Revisiting the Privacy Paradox on Social Media: An Analysis of Privacy Practices Associated with Facebook and Twitter

Mary Jane Kwok Choon
Université du Québec à Montréal

ABSTRACT

Background *Since the development of social media, social network sites (SNSs) such as Facebook and Twitter have been at the centre of privacy controversies and debates. Meanwhile, users continue to expose their personal information.*

Analysis *This ethnographic research examines 20 young adults' privacy practices and their relationship to privacy when they are using social network sites.*

Conclusions and implications *The privacy paradox is shaped by various factors, such as a limited knowledge of institutional surveillance practices, low visibility of these practices in context, a perception of control over the publication of information, and thin social trust. These findings provide empirical support for the application of the contextual integrity approach on social media and the development of a critical media education even at an adult age.*

Keywords *Social media; Privacy paradox; Self-exposure; Contextual integrity*

RÉSUMÉ

Contexte *Depuis le développement des medias sociaux, les réseaux socionumériques (RSN) tels que Facebook et Twitter ont été au centre des controverses et débats liés à la vie privée. Cependant, les usagers continuent d'exposer leur information personnelle.*

Analyse *Cette recherche ethnographique analyse les pratiques de la vie privée des jeunes adultes et leur rapport à la vie privée quand ils utilisent les réseaux socionumériques.*

Conclusions et implications *Le paradoxe de la vie privée est façonné par plusieurs facteurs tels qu'une connaissance restreinte des pratiques de surveillance institutionnelle, la faible visibilité de ces pratiques en contexte, une perception de contrôle sur l'information publiée en contexte et une faible confiance sociale. Ces résultats offrent un soutien empirique à l'application de l'approche de l'intégrité contextuelle sur les médias sociaux et une éducation critique aux médias même à un âge adulte.*

Mots clés *Médias sociaux; Surveillance; le paradoxe de la vie privée; l'exposition de soi; l'intégrité contextuelle*

Mary Jane Kwok Choon is a researcher at Université du Québec à Montréal. Email: kwok_choon .mary_jane@courrier.uqam.ca .

Canadian Journal of Communication Vol 43 (2018) 339–358 https://doi.org/10.22230/cjc.2018v43n2a3267

Introduction

With the development of social media,[1] which are surveillant in nature, privacy concerns arose among the public (Barnes, 2006; Hargittai & Marwick, 2016). Social network sites (SNSs) such as Facebook and Twitter have been at the centre of privacy controversies and debates. In 2010, the Office of the Privacy Commissioner of Canada filed a complaint against Facebook to have the SNS limit the use of information by application developers (OPC, 2016). In 2017, the Spanish data regulator fined Facebook as the SNS had infringed data protection laws; Facebook was accused of not informing users of the use and purpose of the collection of sensitive data (Lomas, 2017). In an earlier instance, hackers exposed users' passwords on Twitter (Cubrilovic, 2009).

Despite these concerns, the trend that has been observed is that users expose their personal information on SNSs (Brandimarte Acquisiti, & Loewenstein, 2012; Granjon & Denouël, 2011; Gross & Acquisiti, 2005). Exposure within these technological contexts is understood as the action of showing, exposing, rendering visible and at the same time of being exposed (Ball, 2009). Several media outlets published stories on social media users who lost their reputation and jobs because of their posts. For example, British trainee Kevin Colvin realized that showing too much on Facebook has negative consequences (see Randall & Richards, 2008). After giving a false reason for his absence to his employer, he went to a Halloween party and posted a photo of himself in a fairy costume on Facebook. One of his colleagues showed the picture to his supervisor and Kevin was promptly dismissed (see also Reid, 2011). In Canada, 80 students from various high schools and CEGEPs in Laval and Québec created a Facebook group in which they made death threats against their professors (see TVA Nouvelles, 2011). When a TVA Nouvelles reporter questioned students, "Do you think it's right that the police and teachers accessed this group?" They said that what they wrote on Facebook is "private." (TVA Nouvelles, 2011).

Young adults are the most present on social network sites compared to other cohorts of users in Québec (Cefrio, 2015, 2017). In 2016, 67 percent of users aged 25 to 44 years old use a social network site such as Facebook, Linkedln, Twitter or Snapchat (Cefrio, 2017, n = 1,001). There were 64 percent who used Facebook in the province compared to 57 percent in the rest of Canada (Cefrio, 2017). Québec young adults are often portrayed by media outlets as being unaware of the privacy risks associated with exposure online (Radio-Canada.ca, 2013; TVA Nouvelles, 2011). For example, an employer said that young people often used social network sites to share their "state of mind and that's an issue when they are searching for a job" (Radio-Canada.ca, 2013). Based on data collected from an ethnographic study, using methods of participant observation and 40 qualitative interviews, 20 Québec young adults' privacy practices and relationship to privacy when they were using Facebook and Twitter were examined. This research explains young adults' privacy protection strategies on both SNSs and the factors that shape the privacy paradox. The present study shows that users are unaware of the consequences of institutional surveillance practices on privacy, and that this relates to the fact that notice and consent are problematic on SNSs. These findings provide empirical support for the application of the contextual integrity approach on social media and the development of a critical media education even at an adult age.

Privacy practices on social network sites

Prior studies showed that social media users are to some extent unaware of privacy risks. For example, users are disclosing their real names on Facebook and are perceiving the benefits related to self-exposure rather than the risks associated with such practices (Gross & Acquisiti, 2005). Further, Brandimarte, Acquisiti, and Loewenstein (2012) argued that the more students think they have control over the publication of personal information in context, the less likely they are concerned about privacy risks and the more they reveal personal information on Facebook.

Other studies focused on the factors that shape self-exposure on SNSs. Tufekci (2008) conducted a survey of 704 students and discovered that 94.9 percent of them disclosed their real names on Facebook, while 62.8 percent did so on MySpace. Students alternated between self-exposure and control of information, because concealment of their information did not offer them a chance to attract the attention of their audiences. Boyd and Hargittai (2010) analyzed the practices of young adults from 2009 to 2010 on Facebook. Privacy settings changed during this period. They discovered that users with greater technical skills frequently changed their privacy settings. Other researchers found that the exhibitionism of French students on social media sites was part of a strategic process during which they controlled the visibility of their personal information and were searching for recognition (Granjon & Denouël, 2011). Ellison, Vitak, Steinfield, Gray, and Lampe (2011) analyzed how social media users balance between the sharing of personal information and the need to control disclosures. Users who activated privacy settings "reported higher perceived bonding and bridging social capital" (p. 26). Drawing from Putnam (2000, chap. 1, para. 23), bonding social capital is essential to strengthen reciprocal relationships and the development of solidarity. Bridging social capital is to provide access to other resources that cannot be obtained from close friends. It is an asset to succeed. Marwick and Boyd (2011) found that Twitter users negotiate their identities in order to brand themselves and be "authentic." Drawing from the work of Theresa M. Senft, they described this practice as micro-celebrity. Users alternate between self-exposure and self-censorship, as the site does not have the privacy settings to separate the different audiences.

