

## Privacy and Social Media – The Blurring Of Public and Private Space (and How to Deal with It)

Mark Hayes and Oana Dolea<sup>1</sup>

### 1. Introduction

It could be said that privacy and the Internet are akin to ice cubes in hot chocolate – one simply dissolves the other.<sup>2</sup> In the most basic sense, after all, they are opposites: while the main purpose of the Internet is to disseminate large amounts information to many people as fast as possible, privacy is a concept that generally seeks to limit the flow of certain types of information. But is it inevitable that the continually growing importance of the Internet in social interaction, business, culture and countless other aspects of daily life means that online privacy will become a *non sequitur*, a thing of the past?

Online social media, in its increasingly diverse and complex forms, has expanded considerably in the past five years. It has become an important dimension of personal interaction for a significant segment of the population. Social networks, location-based services on mobile phones, and other social media innovations have multiplied and simplified our ability to share information online. Social media tools such as Facebook, Twitter, LinkedIn, Hi5, etc. have taken on a similar role to what local newspapers and radio stations once did; that is, bringing a community of people with common interests and values together to share ideas and information. This expansion has, however, increased the risk that this shared information will be exploited by individuals and public and private sector entities, often without the knowledge or consent of the individual whom the information concerns. While the different forms of social media have developed rapidly as tools for the dissemination of personal information in the online community, the legal and practical frameworks for understanding if, and to what extent, this information should be protected have not evolved quite as quickly. Of course, this has been

---

<sup>1</sup> Both of Hayes eLaw LLP, Toronto. © Mark Hayes and Oana Dolea, 2010. This article was presented at the 2010 Annual Meeting of the Canadian IT Law Association in Montreal, Quebec. This article is intended as a general summary of the law and is not legal advice. The opinions expressed in this article are personal to the author and may not represent the opinions of Hayes eLaw LLP or any of its clients. If you need assistance with any of the legal issues mentioned in this article, please consult a lawyer.

<sup>2</sup> Office of the Privacy Commissioner of Canada, “Unique Challenges to Privacy Rights Posed by the Internet and Other Emerging Technologies (Speech)”. Delivered by Lisa Madelon Campbell and Daniel Caron, Legal Services, Policy and Parliamentary Affairs Branch, at Toronto, Ontario. March 27-28, 2008. Available at: [http://www.priv.gc.ca/speech/2008/sp-d\\_080327\\_lc\\_e.cfm](http://www.priv.gc.ca/speech/2008/sp-d_080327_lc_e.cfm). Accessed on: August 14, 2010.

made additionally difficult by the fact that social media allows those with access to interact simultaneously, and share not only printed information, but rich media, with pictures, music and videos. Even keeping track of what information is available, in what format and from where it originates, in order to be able to designate it as private or public is proving a more and more difficult task as Internet technology, and particularly social media, becomes increasingly complex and widespread.

The goal of this paper is to discuss the scope of the concept of “online privacy,” and in particular what is the line between the public and private sphere in the context of online social media? The first part of the paper will present an overview of the meaning of privacy in the online space. This will be followed by a review of the Privacy Commissioner of Canada’s decision regarding perceived violations by Facebook of Canadian privacy law, which will set out a number of areas which present privacy concerns in the context of online social media. Finally, we will discuss the advantages of using social media for businesses wishing to increase their competitiveness and protect their brand, and strategies for doing so in a way that minimizes or ameliorates privacy concerns.

## **2. Public vs. Private Sphere: The *Facebook Case* and beyond**

Advances in social media technology are blurring the line between what we consider to be private and public spheres for personal information by altering the way in which privacy rights are interpreted. The importance of understanding where the public sphere ends and the private one begins in the context of social media lies in the potential effects of unregulated collection, use, disclosure of personal information by users, including a loss of control over one’s own personal information, which, with the “help” of social media technology, can precipitate unpredictable effects on reputation, and the proliferation of unscrupulous data marketing.

