules about what is ok (and what is not ok) to put on Facebook.		It's important to have agreements with friends about the type of information that can be posted on Facebook.	
	I don't post identifying information such as addresses, phone numbers and birthdays on Facebook.		I am fine with posting identifying information such as addresses, phone numbers and birthdays on Facebook.	
	If someone wants to keep something on Facebook "private", he or she should make sure people know about it.		Before talking about information posted by someone on Facebook, it is my job to find out how widely they want it shared.	
6. Lurking	I use Facebook to lurk friends' profiles.		Facebook is for connecting with people, not for lurking.	
	I regularly look at Facebook photo albums of people I don't know.		I only look at Facebook photos of people I know well.	
	I would ask others to help me view profiles I can't access.		I don't try to look at profiles that are closed to me.	
	Just because I look at others'		I look at someone's profile when I	



	profiles doesn't mean I want to friend them.		want to get to know him or her better.	
	Facebook is only one of many ways to find out more about someone.		Lurking outside of Facebook is creepy.	

## Appendix 3: Q Sort Factor Matrix with Defining Sorts

Factor Matrix (* indicates a defining sort)			
Q-sorts	Factor loadings		
	1	2	3
Q01	*0.6187	0.3041	0.1520
Q02	*0.6945	0.4818	0.0534
Q03	*0.6595	-0.1609	0.3683
Q04	*0.7632	0.0281	0.4217
Q05	*0.6694	0.1561	0.0694
Q06	0.2987	0.2422	*0.5890
Q07	0.3155	*0.5118	0.1924
Q08	0.0760	*0.5557	0.1792
Q09	0.5195	0.2622	0.2736
Q10	*0.7617	0.2886	0.2841
Q11	*0.5681	0.3242	0.3956
Q12	0.3132	0.2433	*0.5142
Q13	0.2913	*0.6974	0.1932
Q14	0.4725	*0.6342	0.3398
Q15	-0.0792	0.5410	*0.6145
Q16	*0.5238	0.4224	0.2791
Q17	0.0995	*0.8133	0.1050
Q18	0.2338	0.2313	*0.5178
Q19	0.4886	0.3055	*0.6054
Q21	0.1072	0.5277	0.4553
Q22	0.3442	0.5722	0.1924
Q23	0.3263	0.3794	*0.5544
Q24	*0.5706	0.0285	0.4581
Q25	*0.6898	0.1636	-0.0181
Q27	0.1282	0.3707	*0.5265
Q28	*0.5227	0.4936	0.0907
Q29	0.5238	0.4075	0.2048
Q30	0.2767	*0.7036	0.1410

Q31	0.3970	*0.5785	0.2077
Q32	0.3689	*0.4712	0.0750
Q33	*0.6951	0.3747	0.1125
Q34	*0.5347	0.3747	-0.0155
Q35	*0.5480	0.2995	0.2518
Q36	*0.5055	0.4142	0.1353
Q37	0.2287	-0.0203	*0.6512
Q38	-0.0826	-0.0113	*0.5210
Q39	*0.5714	0.3169	0.4085
Q40	0.2965	*0.6595	0.0510
Q41	0.1891	*0.4676	0.4187
Q43	*0.5249	0.4384	0.1985
Q99	*0.6699	0.3906	0.1516
Variance explained	22%	18%	12%

## Appendix 4: Consensus Statements

Consensus Statements with Q-Sort Value for Each Factor			
All statements are non-significant at $P > .01$ Those flagged with an * are also non-significant at $P > .05$			
Statements	Factors		
	1	2	3
I use Facebook friendships as a way to get to know new people.*	-1	-1	0
I would share my Facebook password with people I trust.	-4	-3	-3
Content posted on Facebook should be positive.*	-1	0	0
What I see on Facebook necessarily representative of real life.	-3	-4	-5
Content posted on Facebook shouldn't be boring.*	-2	-1	-1
If I'm uncomfortable with it, I can always "untag" myself from content posted by others.	2	4	2
People can post good and bad stuff about themselves on Facebook.*	0	0	0
Privacy settings limit people's ability to find out about each other.	-1	-1	0
For me, Facebook is all about parties and having a good time with other people.*	-2	-3	-4
It's important to me to have a large number of Facebook friends.*	-4	-5	-4
Lurking outside of Facebook is creepy.	1	2	0