Scholars have examined users' privacy concerns. Raynes-Goldie (2010) conducted an ethnographic study of the privacy practices of 20 Canadian users. Most of them were concerned about the control of personal information during social interactions (social privacy). According to the researcher, users care less about the use of personal information by institutions and third parties (institutional privacy). Boyd's (2008) ethnographic study of American teenagers shows that informants feared that authority figures such as parents, teachers, or college officers might access their personal information.

Barnes (2006) drew attention to the privacy paradox on social network sites. Teenagers knew the privacy risks linked to MySpace use, but they continued to expose themselves. Young and Quan Hasse (2013) revisited the privacy paradox. In their study, far from being naïve, Canadian university students developed various strategies to protect privacy during social interactions on Facebook. However, no strategies were mobilized to control the use of personal information by institutions and third parties. Hargittai and Marwick (2016) discovered that American users aged 19 to 35 are aware

that privacy is networked. Although they protect their privacy during interactions on social media, they know that other users and institutions can violate privacy. The privacy paradox is associated with online apathy.

While the literature explains the privacy practices of social media users, we lack a deeper understanding of users' relationship to privacy when they are using social network sites that have different architectures, terms of service, and privacy policies. Scholars have not examined the factors that shape this relationship. An improved understanding of privacy practices and users' relationship to privacy when they are using different social network sites will inform privacy debates and is important for the development of adequate policies that will reflect users' practices (Young & Quan-Hasse, 2013). As mentioned before, Canadians use several social media sites in everyday life (Cefrio, 2017; Insights West, 2016), and young adults are the most present on social network sites (Cefrio, 2010, 2014, 2017). In the news, techno-pessimistic discourses portray young adults' privacy practices on social media (Radio-Canada.ca, 2013; TVA Nouvelles, 2011). To address the gap in the literature, this study investigates how young adults in Québec are negotiating privacy when using Facebook and Twitter, and the factors shaping their relationship to privacy. It aims to answer the following two research questions:

> RQ 1: How do young adults negotiate privacy when they are using Facebook and Twitter?
>
> RQ 2: What are the factors that are shaping their relationship to privacy on social network sites?

Surveillance, visibility, and privacy

Social media are surveillant in nature, which has consequences on privacy (Trottier & Lyon, 2012). Institutional surveillance practices are becoming more and more decentralized and networked (Lyon, 2002). In the context of Internet surveillance, Stalder (2011) identified two types of practices: back-end and front-end. In the first case, back-end surveillance is supported by servers and databases that are accessible only to website owners. Data collected by website owners and stored in databases, is used to serve commercial and other purposes and to model interfaces that are more or less easy to use. Front-end surveillance is the monitoring of users' activities online, in order to generate contents (data, metadata) with the help of algorithms, and provide opportunities to users through these interfaces. Surveillance practices may be visible, invisible, or have a low visibility during social interactions (Ball, 2009; Marx, 2006). For Brighenti (2010), different forms of visibility are imposed and negotiated through architectures that promote the exercise of surveillance. Within this framework, social control is exercised through website architectures that promote the visibility of personal information. Visibility as control is in tension with the forms of visibility that users negotiate to obtain recognition (visibility as recognition). The rules of visibility that are applied to personal information will vary depending on the architectures of the websites, their terms of service (TOS), and their privacy policies. Website owners offer a contract that users have to either opt out of or opt into. As Nissenbaum (2011) explained, "The gist of this approach is to inform website visitors and users of online goods and services of

respective information-flow practices and to provide a choice either to engage or disengage." (p. 34). The contract is presented in the form of notice and consent (choice) (Nissenbaum, 2011). Some rules of visibility may change, to the detriment of users' privacy (Trottier & Lyon, 2012). For example, website owners might add default settings to interfaces without users' consent. Therefore, unanticipated forms of visibility provide access to personal information to different audiences, and this may contribute to privacy violations.

Privacy can refer to "freedom of thought, control over one's body, solitude in one's home, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations" (Solove, 2008). Privacy is a "slippery concept … encompassing a variety of meanings" (Viseu, Clement, & Aspinall, 2003, p. 1). The control approach has often been used to address privacy in relation to technological and communication contexts. Westin (2003) defined privacy as the right of individuals to determine how their personal information can be communicated to others. However, the boundaries between the "public" and the "private" are rather fluid, and vary depending on situation or context (Marx 2001). Therefore, context is important when we are framing privacy. Nissenbaum's (2011) contextual integrity approach considers that privacy is contextual and that contexts are governed by informational norms—mainly norms of appropriateness and distribution. Norms of appropriateness indicate what is appropriate behaviour in a given context, and norms of distribution refer to the distribution of information. A violation of informational norms can contribute to a violation of privacy and a lost of integrity of personal information. Davis and Jurgenson (2014) used the work of Nissenbaum to explain how SNSs are causing collisions and collusions of contexts. The first type of collision happens when SNSs' architectures allow information to seep from one context to the other without users' consent (e.g., when privacy settings are by default public). Collusion of contexts occurs when an individual contributes to the seeping of information from one context to the other (e.g., users' personal information being exposed by colleagues on Facebook). Social surveillance is also practised between peers within SNSs during interactions and can contribute to an invasion of privacy (Marwick, 2012). On SNSs, privacy can also be violated by a third party. Etzioni (2015) identifies this process as privacy violation triangulation.