### **2.1 Privacy in social media: the shifting meaning of “reasonableness”**

The starting point for an analysis of the meaning of privacy in the context of online social media is to identify what it is we don’t know, specifically the precise location of the dividing line between the public and private sphere in that context. The numerous and continually evolving forms of social media that have and continue to arise are structures to which the rules of privacy have not previously been applied. This dividing line between the private and public spheres of

protected information is continually changing and must, by its very nature, shift as it adapts to the circumstances of a particular context. As such, the scope and meaning of privacy rights in traditional offline contexts may not be the same as, or even analogous to, privacy rights as applied to social media. Changing social attitudes to the sharing of information are constantly and forever altering our traditional concept of privacy.<sup>3</sup> In other words, the concept of privacy in the social media environment will be mostly influenced by the attitudes of users to what should “reasonably” be protected as being private information.

Reasonableness is a flexible and adaptable concept, which can change over time, influenced by changing circumstances and perceptions. The requirement of “reasonableness” is central to Canadian privacy. Section 5(3) of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) states that:

“An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.”

PIPEDA thus imposes an overall reasonableness threshold regarding the extent of the collection, use, or disclosure of such personal information. The concept of “reasonableness” appears in many other contexts in PIPEDA and in provincial privacy legislation, although the word itself is generally not defined.

Therefore, a basic privacy compliance question is whether it is reasonable to permit the collection, use and disclosure of users’ personal information by social media services such as Facebook in exchange for the free service offered. In the recent assessment of Facebook’s activities by the Office of the Privacy Commissioner of Canada (OPC), discussed below, one of the issues analyzed was whether it was legitimate for Facebook to be collecting and disclosing certain user personal information for the purpose of operating its Facebook ads service, in order to gain the revenue necessary to provide user access to Facebook for free. The question that arose can be broken down into two parts:

- Is the provision of the advertisements, combined with the inability of users to opt out of receiving such advertisements, a “reasonable purpose” for the collection and disclosure of users’ personal information?

---

<sup>3</sup> *Ibid.* note 2.

- What personal information may reasonably be collected and disclosed to be able to operate the ads function of Facebook?

Determining what is “reasonable” in any specific privacy context has always been a difficult and confusing exercise. What is “reasonable” and “appropriate” use of personal information to one person may be “unreasonable” and “inappropriate” to another. While the courts have over the years been able to handle reasonableness concepts in other contexts, there is reason to believe that privacy issues, at least at this early stage, may be somewhat more of a challenge. One example is instructive. In August 2001, the Public Interest Advocacy Centre (“PIAC”) commissioned an opinion poll<sup>4</sup> to determine what “secondary” marketing uses Canadians felt were justifiable.<sup>5</sup> Although clearly the sponsor of the study hoped to demonstrate that Canadians were solidly opposed to certain practices, in fact the study's results show a remarkable split in public opinion. The report's authors concluded that:

- Reflecting broad variations in attitudes in this area, there is little that can be assumed about individual consumer consent to secondary marketing. In fact, Canadians have widely differing views in this area.
- While many Canadians — a slim majority (52 per cent) — expect that companies they purchase from will try to build an ongoing relationship with them, an almost equally large number do not. Likewise, a large segment of the population also expect that companies will keep track of their purchases for further marketing purposes. Again, however, there is a not insignificant number who do not, ranging from 20 per cent to a third, depending on the type of company.<sup>6</sup>

In view of this wide and evenly-distributed disparity of opinion, it can be difficult to know what is meant by the use of the term “reasonable” in section 5(3) of PIPEDA. The results of the PIAC survey would seem to indicate that it will be challenging to find that any specific purpose will not be reasonable when public opinion is so polarized – in effect, whichever decision is made, the views of about half of the population must be found to be “unreasonable”. It is likely

---

<sup>4</sup> The results were available at [http://www.piac.ca/privacy/survey\\_results\\_in\\_english](http://www.piac.ca/privacy/survey_results_in_english) as of October 13, 2010.

<sup>5</sup> In this context, “secondary marketing” refers to using personal information to target individuals for the marketing of products or services different from the ones in respect of which the information was originally collected.

<sup>6</sup> Ekos Research, “Business Usage of Consumer Information for Direct Marketing: What the Public Thinks”; <http://www.piac.ca/Directmarketing%20survey%20E.pdf>, at page 3.

that any similar question would elicit a similarly split set of personal opinions, and that those opinions might very well be split depending on a number of factors such as age and education.