## Appendix 5: Factor 1 Distinguishing Statements

Distinguishing Statements for Factor 1 with Q-Sort Value for Each Factor			
Statements for Factor 1 are significant at $P > .01$			
Statements	Factors		
	1	2	3
I should be the one to decide what is posted about me on Facebook.	4	0	1
Before posting photos on Facebook, people should get permission from anyone who appears in them.	4	-2	0
If someone wants to keep something on Facebook “private”, he or she should make sure people know about it.	3	1	-2
I don’t post identifying information such as addresses, phone numbers and birthdays on Facebook.	3	5	-2
I wouldn’t share information by letting others look at profile through my Facebook account.	2	-2	-2
People I friend on Facebook are people I already know.	2	4	4
There are rules about what is ok (and what is not ok) to put on Facebook.	1	3	1
Information posted on Facebook is meant to be shared widely.	1	-2	-1
Before talking about information posted by someone on Facebook, it is my job to find out how widely they want it shared.	0	-2	0
Just because I look at others’ profiles doesn’t mean I want to friend them.	0	3	3
Everyone should know that at a social event photos will be taken and posted on Facebook.	0	2	2
I keep information I find on Facebook to myself.	0	-2	-3
I only look at Facebook photos of people I know well.	0	-3	-2
I can share information I find on Facebook with friends and acquaintances.	-1	1	1
It’s ok to let my real world friends look at profiles through my Facebook account.	-2	1	2
I use Facebook to lurk friends’ profiles.	-2	0	0
My Facebook profile represents my true self.	-2	-4	1
Once someone is a Facebook friend, he or she is a Facebook for life.	-2	-3	-5
It’s ok to tag others in photos or posts without checking with them first—they can always “untag” themselves.	-3	1	-1
I can use information I find on Facebook in any way I want.	-3	-3	-2

Facebook is a good place to post everyday details about life	-4	-2	-2
I would ask others to help me view profiles I can't access. 42	-4	-2	0

## Appendix 6: Factor 2 Distinguishing Statements

Distinguishing Statements for Factor 2 with Q-Sort Value for Each Factor			
Statements for Factor 2 are significant at $P > .01$			
Statements	Factors		
	1	2	3
What I see on Facebook necessarily representative of real life.	4	5	2
I don't post identifying information such as addresses, phone numbers and birthdays on Facebook.	3	5	-2
There are rules about what is ok (and what is not ok) to put on Facebook.	1	3	-1
People should consider what their friends would want before posting content about them on Facebook.	4	2	4
It's ok to tag others in photos or posts without checking with them first—they can always "untag" themselves.	-3	1	-1
If someone wants to keep something on Facebook "private", he or she should make sure people know about it.	3	1	-2
I use Facebook as a way to connect with lots of new people outside my close circle of friends and family.	-1	1	0
Information posted on Facebook is meant to be shared widely.	-2	1	-4
I only accept people who are close to me in real life to be my Facebook friend.	0	0	1
I regularly look at Facebook photo albums of people I don't know.	-3	-1	-3
Other people can post the content they want about me on Facebook.	-5	-1	-4
People should check with others before tagging them in photos or posts.	2	-1	1
Facebook is for connecting with people, not for lurking.	2	-1	1
I keep information I find on Facebook to myself.	4	-2	-3
My Facebook profile represents my true self.	-2	-4	1
For me, Facebook is a place to post private thoughts and moments.	-5	-5	-5

## Appendix 7: Factor 3 Distinguishing Statements

Distinguishing Statements for Factor 3 with Q-Sort Value for Each Factor			
Statements for Factor 3 are significant at $P > .01$			
Statements	Factors		
	1	2	3
When I post something on Facebook, I am making a public announcement.	2	1	5
It is the quality not the quantity of Facebook friends that matters.	2	2	5
I use Facebook as a way to connect with lots of new people outside my close circle of friends and family.	1	2	4
Facebook is only one of many ways to find out more about someone.	1	2	4
I look at someone's profile when I want to get to know him or her better.	0	0	3
I would never share my Facebook password.	5	5	2
My Facebook profile represents my true self.	-2	-4	1
When I post something on Facebook, I am making a public announcement.	1	2	-1
It's ok to tag others in photos or posts without checking with them first—they can always "untag" themselves.	-3	1	-1
I am fine with posting identifying information such as addresses, phone numbers and birthdays on Facebook.	-5	-5	-1
There are rules about what is ok (and what is not ok) to put on Facebook.	1	3	-1
It's ok to post any cool, fun content about friends on Facebook.	-1	0	-2
I don't post identifying information such as addresses, phone numbers and birthdays on Facebook.	3	5	-2
If someone wants to keep something on Facebook "private", he or she should make sure people know about it.	3	1	-2
I keep information I find on Facebook to myself.	0	-2	-3
Other people can post the content they want about me on Facebook.	-5	-1	-4