Privacy is also networked, as Hargittai and Marwick (2016) explained: "Privacy is not an individual process, but rather a collective effort that requires the cooperation of those with whom we connect on social media, as well as the technological affordances of the social media sites themselves" (p. 3752). In context, privacy is negotiated by individuals during social interactions. Goffman's (1973) contributions prove useful and are associated with the performativity of privacy (Donath, 2007; Marwick & Boyd, 2011). Users will negotiate the boundaries between the "private" and the "public" according to the audiences present and thus proceed to the segregation of audiences. Self-exposure can be voluntary and involuntary and shaped by various factors, as discussed earlier, including social capital benefits, perception of control over the publication of information, mimesis of micro-celebrity practices, and internalization of social control (Brandimarte et al., 2012; Ellison et al., 2011; Proulx & Kwok Choon, 2011). Some privacy protection strategies of users on SNSs are deleting comments on their Facebook

profile and contacts from the friends list, using social steganography (which is the art of concealing information to a specific audience), practising self-censorship on Twitter, restricting Facebook profiles, and sending private messages on Facebook chat (Boyd, 2010; Marwick & Boyd, 2011; Raynes-Goldie, 2010). Privacy negotiation is also a dialectical process. Individuals will try to have control over information they are sharing and information that comes from others to achieve an optimal level of privacy. They also want to match the achieved privacy with the desired one (Altman, 1975; Tufekci, 2008).

Methods

From January 2013 to October 2015, this author conducted a virtual ethnographic research study of Québec young adults' privacy practices.[2] Most young adults in Québec who use SNSs are students (Cefrio, 2012, 2014). After obtaining the certificate of ethical acceptability of research on human subjects from my institution, I sent out a call for participation to students enrolled in a bachelor's degree program at a university in Montréal by email, a mean of communication frequently used by students to check updates on their study programs. Recruitment criteria were based on age (18- to 34-years old) and use of Facebook and Twitter. Upon obtaining users' consent, I became Facebook friends with study participants and started following informants' Twitter accounts. To grasp the online culture (practices, norms, and values), I approached the Internet as a space where culture is formed and reformed and is embedded in everyday life (Hine, 2008). Therefore, online and offline research methods, such as participant observation, and qualitative open-ended and semi-structured interviews were employed. I observed the online culture and participated in users' activities in order to get a sense of what they are doing and sharing in this context.[3]

Qualitative interviews proved to be an efficient way to understand online practices from the point of views of young adults (Spradley, 1979). Open-ended and semi-structured interviews of 90 minutes were conducted in an offline context with a total of 20 young adults. The goal was not to have a representative sample of social media users but rather to understand the privacy practices of this small group of users and infer privacy patterns. The data saturation criterion was also taken into consideration. The open-ended one-on-one interviews consisted of an open discussion in front of the computer, with the question: Can you show me what you do on Facebook and Twitter? The participant and researcher together explored profile pages to grasp uses of both SNSs. Further, the motivations for self-exposure and privacy protection strategies were discussed. The terms of service (TOS) and privacy policy pages of both SNSs were also visited. Informants explained the privacy choices they had made for each SNS.

Data collected during the first interview was used to construct the grid for the semi-structured interview. To understand informants' relationship to privacy, what users think of privacy policies, TOS, advertising and applications, the circulation of information on SNSs, control over personal information, reputation of SNSs in terms of privacy protection, friendship on SNSs, and the difference between online and offline privacy were further explored. The aim was to encourage users to reflect on privacy related to SNSs. Rather than bringing up the relationship between surveillance and privacy during discussions, informants gave their own impressions on surveillance. The 40 interviews were audio-recorded and transcribed on separate sheets. Interview

questions were grouped by topic. Users' answers for each question were thoroughly read, and quotations relevant to the two research questions were highlighted and compared with interview data. Both concepts and main themes were identified. Informal conversations with research participants were conducted via Facebook Chat to elucidate the meaning of interview data and observed phenomena. To protect users' anonymity, pseudonyms are used throughout the text. Users' identity on Facebook posts were blurred using PDF tools.

Results

The following three sections provide the main findings of this research on the following themes: self-exposure and the desire for recognition; privacy protection strategies; and the privacy paradox.

Self-exposure and the desire for recognition

Self-exposure in the context of Facebook and Twitter uses is related to visibility as recognition. Participants had joined Facebook in 2007 and had restricted their profiles to friends only. Their social network was composed of close friends, family members, and acquaintances (see Table 1). During social interactions, young adults in this study exposed several types of personal information on Facebook, such as selfies, photos showing users' participation in social activities, geolocation information, inside jokes, and online articles, as well as identification information, such as a profile picture, their actual name, university, employer, and city of residence or birth. In addition, within Facebook groups, they disclosed information related to academic group work. Users employed the following promotional strategies: 1) adding filters to selfies on Instagram before publishing them on Facebook and identifying peers and specific locations as a way to showcase their social life; 2) sharing articles and giving importance to societal issues; 3) sharing inside jokes in order to maintain strong ties. Users projected advantageous physical attributes, expressed positive emotions, and showed critical thinking skills on Facebook.

Table 1: Participants' social media statistics

Participants	Number of followees onTwitter	Number of followers onTwitter	Number of Facebook Friends
Corinne	121	28	338
Elissa	212	28	350
Giliane	139	41	116
Illona	816	1616	580
Joey	14	27	600
Karine	11	9	445
Lana	135	30	328
Léa	120	59	588
Liloo	16	3	476
Lily	270	33	550
Lovna	223	98	545
Ludovic	190	29	438
Maurice	80	8	566
Mira	644	70	448
Molly	226	41	326
Noemie	339	53	431
Romeo	94	27	122
Sebastian	600	150	330
Romeo	94	27	122
Tara	502	28	56

Recognition is obtained during interactions and is mediated by the architecture of visibility. For example, Sheila shared a photo on Tara's birthday on her profile (see Figure 1). She tagged four friends and therefore made visible their identities and location. Reciprocity is reflected in the mutual appreciation of comments and users' physical appearance and the systematic use of smileys. The number of "likes" and comments represents a form of recognition from online communities. Personal recognition is obtained during social interactions between friends and acquaintances (Brighenti, 2010). It allows users to get emotional benefits and maintain strong and weak ties. Further, informants activate the geolocation feature to showcase their social life and to obtain "likes." Illona explained:

> I just geotag when it's something fun: a show, for example. I went to New York, I tagged it. You want to show people something about your life. When you go to Cancun. You want everybody to know that you're in Cancun, so the world knows you have a social life! (Personal interview, July 4, 2013)

In comparison, users have a public account on Twitter. Most users joined the social network in 2012 to follow the trend. Their followers, tweets, retweets, and conversations revolve around personal interests and tastes, such as pop culture, politics, Québec culture, international news, entertainment, culinary specialties, sport, and everyday situ-

Figure 1: Sheila's Facebook post

Figure 2: Illona's tweet

Note: Translated from French: "It was long before the release of the second album of @LessoeursBoulay, but it was worth the wait Sweet Jesus, it's good!"

Figure 3: Elissa's tweet

Note: Translated from French: "Very beautiful show of SUUNS. Thank you."