Further, in the online context, and therefore in the context of social media, the sense of what is “reasonable” with regard to collection, use and disclosure of personal information may in some cases differ from traditional understandings of privacy. Privacy expectations may continue to change as the Internet and the way we interact with and through it also evolve. The question is often asked (especially in the popular media) whether there is any privacy expectation left on the Web. Emily Nussbaum, writing in *New York Magazine*, identifies a generational trend: it is only the older generations that still seem to care about privacy. She states that “as younger people reveal their private lives on the Internet, the older generation looks on with alarm and misapprehension not seen since the early days of rock and roll.” According to a recent study, 61% of 13-to-17 year olds have a profile online, half with pictures, and perhaps as much as 55% of 12-to-17 year olds have one also – all proof of a generation that is at ease with and dominates social media. She describes 20-somethings that view posting anything from nude pictures to diaries and phone numbers as simply a part of documenting their life and sharing it with others. They are accepting of the negative consequences that can arise from sharing so much, because of what they perceive as the positive aspects of having such a strong presence online. Nussbaum concludes that members of the younger generation think of themselves as having an audience, find sharing personal information in the public space much more natural than previous generations, and have thicker skin than older generations, allowing them to more easily accept more risks to their privacy posed by heavy use of social media.<sup>7</sup>

Perhaps even more significantly, a 2009 study undertaken for the OPC also revealed that, “generally, people did not indicate being very concerned about their personal privacy online - either in general, or specifically in terms of their activities on social networking sites.”<sup>8</sup>

---

<sup>7</sup> Emily Nussbaum, “Kids, the Internet and the End of Privacy: the Greatest Generation Gap since Rock and Roll”. *New York Magazine*. Available at: [www.nymag.com/news/features/27341](http://www.nymag.com/news/features/27341). Accessed on: October 5, 2010.

<sup>8</sup> Office of the Privacy Commissioner of Canada, “Decima Research Report: Focus Testing Privacy Issues and Potential Risks of Social Networking Sites.” March 20, 2009, at page 4. Available at: [http://www.priv.gc.ca/information/survey/2009/decima\\_2009\\_02\\_e.cfm](http://www.priv.gc.ca/information/survey/2009/decima_2009_02_e.cfm). Accessed on: August 14, 2010.

Additionally, while older groups surveyed revealed that they mitigate any concerns by way of increased personal privacy management, younger generations described taking fewer precautions and seemed less concerned with online privacy overall. Interestingly, all of those surveyed acknowledged being aware of social media services, notably Facebook, using user personal information to target advertising to their users, while stating that they believed third parties having access to their information was something they assumed was happening and was a reasonable cost of using the social media service. The individuals surveyed indicated that the benefits of social media, primarily of being able to stay in touch with friends easily and free of charge, outweighed any risks, such as “low-value personal information being exploited in any harmful way.”<sup>9</sup> Additionally, a study conducted by the Institute of Information Systems at Berlin’s Humboldt University recently found that, while people may be objectively concerned about how their information is handled in an online context, they easily forget such privacy concerns when faced with entertaining exchanges online, or offers of appropriate benefits in exchange for divulging certain personal information.<sup>10</sup>

It seems, therefore, that a new way of thinking about privacy may have emerged in the online context, at least amongst a sizeable segment of the user population. The question, in terms of applying the existing privacy laws in the social media context, may then become “which generation gets to decide?” How does a privacy regulator account for changing and disparate attitudes toward the concept of what is “reasonable” collection, use and disclosure?

In addition to variations across different across age groups and other demographic segments, views about the reasonableness of privacy protections can and do change over time. This is especially the case in the constantly evolving culture (or, more accurately, cultures) of the Internet. For example, the idea of using email to distribute advertising through the Internet provoked strong protests from a large number of users in the early 1990s. In 1993, Phoenix attorneys Laurence Canter and Martha Siegel emailed thousands of newsgroups advertisements for their legal services. Their Internet provider received over 30,000 vigorous complaints, mostly

---

<sup>9</sup> *Ibid.* note 8, at page 5.