Figure 4: Sebastien's tweet

Note: Translated from French: "No sugar in the sugar jar, I have to put asparthame in my coffee. How can people drink that?!! #negativeemotion."

ations. Informants engage in micro-celebrity practices (see Marwick & Boyd, 2011, for a definition of tweet, retweet, followers, and followees). Self-branding is achieved by initiating conversations, tweeting and retweeting during specific events, and sharing daily situations and emotions on Twitter (see Figures 2, 3, and 4). The aim is to be visible in the Twitter sphere, attract attention, and obtain recognition from celebrities and strangers.

According to Marwick and Boyd (2011), "the ability to attract and retain attention are marks of one's status" (p. 127) in the Twittersphere. Visibility as recognition on Twitter occurs between strangers during the routine categorization of individuals (Brighenti, 2010). The fact that their tweets are retweeted or favourited, and the feedback that they generate as well as an increase in followers represent the recognition users obtain from strangers. For example, Mira shared her positive and negative emotions and celebrity tweets:

> I retweet about Place des Arts events, I find it cool. I advertise a little bit. People will see that Place des Arts is following me on Twitter. It's a form of prestige. It's fun when they reply to you. I feel a little bit important. Even Danny Turcotte, he jokes a lot, sometimes I will share crosswords on Twitter, and he will retweet me. (Personal interview, July 3, 2013)

On Twitter, users judge each other according to their interests, tastes, and tweet topics. They do not know each other and are not judged on their singularities. Visibility as recognition allows users to maintain "virtual" ties.

Privacy protection strategies

From social steganography to a restricted profile

The desire to expose oneself is linked to the need to protect one's privacy (Altman, 1975). Users of social network sites mobilize strategies to protect privacy during social interactions and to conceal information from a specific audience. Strategies on Facebook for social steganography include deleting contacts from their friends' lists and sharing private information through Facebook Chat. Informants said:

> "I am giving up Pippa, you are the devil!" [she reads]. This is an inside joke. Pippa my friend, is encouraging me to post information on Facebook as I told her that I am leaving the site for a while. (Noemie, personal communication, February 2, 2014)

> I am doing a little bit of "cleaning up." I am deleting friends from my list. I no longer know them, therefore I am not interested in what they are doing. I don't want them to see what I am doing either. (Corinne, personal interview, March 21, 2013)

> My friend is depressed and she expresses her negative emotions all the time on Facebook. People do not like it, to have people sad all the time.

> As I do not want to disturb my Facebook friends, I will not do that. I will try to make my Facebook page more joyful. There is a boundary that I built. I will rather call someone or express myself on the Facebook Chat. (Elissa, personal interview, June 17, 2013)

Another strategy to protect privacy is self-censorship. Informants do not disclose "trash" and nude photos on Facebook. If they are "identified" on this type of photo, they will remove these "identifications" by making use of the appropriate settings. They also do not activate the geolocation feature when they are at home, at their friends' place, and at the doctor's office. From their point of view, employers are watching over Facebook profiles. Ludovic said:

> I post pictures of me partying, but I am not throwing up on the floor and I am not showing my belly on the roof. I am having fun. It takes a crazy employer to stalk me on Facebook and see how I am partying. It is a certain fear. I say to myself that an employer can have different political views than I have and may not want me on his team. (Personal interview, July 6, 2013)

For Goffman (1973) self-censorship is a strategy that an individual will employ to hide some facts to an audience: "[A]lthough in certain representations, and even in certain particular roles, when the actor is in a position to have nothing to hide, there is usually something that he cannot openly address in all his activities" (p. 66). Self-censorship is the only privacy strategy on Twitter. From users' perspective, audiences on Twitter will not be interested in photos taken at social events. In addition, the geolocation feature is not activated on Twitter. Users fear being stalked by strangers. Illona explained why she did not activate the geolocation feature on Twitter:

> That's not interesting. There are more people I do not know and it's a little creepy. Let's say I am at home, and someone knows where I live, and I do not know him. If I have never seen him in my life. On Facebook, I had at least an interaction with them. On Twitter, people everywhere follow me. (Personal interview, July 4, 2013)

This strategy of self-censorship is employed when users think that they lack control over personal information (Hargittai & Marwick, 2016).

Facebook profiles restricted to friends only

Another strategy is having a Facebook account restricted to friends only. The participants in this study did not read the privacy policy section of the SNS, since Facebook incorporated some changes with the implementation of the Timeline. They did not see notices of changes in context. During the interview, young adults found the discourses that explained privacy policies incomprehensible. Users were concerned because personal information that they thought was restricted to Facebook friends was by default accessible to a greater audience. Profiles were listed by external search engines by default, profile photos were visible to everyone, and applications had access to personal information without their consent. Young adults experienced collisions of context (Davis & Jurgenson, 2014). During the interview, users all activated the adequate settings. From their point of view, website owners have something to hide and

are concealing to users the extent to which personal information is subjected to an invisible audience. Informants explained:

> I know that at one point they changed their options, but it was written in the little corner in a small window. Of course, most people will move on. You're not going to read—you look at it one by one, it's long. Then how it's done. It's like thirty lines for not much. You could have a window written: "Do I want to make all my information public or private?" That's it! Sure they want to make it more complicated than it should be there. (Sebastian, personal interview, March 18, 2013)

> Two hundred and ninety-three applications, I do not know why they are there. No, I do not know them [she reads the application settings]. Sometimes I think Facebook makes it by default, if you do not see, it puts it automatically like that. (Lily, personal interview, March 5, 2013)

In addition, participants had heard in the media, in the classroom, and from their friends that Facebook was endangering privacy. Giliane said:

> In terms of privacy, it's zero. You can just hope that what you put on your Facebook, it will not come back to you. Its reputation is not very good in relation to privacy. It is public as everything can seep out. I keep it in mind. It's not like your house, it's really something that's open to everyone. If someone wants to "break into" your account, the information can come out. (Personal interview, July 8, 2013)

Informants think that it is easier to negotiate privacy within offline contexts than online. Boundaries are porous online and information can seep from one context to the other. Users perceived that Facebook architecture mediates social surveillance practices, and this can contribute to a loss of control over privacy (Marwick, 2012).