<sup>10</sup> *Supra.*, note 2.

in the nature of “flames”, causing it to actually cancel Canter & Siegel’s Internet account.<sup>11</sup> It is probably unnecessary to note that the public perception of, and tolerance for, online advertising is now dramatically different, as most Internet users view advertising on the Internet as an integral, reasonable part of the online experience. However, the fact that only a few years ago the idea of sending email advertisements would be seen as reprehensible underscores the fact that attitudes about online privacy can and do change radically over time and that the reasonableness of personal information uses must be assessed in a fluid and confusing environment.

## 2.2 The “Facebook” case: applying privacy law to the context of social media

On July 16, 2009, the OPC released its “Report on Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the Personal Information Protection and Electronic Documents Act.” The report was in response to a complaint by CIPPIC that Facebook’s activities were in violation of Canadian privacy law. Comprising 24 allegations ranging over 11 distinct subjects, the CIPPIC complaint addressed Facebook’s policies with regard to default privacy settings, collection and use of users’ personal information for advertising purposes, disclosure of users’ personal information to third-party application developers, and collection and use of non-users’ personal information.

The Facebook case highlights some important challenges to the notion of privacy that arise in the context of online social media, and proposes reinterpretations of each respective dimension of the “privacy right” as applicable in the context of social media.

### 2.2.1 Jurisdiction: the application of territorial privacy laws

The Internet has evolved into an effective business and communication tool, but its operation has also created a number of jurisdictional questions in these contexts. Which state has jurisdiction over a legal dispute that arises out of activity over the Internet? What set of substantive legal rules will apply to such a dispute? Will one jurisdiction’s ruling in connection with such a dispute be enforced in another, and how?

---

<sup>11</sup> Jordan Rappaport, “Attorney Advertising on the Internet”. Available at <http://osaka.law.miami.edu/~froomkin/seminar/papers/rappaport.htm>. Accessed on: October 8, 2010.

CIPPC's privacy complaint against Facebook raised a number of jurisdictional issues. Given the fact that Facebook is an American-based company, does PIPEDA even apply to it and other such foreign web-site operators? Would the OPC even have jurisdiction to investigate the complaint under PIPEDA? While the Assistant Commissioner's report did not discuss this issue directly, the Federal Court of Canada has previously ruled, in *Lawson v. Accutech Inc.*<sup>12</sup>, that even though PIPEDA is not a long-arm statute, the OPC does have jurisdiction under PIPEDA to investigate a foreign-based entity where that entity had a real and substantial connection to Canada. In that case, as in the Facebook situation, the substantial connection was the fact that the foreign entity was collecting and using personal information of Canadians without their consent. The underlying assumption behind PIPEDA is, therefore, that it applies to website operators collecting personal information of Canadians, no matter where the service may originate. In the United States, the Federal Trade Commission applies a similar approach, as the Children's Online Privacy Protection Act applies to operators of both U.S. and foreign-based commercial websites that are directed at or knowingly collect information from children in the United States.<sup>13</sup>

The Facebook case illustrates that a complete analysis of "privacy" and "privacy regulation" in the online context must consider the potential for jurisdictional uncertainty that characterizes the online sphere. This is important, since a restrictive view of jurisdictional competence of privacy regulators can limit the effectiveness of local laws aimed at protecting consumers. The potential consequences of limited privacy protection jurisdiction include individuals being subjected to privacy laws offering different, often lesser, protection than that expected under the laws and privacy philosophy of the home jurisdiction. Organizations can then take advantage of this situation to engage in "forum shopping" or regulatory arbitrage, such as launching privacy-invasive technologies in jurisdictions with more relaxed approaches to privacy.<sup>14</sup>

---

<sup>12</sup> [2007] 4 F.C.R.

<sup>13</sup> United States Federal Trade Commission, "Frequently Asked Questions about the Children's Online Privacy Protection Rule", FAQ 19. Available at: <http://www.ftc.gov/privacy/coppafaqs.shtml>. Accessed on: October 5, 2010.

<sup>14</sup> Supra, note 2. Michael Geist, quoted on page 2 and 3.

### 2.2.2 Advertising: what is a reasonable purpose?

Partly as a result of the popularization of the Internet, personal information of individuals has become very valuable. An entire online industry exists and specializes in the collection, compilation, analysis and dissemination of individuals' personal data to other individuals or organizations.<sup>15</sup> In the context of social media, users' information is collected and disseminated to advertisers in exchange for the revenue that keeps social media services operating. The Assistant Commissioner's analysis on this issue in the context of the Facebook case highlights how this reality affects the scope of privacy rights in the context of social media.

Facebook, like all social media sites, requires revenue to be able to offer its free services. Advertising is the source of revenue essential to the provision of the service. Facebook's users must therefore be willing to receive a certain amount of advertising, or the service will not be able to continue to operate. Facebook provides aggregated user information to its advertisers in order to allow them to target their desired demographic. While users may opt out of Social Ads, which are targeted to each user based on their actions on Facebook, Facebook does not allow opting-out of Facebook Ads, which are targeted based on particular demographic groups created on the basis of aggregated user information. CIPPIC's complaint to the federal privacy Commissioner claimed that the inability of users to opt-out from all types of targeted advertising delivered through Facebook, including Facebook Ads, was in breach of their privacy rights.

In deciding whether Facebook could validly require users to receive targeted Facebook Ads, the Assistant Commissioner undertook an analysis of whether Facebook's use of personal information in this context was reasonable. First, she found that, in serving targeted ads to users, Facebook was engaging in "uses of personal information under the Act [PIPEDA]."<sup>16</sup> This is a somewhat controversial finding. Facebook argued that the data that was used to target the advertising was in fact anonymous and could not be used to identify the user. This is a common view of online advertisers who use devices such as cookies and web beacons to gather

---

<sup>15</sup> *Ibid.*

<sup>16</sup> Office of the Privacy Commissioner of Canada, "Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. under the *Personal Information Protection and Electronic Documents Act*" (Report by Elizabeth Denham, Assistant Privacy Commissioner of Canada), July 16, 2009, at para. 132. Available at: [http://www.priv.gc.ca/cf-dc/2009/2009\\_008\\_0716\\_e.cfm](http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm). Accessed on: August 3, 2010.

information about the browsing habits of a computer user (or perhaps multiple users of a single computer) to determine what advertisements should be inserted onto the user's browser. The Assistant Commissioner did not accept this distinction and saw the targeting of ads as a personal information use even though the information used to do the targeting had little or no ability to actually identify the individual.

The Assistant Commissioner then based her analysis on the distinction between uses of personal information for primary and secondary purposes. Given the vital nature of advertising revenue to Facebook's operating model, the use of personal information was deemed to be a primary purpose, because it is essential to the service.<sup>17</sup> Furthermore, she noted that while the delivery of Facebook Ads targeted to users according to their demographic group was not intrusive, the delivery of Social Ads based on specific actions of the user was much more so. In fact, the Assistant Commissioner commented, "the Social Ad takes on the appearance of an endorsement of the product by the user."<sup>18</sup> Due to their less-intrusive nature and the essential nature of advertising revenue in the context of the Facebook service, the Assistant Commissioner found that the mandatory provision of Facebook Ads was in fact a reasonable way for Facebook to be using its members' personal information, while the consent of users was required for the serving of Social Ads using the personal information of users.

The OPC analysis on this issue indicates a departure from the standard scope of the "privacy right." The definition of "reasonableness" with regard to privacy and advertising in the context of social media is adapted to take into account the special factual context – namely, the essential nature of the advertising in this context – in which the meaning of "privacy" is being applied. Interestingly, the analysis contains little reference to the actual views of Facebook users, who were apparently not asked for their opinion on the issue.

### 2.2.3 Consent of non-users

Another important privacy issue addressed in the Facebook case is the privacy rights of non-users of social media. Users have the ability to disclose to Facebook, as well as similar social media operators, the personal information of non-users by directly posting it on their own or

---

<sup>17</sup> *Ibid.*, at para. 131.

<sup>18</sup> *Ibid.*, at para. 133.

other users' profile, by tagging images or videos with the names of non-users or by disclosing the email of such a non-user in the course of inviting them to join the service. This creates a potential consent problem under PIPEDA since Facebook has no direct means by which to obtain consent from non-users.