The privacy paradox

These results suggest that privacy on SNSs is important for the protection of reputation and is a way of protecting oneself against social surveillance. On Facebook, users expect to have control over personal information, though they are aware of some privacy risks. Privacy violations on Facebook can contribute to a loss of reputation that could be detrimental to their career. In comparison, publicity is more important than privacy on Twitter. Privacy is to a certain extent valued but is not a priority. The privacy paradox is shaped by a limited knowledge of institutional surveillance practices, the low visibility of institutional surveillance practices in context, the perception of control over the publication of information in context, and thin social trust in Facebook friends.

A limited knowledge of institutional surveillance practices

The knowledge of users in this study on institutional surveillance practices and social surveillance was limited and vague. The idea that "somebody somewhere can have access to their personal information" was omnipresent. Noemie explained:

> From the moment that you post something on Facebook or Twitter, it does not belong to you. Someone, somewhere will have access to it. You have

> to be cautious. Doing screen shots of pictures, sharing it in another context, or modifying it is easy. (Personal interview, June 12, 2013)

The collection of personal information for SNS advertising systems and the collection of personal information by third parties are not considered as a privacy threat but as an exploitation of personal information. Some participants somewhat naively thought that they had opted out of the Facebook advertising system with AdBlock. The software is used as a spam blocker. As Ludovic remarked:

> What's strange is that Facebook is free but you have the ads. But then I removed the advertisements. You know AdBlock on Google Chrome, I put AdBlock and I no longer see the ads. Facebook is free with no ads [laughs]. We circumvent the system and they will realize that everyone has AdBlock. (Personal interview, March 6, 2013)

Maurice is the only one who mentioned that federal agencies are monitoring social media. Young adults were not aware that their Twitter profiles are listed by search engines external to the site and that they gave their consent to Twitter to collect their personal information on third-party sites. This information circulated on the Twitter user feed, but informants did not see it. They also had never read the privacy policy section on Twitter. To the question "Who can see your personal information on Twitter?" Users said:

> Everyone. My followers and those who are in the groups with the hashtags … (Ludovic, personal interview, March 6, 2013)

> My followers, and the people who come to see my page, if there are … (Elissa, personal interview, March 5, 2013)

It should also be noted that at the time of this study, users were familiarizing themselves with Twitter and did not understand the flow of information on the SNS. The more knowledge users have about surveillance practices, the more they will develop a critical attitude toward privacy. Marx (2006) explained the relationship between knowledge, our ability to understand, and our ability to undertake reflective actions as follows:

> Even when we have one or two pieces of information, this may be revealing when there is general cultural knowledge. Here, visibility does not refer to what we see concretely, but what we know (or we discover) as participants in a culture. The success of Sherlock Holmes, for example, rests in part on his ability to deduce relevant facts from his vast knowledge of culture and society. He frequently used his general knowledge to understand and locate a culprit. (p. 103)

Users' limited knowledge of institutional surveillance practices in the context of SNSs explains why users in this study were still engaging in self-exposure. Informants did not expect to have control over the use of their personal information by institutions and third parties, and they did not mention the threats related to privacy violation by triangulation.

Low visibility of institutional surveillance practices in context

The low visibility of institutional surveillance practices in context, such as low-profile

notices of architectural changes, shapes this paradoxical relationship to privacy. Social control is exercised on SNSs (Proulx & Kwok Choon, 2011). For website owners, the aggregation and use of data for commercial purposes is more important than users' privacy, and this could explain the opacity that surrounds notice and consent in the context of use (Nissenbaum, 2011). The lack of clarity surrounding privacy policies marginalizes the reflexivity of individuals to a certain extent in relation to privacy, as they may be unaware of architectural changes. This, in turn, can lead to involuntary exposure of personal information. Ball (2009) explains the relationship between self-exposure, surveillance, and visibility mechanisms in those terms:

> Technical seeing now means that invisible realities, and that which is deliberately hidden or secret can become available to view without our knowledge. Windows on the world become windows on the individual, and the individual is not guaranteed to realize they are on display. (p. 644)

While surveillance practices appear less visible and distant, their impact on privacy seems abstract. For Viseu, Clement, and Aspinall (2003), the endangerment of privacy has an abstract and distant character on a daily basis. Privacy becomes valuable when there is an invasion. For example, users in this study changed their privacy settings to make Facebook profiles more "private" when they experienced collisions of context. Once this action was taken, they felt that they had more control over the publication of information.

The perception of control over the publication of information in context

Young adults in this study expressed different perceptions of privacy in relation to Facebook at three distinct moments. Before exploring the privacy policies section on Facebook, users were confident about the state of protection of their profiles. The moment they realized their personal information was exposed by default to an extended audience, they were concerned and activated the adequate settings. During the second interview, they highlighted several risks related to social surveillance and said that nothing was "totally private" on the internet. They were still worried about their privacy, because the idea that personal information was visible to strangers was always present. However, users confirmed that they trusted Facebook privacy settings. Informants thought they had control over the publication of information in context. The more individuals perceive that they have control over the information published in context, the more they are likely to continue to expose themselves (Brandimarte et al., 2012).

In comparison to Facebook, young adults in this study thought that Twitter had a better reputation in terms of privacy. Users explained:

> People do not really talk about privacy on Twitter. The "discourses" are more about Facebook than Twitter. (Giliane, personal interview, July 8, 2013)

> I did not hear anything about it. But, really, I think it's more protected than Facebook because your tweet, you can block it, and you can even erase it. Maybe Facebook already has a well-established bad reputation that it's not protected. (Illona, personal interview, July 4, 2013)

Users perceived that a desired level of privacy had been achieved on both sites. From the perspective of informants, the networked nature of privacy on SNSs is in their propensity to introduce all sorts of invisible audiences (Boyd, 2008; Hargittai & Marwick, 2016).

Thin social trust in Facebook friends

Another factor that shapes the privacy paradox is the trust young adults place in their Facebook friends. The more people trust, the more inclined they are to disclose information. Social trust is an important component of SNS interactions. For Putnam (2000), social trust is defined as trust placed in individuals and not in institutions. In his analysis of Americans' sociability during the twentieth century, he was interested in two forms of trust: thick trust and thin trust. The first is the one we place in our personal circles, usually composed of close friends, relatives, and family. The second concerns other acquaintances. He noted a decline in trust in the 1960s that was shaped by individuals' perceptions of strangers, built through their social experiences and shaped by psychological traits (paranoia, cynicism, etc.). However, for a more recent period, Putnam (2000) found that thin trust has begun to develop with the internet and the emergence of small groups whose activities include, for example, reading or fighting alcoholism (Alcoholics Anonymous). Individuals are grouped around interests or common values without really knowing each other. Most informants claimed that they trust their social networks. For example, Noemie compared her Facebook profile with a closet:

> Facebook, when I post something, I feel more like I'm with my circle away in, for example, a closet, and I will say, "I painted my baby's room today." In the closet a person can have a recorder and a camera, but I trust the people in the closet. (Personal interview, June 12, 2013)

It is a form of thin social trust that young adults place in their social networks. As Donath (2007) said, "SNSs can actually increase trustworthiness, by placing people within a context that can enforce social mores" (p. 236). Moreover, Putnam (2000, chap. 8, para. 15) remarked that having or not having trust in individuals is linked to social experiences. Only two informants experienced collusion of contexts on Facebook. Therefore, most young adults in this study believed in the trustworthiness of their contacts.