The OPC's analysis of this issue was based on a distinction between "activities conducted by Facebook users strictly for personal reasons and those activities in which Facebook itself is involved."<sup>19</sup> In the view of the Assistant Commissioner, obtaining consent from non-users for the use of their personal information is only necessary in contexts where the social media operator intends to use this information for its own purposes.<sup>20</sup> In the case of Facebook, a distinction was made between users sharing personal information of non-users on their profile, which was seen as a use for personal purposes and outside the scope of PIPEDA (thus relieving Facebook from the obligation to obtain the non-users' consent) and the up-loading of non-user emails in the context of the "Invite New Friends" feature, for example, from which Facebook benefits by gaining new members and thereby increasing its ability to generate revenue.

Facebook agreed to mitigate the privacy concerns raised by the OPC by undertaking to provide the appropriate information to users to ensure that they have the consent of non-users to share their information with Facebook, and exercising reasonable due diligence to make sure this is happening.

#### 2.2.4 Consent for third-party disclosure of collected information

In the context of a number of social media services, including Facebook, the issue of disclosure of users' personal information to third parties is a relevant concern. How and when is consent for such disclosure necessary? How much personal information should be disclosed? What safeguards is the operator obliged to provide before disclosing the information to third parties?

In the Facebook complaint, the key issue in this respect relates to the Facebook Platform, which enables third parties to create Facebook applications that users can add to their

---

<sup>19</sup> *Ibid.*, at para. 306.

<sup>20</sup> *Ibid.*, at para. 311.

accounts.<sup>21</sup> This highlighted a number of issues related to consent to the collection of users' personal information for, and extent of disclosure by Facebook to, third party application developers, including (i) the failure to disclose the purpose for which personal information was disclosed to third party application developers; (ii) providing third party developers with personal information beyond what is necessary for the purposes of the application; (iii) not notifying users of the implications of withdrawing consent to sharing personal information with third party application developers; and (iv) allowing third party developer access, without adequate notice, to personal information of users when friends or fellow network members added the application.<sup>22</sup>

In response to the complaint, the Assistant Commissioner's report stated that a social media service such as Facebook would have to prevent a third party application from accessing any user personal information until either the social media service or the third party obtains express consent for each type of data the app operator wants to access. While disclosure of collected personal information to third parties is also an issue that arises in traditional privacy analysis, specific technological and operational aspects of Facebook create a completely new context in which this challenge must be resolved.

#### 2.2.5 Data retention: what is reasonable?

The extent to which personal information collected from individuals is retained and stored is also an important element of the notion of reasonableness that is central to privacy regulation. Both PIPEDA<sup>23</sup> and provincial privacy statutes contain provisions specifying that no more personal information can be retained than is necessary for a particular identified purpose, and that such information cannot be retained or stored for longer than necessary for that purpose.

---

<sup>21</sup> *Ibid.*, at para. 147.

<sup>22</sup> *Ibid.*, at para. 146.

<sup>23</sup> Section 5(1) of PIPEDA mandates that organizations collecting personal information must abide by the Principles set out in Schedule 1 to the Act. Principle 4 sets out that only the information necessary for the purposes identified by the organization may be collected. Principle 5 states that personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law, and may only be retained only as long as necessary for the fulfillment of those purposes.

The Facebook case illustrates how this issue can arise in the context of social media as a result of the distinction between deactivation and deletion of a user's account. When a Facebook account is deleted, all personal information of the user collected by Facebook is also deleted. However, when a user simply deactivates their account, their personal information is retained indefinitely. The Assistant Commissioner emphasized the fact that deactivation does not mean deletion and that notice be given to users outlining the availability of both options and outlining the differences between them in terms of information retention. The Assistant Commissioner also suggested that Facebook impose a retention policy "whereby the personal information of users who have deactivated their accounts will be deleted from Facebook's servers after a reasonable length of time."<sup>24</sup> Facebook resisted this recommended measure as inappropriate in the context in which deactivation occurs, citing the expectations of users who deactivate and then reactivate on a longer timeframe that their social connections will be intact when they return.<sup>25</sup> The difference of opinion on this issue exemplifies how the definition of "reasonable" data retention in the social media context differs from the traditional application of privacy rules.

The Assistant Commissioner's assessment of different issues highlighted in the complaint against Facebook demonstrates that the unique way in which social media services operate may at times dictate a different definition of "reasonableness" and that the difficulty in this particular exercise remains finding a way to adapt the meaning and application of existing privacy laws in an environment where the traditional perception of privacy and privacy rights may not apply.

### 2.3 Privacy and social media: two practical applications

Privacy issues relating to social media have practical effects outside of the operation of those services. The scope of privacy in the social media context can affect an individual's reputation, for example, given that so much personal information is collected and potentially disseminated in uncontrolled ways. What is deemed to be "private" versus "public" can have adverse consequences on online aspects of an individual's offline life, but may not be the

---

<sup>24</sup> Supra, note 16, at para. 249.

<sup>25</sup> *Ibid.*, at para. 251.

deciding factor in other social media-related issues, such as the decision whether to allow disclosure of personal information located on social media profiles in the context of litigation.

### 2.3.1 Employment

Should an individual have to think twice before posting a party picture onto their social media page profile? In recent years, many employers have developed a practice of accessing and reviewing candidate profiles on social media websites. Not surprisingly, this practice has attracted controversy, partially because there is no common understanding of whether some or all of the personal information available on a social media site should be considered to be in the “private sphere”. As previously discussed, there is a clear gap between different generations’ perception of privacy. Young graduates just entering the work force see information posted online as private, while older people, who are usually also those in management positions doing the hiring, often do not share the same notion of “network privacy.” Ryerson University Professor Avner Levin explains that the notion of “network privacy” refers to a belief that information shared within an individual’s personal social network is considered private as long as its dissemination is limited to that social network.<sup>26</sup> In his study of 2,000 young people, Dr. Levin also found, based on their “network privacy” understanding of social media, that younger people did not express much concern that personal information would be accessed by an employer.

According to a recent speech by the former Assistant Commissioner, Elizabeth Denham, users of social media still “misunderstand privacy risks in an environment that promotes disclosures because it feels intimate and is immediate.”<sup>27</sup> Such users do not seem to fully appreciate the fact that, once posted online, information may become widely available despite the privacy settings of a particular social media application. As discussed above, the scope of privacy rights in the context of social media has not yet been formally established and reasonable expectations of privacy may still vary widely as between employers and employees. In Europe, German lawmakers are attempting to bring some clarity to the issue of whether social media profile information should be considered public and accessible to potential

---

<sup>26</sup> *CBC News Online*, “Prof says young people have unique sense of Facebook privacy,” September 4, 2008. Available at: <http://www.cbc.ca/technology/story/2008/09/04/facebook-privacy.html>. Accessed on: August 27, 2010.

<sup>27</sup> *Ibid.*

employers; a draft law on employee data security will make it illegal to become a Facebook friend with an applicant in order to obtain profile information for the individual that is designated as “private.”<sup>28</sup> While such legislation would create a stronger division between privacy-protected information on social media sites, which would be identified as belonging to the private sphere, while the remaining parts of social media profiles would belong to the public sphere and thus remain legally accessible to scrutiny by employers, the divergent views held by individuals about what information is private and how it should be restricted make the drafting of such rules very difficult.

The former Assistant Commissioner has stated that, while no investigation into employment candidate background checks on social networking sites has been undertaken so far, PIPEDA is likely to prevent this type of collection of information by companies without consent. PIPEDA mandates obtaining consent for any collection of personal information, and some employers may not inform candidates that they will be subject to a check. Many employers do obtain a wide-ranging consent from prospective employees that permits the employer to access information about the applicant, and this consent is what many employers rely on to access social media information. However, PIPEDA also imposes accuracy and reasonableness requirements with regard to the collection of information, opening up questions of whether it is reasonable to use a candidate’s personal profile on social media to determine their suitability for a job.<sup>29</sup> Once again, given the divergent views on privacy in the social networking context, concretely interpreting PIPEDA rights in this context is likely to prove difficult.