Implications for privacy debates

The problem with notice and consent (choice)

Findings from this study show that once users achieve the desired level of privacy, they do not show an interest in privacy policies again. Young adults have to experience a privacy violation in order to pay attention to these policies. Informants trusted SNSs to a certain extent. At the same time, a form of opacity surrounds notice and consent.

Users recognized that privacy policies should be more clear, visible in the context of use, and easily accessible. There are existing tensions between visibility as control and visibility as recognition, which show that it is difficult for users to manage privacy on social media. Findings indicate that there is a need for more transparency in privacy policies

and the development of adequate contextual parameters. According to Etzioni (2015), increasing transparency in institutional surveillance processes can be a means of informing the public about issues related to the collection of personal information.[4] Hence, different measures could be adopted to revise notice and privacy policy language:

1. Developing visible contextual parameters to inform users of architectural changes. For example, notices of architectural changes could be integrated in the News Feed and Mini Feed on Facebook.
2. Reducing the path that users must take to access privacy settings. For example, to opt in and opt out of the use of personal information by advertisers, a user must leave the Facebook site and visit the Digital Alliance Advertising site and read a series of terms of service before being able to opt out. That user must check that third parties are not added to the Facebook advertisers list. On Twitter, the information associated with public accounts and protected tweets is accessible on the privacy policy section page only after a user clicks on the "to know more" and "protect my tweets" tabs.
3. Revising the discourses related to privacy policies. They are lengthy and written in legal jargon. There is also a translation problem. Privacy policies have been translated literally from English to French, which shapes their understanding by francophone users.

The promotion of transparency in SNS contexts could foster informed consent, but does not guarantee privacy protection. As Nissenbaum (2011) argued, notice and consent is problematic as new third parties such as advertisers or data mining companies are added to the list of actors that have access to personal information. Young adults in this study were concerned that access to personal information had been granted to several application owners on Facebook. Therefore, website owners should try to adopt the contextual integrity approach (Nissenbaum, 2011). The objective is to understand users' privacy expectations and articulate those expectations with context-based rules. Such an action could, in the words of Nissembaum (2011), "buttress informed consent" (p. 45). The fact that young adults activated the adequate privacy settings on Facebook after realizing that personal information was accessible to third parties and invisible audiences indicates that they expect personal information to stay in the context of use. Thus, context-specific informational norms being advertised by website owners through privacy policies and TOS need to be clarified, and users should be notified appropriately when changes occur in the flow of information.

The need for critical media education

The privacy paradox shows that users internalize social control while being aware of some risks associated with social surveillance practices. Informants did not seem concerned about the use of personal information by institutions and third parties, because they had a limited knowledge of the risks linked to institutional surveillance practices. The existing relationship between surveillance and privacy was vague for these individuals. So, can a critical media education foster this type of knowledge?

In Québec, media education is integrated into the school curriculum at an early age. Its aim is to "lead students to demonstrate a critical, ethical and aesthetic sense

towards the media and to produce media documents respecting individual and collective rights of groups" (MEES, 2015). The main objective is to develop a critical sense among high school students by providing them with tools to understand both the benefits and the risks associated with their media uses. There is a focus in the media education curriculum on "privacy and reputation." However, it would be pertinent to develop a teaching module on "knowledge of surveillance practices" and underline the importance of privacy and accountability.

Steeves (2010) recognized the importance for teenagers and children to develop a critical attitude toward privacy. Considering the speed at which the architectures of social network sites are changing, young adults should also receive a critical media education, as what they learned about SNSs when they were teenagers is obsolete. It would also be relevant to teach obfuscation techniques to show students the mechanisms associated with institutional surveillance practices and how to protect their personal information. Brunton and Nissenbaum (2015) define obfuscation as "the deliberate addition of ambiguous, confusing or misleading information to interfere with surveillance and data" (p. 1). Knowing these techniques would allow users to maintain a balance between disclosure and concealment of information. For example, the software Facecloak enables Facebook users to make their identification information visible to a small circle of friends by encrypting them and saving them on a different server than Facebook. Facecloak is one way to make information ambiguous and protect oneself from institutional and social surveillance. Using these techniques can contribute to a better protection of privacy and a greater autonomy of action. As Marx (2015) has written, "Subjecting surveillance and privacy-hungry technologies to critical analysis and making them more visible and understandable hardly guarantees a just and accountable society, but it is surely a necessary condition for one" (p. 126).

Conclusion

This ethnographic research of social media users' privacy practices shows the complex relationships between surveillance, visibility, and privacy. These results are contextual and are related to this small group of users, who are university students. Users' privacy practices did not change after the interviews. It is necessary to further analyze how different groups of Canadian young adults understand privacy as a concept, for it can be defined in multiple ways. It is also relevant to grasp users' knowledge of privacy laws to understand their level of privacy awareness. The privacy paradox cannot be defined only in terms of users taking risky opportunities, while being aware of some privacy risks. It is shaped by various factors. Young Canadian users seem less aware of the risks associated with the collection and use of personal information by institutions and third parties than American users (Hargittai & Marwick, 2016; Raynes-Goldie, 2010; Young & Quan-Hasse, 2013). In the USA, Facebook gained popularity among the population in 2004 (Boyd, 2008), and Twitter was launched in 2006. In Canada, it was between 2009 and 2012 that a growing number of users joined Facebook and Twitter (Cefrio, 2010, 2014). Informants started familiarizing themselves with SNSs and privacy policies during this period and are still trying to grasp the flow of information on these online spaces. This flow is complicated due to architectural changes, the fact that users are uninformed about institutional surveillance practices, and the

opacity surrounding notice and consent undermine privacy protection during social interactions.

Findings show empirical support for the application of the contextual integrity approach on social media. The way that TOS and privacy policies are presented on SNSs and the frequent changes in the flow of information raise several questions on the nature and value of notice and consent and its propensity to provide the adequate tools for privacy protection. Future research needs to explore what social media users consider as adequate notice and informed consent, and how they engage with different privacy policies and TOS across several social media platforms. Further, as Nissenbaum (2011) explained, the privacy in public dilemma cannot be solved only through notice and consent, though it can play an important role in privacy protection. The privacy agenda is not only undermined by commercial purposes, but also by state surveillance. In Canada, the fifth principle of the fair information principles in the Personal Information Protection and Electronic Documents Act (PIPEDA, n.d.) recognizes to a certain extent the notion of context by limiting use, disclosure, and retention of personal information. However, with the adoption of Bill C-51 in Canada, anti-terror legislation, privacy is also in danger. The internet police have the right to intercept private communications on social media to fight cyber-criminality and share users' personal information with federal agencies (Canada, Library of Parliament, 2015). Will social media users have to retreat into self-censorship to protect their privacy? Will they have to choose between freedom of expression and privacy? Collective efforts are required to address the privacy paradox on social media and also the shift in privacy policies and surveillance laws, which have tremendous repercussions on individual privacy in this context.

Acknowledgements

The author is deeply grateful to the Ministry of Education, Recreation and Sports of Québec; the Faculty of Communication and School of medias of Université du Québec à Montréal, for funding her doctoral research. The author is also grateful to her PhD advisor and to study participants for their support throughout this process. The author would like to thank the reviewers for their insightful comments and suggestions on this manuscript.

Notes

1. Social media sites are a family of applications that enable users to participate in the production and sharing of content through interfaces that are user friendly. Such applications include wikis, virtual social worlds, virtual games, social network sites and blogs (Kaplan & Haenlein, 2010).

2. This research forms part of the author's doctoral research, carried out from 2009 to 2016. For Hine (2008), virtual ethnography is ethnography on, of, and through the internet.

3. I commented and "liked" users' Facebook posts. After both interviews, I created a Facebook group to keep users informed about my research and share information on surveillance and privacy issues. I also replied to informants' tweets.

4. Through the years, the Office of the Privacy Commissioner of Canada has provided privacy recommendations in order that Canadians' rights are respected when they are using SNSs (OPC, 2016).

References

Altman, Irwin. (1975). *The environment and social behavior: Privacy, personal space, territory, and crowding.* Monterey, CA: Brooks/Cole Publishing.

Ball, Kirstie. (2009). Exposure. *Information, Communication & Society, 12*(5), 639–657.

Barnes, Susan B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). URL: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/rt/printerFriendly/1394/1312 [January 28, 2017].

Boyd, Danah. (2008). *Taken out of context: American teen sociality in networked publics.* [Unpublished doctoral dissertation]. Berkeley, CA: University of California, Berkeley.

Boyd, Danah. (2010). *Social steganography: Learning to hide in plain sight.* [Blog post]. URL: http://www.zephoria.org/thoughts/archives/2010/08/23/social-steganography-learning-to-hide-in-plain-sight.html [December 4, 2017].

Boyd, Danah, & Hargittai, Eszter. (2010). Facebook privacy settings: Who cares? *First Monday, 15*(8). URL: http://firstmonday.org/article/view/3086/2589 [January 28, 2017].

Brandimarte, Laura, Acquisiti, Alessandro, & Loewenstein, George. (2012). *Misplaced confidences: Privacy and the control paradox.* Paper presented at the ninth annual Workshop on the Economics of Information Security (WEIS), Harvard University, Cambridge, MA.

Brighenti, Andrea Mubi. (2010). *Visibility in social theory and social research.* New York, NY: Palgrave Macmillan.

Brunton, Finn, & Nissenbaum, Helen. (2015). *Obfuscation: A user's guide for privacy and protest.* Cambridge, MA: MIT Press.

Canada. Library of Parliament. (2015). Proj*et de loi C-51. Deuxième session, quarante et unième législature, 62–63 Elizabeth II, 2013–2014–2015.* URL: http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=6932136&Col=1&File=4&Language=F [December 4, 2017].

Cefrio. (2010). *L'explosion des médias sociaux au Québec. NETendances, 1*(1). URL: https://cefrio.qc.ca/media/uploader/medias_sociaux.pdf [April 8, 2018].

Cefrio. (2012). Les médias sociaux ancrés dans les habitudes des Québécois. *NETendances, 3*(1). URL: https://cefrio.qc.ca/media/uploader/NETendances1-reseauxsociauxLR.pdf [April 8, 2018].

Cefrio. (2014). Actualité et nouvelles au Québec : l'ère de la mobilité et de l'information en temps reel. *NETendances, 5*. URL: https://cefrio.qc.ca/netendances/actualites-nouvelles-mobilite-information-temps-reel/web-simpose-principale-source-information/ [April 8, 2018].

Cefrio. (2015). Les médias sociaux : une plus forte présence dans le processus d'achat des Québécois. *NETendances, 6*(1). URL: https://cefrio.qc.ca/media/uploader/FasciculeNETendances2015-MdiasSociaux-Versionfinale.pdf [April 8, 2018].

Cefrio. (2017, July). Médias sociaux et économie de partage en ligne au Québec. *NETendances, 2016.* URL: http://www.cefrio.qc.ca/netendances/medias-sociaux-et-economie-de-partage-en-ligne-au-quebec [December 4, 2017].

Cubrilovic, Nik. (2009, July 19). The anatomy of the Twitter attack. *TechCrunch.* URL: https://techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack [January 28, 2017].

Daily Mail Reporter. (2011). Teacher sacked for posting picture of herself holding glass of wine and mug of beer on Facebook. *Mail Online.* URL: http://www.dailymail.co.uk/news/article-1354515/Teacher-sacked-posting-picture-holding-glass-wine-mug-beer-Facebook.html [January 28, 2017].

Davis, Jenny L., & Jurgenson, Nathan. (2014). Context collapse: Theorizing context collusions and collisions. Information, *Communication & Society, 17*(4), 476–485.

Donath, Judith. (2007). Signals in social supernets. *Journal of Computer-Mediated Communication, 13*(1), 231–251.

Ellison, Nicole B., Vitak, Jessica, Steinfield, Charles, Gray, Rebecca, & Lampe, Cliff. (2011). Negotiating privacy concerns and social capital needs in a social media environment. In Sabine Trepte and Leonard Reinecke (Eds.), *Privacy online: Perspectives on privacy and self-disclosure in the social web* (pp. 19–32). New York, NY: Springer.

Etzioni, Amitai. (2015). *Privacy in a cyber age. Policy and practice.* Houndmills: Palgrave Macmillan.

Goffman, Erving. (1973). L*a mise en scene de la vie quotidienne*. Paris : Les Editions de Minuit.

Granjon, Fabien, & Denouël, Julie. (2010). Exposition de soi et reconnaissance de singularités subjectives sur les sites de réseaux sociaux. *Sociologie, 1*(1), 25–43.

Gross, Ralph, & Acquisiti, Alessandro. (2005). *Information revelation and privacy in online social networks (the Facebook case)*. Research presented at the Workshop on Privacy in the Electronic Society (WPES), Alexandria, VA.

Hargittai, Eszter, & Marwick, Alice E. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*, 3737–3757.

Hine, Christine. (2008). Virtual ethnography: Modes, verities, affordances. In Nigel Fielding, Raymond M. Lee, & Grant Blank (Eds.), *The Sage handbook of online research methods* (pp. 257–270). Newbury Park, CA: Sage Publications.

Insights West. (2016). *Canadian Social Media Monitor 2016*. URL: http://www.insightswest.com/wp-content/uploads/2016/05/Rep_InsightsWest_CDNSocialMediaMonitor_2016.pdf [April 5, 2018].

Kaplan, Andreas M., & Haenlein, Michael. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons, 53*(1), 59–68.

Lomas, Natasha. (2017, September 11). Facebook fined €1.2M for privacy violations in Spain. *TechCrunch*. URL: https://techcrunch.com/2017/09/11/facebook-fined-e1-2m-for-privacy-violations-in-spain [December 4, 2017].

Lyon, David. (2002). Surveillance studies: Understanding visibility, mobility and the phenetic fix [Editorial]. Surv*eillance & Society, 1*(1), 1–7.

Marwick, Alice E. (2012). The public domain: Social surveillance in everyday life (draft version). *Surveillance & Society, 9*(4), 378–393.

Marwick, Alice E., & Boyd, Danah. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. N*ew Media & Society, 13*(1), 114–133.

Marx, Gary T. (2001). Murky conceptual waters: The public and the private. *Ethics and Information Technology, 3*, 157–169.

Marx, Gary T. (2006). Soft surveillance: The growth of mandatory volunteerism in collecting personal information—"Hey buddy can you spare a DNA?" *Lex Electronica, 10*(3), 1–10.

Marx, Gary T. (2015). Coming to terms and avoiding information techno-fallacies. In Marc Rotenberg, Julia Horwitz, & Jeramie Scott (Eds.), *Privacy in the modern age: The search for solutions* (pp. 118–126). New York, NY: The New Press.

Nissenbaum, Helen. (2011). A contextual approach to privacy online. *Daedalus, 140*(4), 32–48.

Office of the Privacy Commissioner of Canada (OPC). (2016). *Rapport annuel au Parlement 2015–2016 concernant la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur la protection des renseignements personnels*. Le temps est venu de moderniser les outils du 20^{e} siècle. URL: https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/201516/ar_201516 [December 4, 2017].

PIPEDA fair information principles. (N.d.). [Information on the Office of the Privacy Commissioner of Canada website]. *Government of Canada.* URL: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle [December 4, 2017].

Ministère de l'Éducation et de l'Enseignement supérieur (2015). Programme de formation de l'école québécoise. Enseignement secondiare, deuxième cycle. Rapport. *Government of Québec*. URL: http://www1.education.gouv.qc.ca/sections/programmeFormation/secondaire2/index.asp?page=domaines1 [January 28, 2017].

Proulx, Serge, & Kwok Choon, Mary Jane. (2011). L'usage des réseaux sociaux numériques : une intériorisation douce et progressive du contrôle social. *Hermès, 59*, 105–111.

Putnam, Robert. D. (2000). *Bowling alone: The collapse and revival of American community* (Kindle ed.). New York, NY: Simon & Schuster.

Radio-Canada.ca. (2013). *Les réseaux sociaux peuvent nuire à la recherche d'emploi*. URL: http://ici.radio-canada.ca/regions/abitibi/2013/11/06/002-prudence-reseaux-sociaux.shtml [January 28, 2017].

Randall, David, & Richards, Victoria. (2008). Facebook can ruin your life. And so can MySpace, Bebo … *The Independent.* URL: http://www.informationliberation.com/?id=24911 [January 28, 2017].

Raynes-Goldie, Kate. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday, 15*(1). URL: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2775/2432 [January 28, 2017].

Reid, Norma. (2011, June 18). Man fired for applauding Vancouver riot on Facebook. *CTV News.* URL: http://bc.ctvnews.ca/man-fired-for-applauding-vancouver-riot-on-facebook-1.659032 [January 28, 2017].

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

Spradley, James P. (1979). T*he ethnographic interview.* New York, NY: Rinehart & Winston.

Stalder, Felix. (2011). Autonomy beyond privacy? A rejoinder to Bennett. *Surveillance & Society, 8*(4), 508–512.

Steeves, Valérie. (2010). Résumé des recherches sur la protection de la vie privée des jeunes en ligne (15p). Commissariat à la protection de la vie privée du Canada. *Government of Canada.* URL: https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2010/yp_201003/ [April 8, 2018].

Trottier, Daniel, & Lyon, David. (2012). Key features of social media surveillance. In Christian Fuchs, Kees Boersma, Anders Albrechtslund, & Marisol Sandoval (Eds.), *Internet and surveillance: The challenges of Web 2.0 and social media* (Kindle ed., pp. 89–104). New York, NY: Routledge.

Tufekci, Zeynep. (2008). Grooming, gossip, Facebook and MySpace: What can we learn about these sites from those who won't assimilate? *Information and Library Science, 11*(4), 544–564.

TVA Nouvelles. (2011, October 19). *Profs menacés sur Facebook.* URL: http://tva.canoe.ca/emissions/tvaendirect/archives/2011-10-19.html [January 28, 2017].

Viseu, Ana, Clement, Andrew, & Aspinall, Jane. (2003). *Situating privacy online complex perceptions and everyday practices* [Draft version]. URL: https://www.oii.ox.ac.uk/archive/downloads/collaboration/seminars/20040317_Situating_Privacy_Online.pdf [January 28, 2017].

Westin, Alan F., (2003). Social and political dimensions of privacy. *Journal of Social Issues, 59*(2), 431–453.

Young, Allison L., & Quan-Haase, Anabel. (2013). Privacy protection strategies on Facebook. Information, *Communication & Society, 16*(4), 479–500.