### 2.3.2 Social Media and Litigation

Recently, an explosion of cases involving social media issues has highlighted the effect on litigation of the way in which privacy is perceived in the context of social media. Most frequently

---

<sup>28</sup> David Jolly, “Germany Plans Limits on Facebook Use in Hiring”, *New York Times*, August 25, 2010. Available at: <http://www.nytimes.com/2010/08/26/business/global/26fbbook.html>. Accessed on: August 26, 2010.

<sup>29</sup> Office of the Privacy Commissioner of Canada, “Work and Play in the Age of Social Networking” (Speech by Elizabeth Denham, Assistant Privacy Commissioner of Canada), Calgary, Alberta, May 12, 2010. Available at: [http://www.priv.gc.ca/speech/2010/sp-d\\_20100512\\_ed\\_e.cfm](http://www.priv.gc.ca/speech/2010/sp-d_20100512_ed_e.cfm). Accessed on: August 22, 2010.

seen in the context of family, criminal and personal injury cases, questions arise about how evidence from social media is and can be used before the courts.

Information from social media sites is often used as evidence that a party's actions are inconsistent with positions or evidence in the action, for example in the context of proving extent of disability. Information about a party's "friends" or contacts could be evidence contradicting a claim that the party did not know or have contact with a particular individual, and a party's communications can be evidence inconsistent with evidence of legal obligations, such as a non-contact order. The legal issues arising here include: (i) whether production of social media evidence is prohibited by privacy statutes (i.e. whether the information contained therein is private or public); (ii) whether and when can a party to be compelled to divulge contents of social media profile or pages; and (iii) whether and when can a social media operator be required to divulge information such as the IP address of a subscriber.

PIPEDA allows an organization to disclose otherwise private information without consent if it is required to comply with a subpoena or warrant issued or an order made by a court, or other person or body with jurisdiction to compel the production of information.<sup>30</sup> PIPEDA also allows disclosure if an organization is required to comply with the rules of court relating to the production of records<sup>31</sup> or if otherwise required by law.<sup>32</sup>

These exceptions generally require a party to litigation to disclose any relevant personal information in their possession or control. While the disclosed information may still be subject to PIPEDA restrictions in the hands of the opposing party, the implied undertaking of confidentiality will also apply and is arguably even more restrictive. Provincial privacy statutes contain similar exceptions.

Litigants who have tried to resist production of relevant personal information evidence solely on the basis of privacy have been consistently unsuccessful. In *Ferenczy v. MCI Medical Clinics*,<sup>33</sup> the plaintiff attempted to exclude damning surveillance evidence. The court found a

---

<sup>30</sup> *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, s. 7(3)(c).

<sup>31</sup> *Ibid.*

<sup>32</sup> *Ibid.*, s. 7(3)(i)

<sup>33</sup> (2004), 70 O.R. (3d) 277.

personal injury plaintiff should be deemed to have given his implied consent to surreptitious observation in cases where physical capabilities are in issue. The court also held that a violation of PIPEDA does not have any direct impact on the issue of admissibility of evidence. Interestingly, the OPC has stated that it has not accepted *Ferenczy* as a precedent.

The admissibility and compellability of social media evidence is therefore primarily a relevance issue, not a privacy issue. Privacy is one factor to be considered in determining the relevance and proportionality of the requested production. While the court will order the production of “private” Facebook pages if there are sufficient grounds to conclude that they obtain relevant evidence, it will not allow “fishing expeditions.” For example, in *Murphy v. Perger*,<sup>34</sup> the court ordered the production of the plaintiff’s private Facebook page. Since the plaintiff had a publicly available site which contained pictures of the plaintiff engaged in certain social activities, it was reasonable to conclude that Facebook would as well, since pictures can also be stored on Facebook. The court concluded that any invasion of privacy would be “minimal” in that case.

In *Leduc v. Roman*,<sup>35</sup> the Ontario Superior Court of Justice allowed the production of all pages of the plaintiff’s Facebook profile to verify the plaintiff’s assertion during a medical exam that “that he did not have friends in his current area, although he had a lot on Facebook.” The court confirmed the fact that social media may contain evidence relevant to the issues in an action. It also established the notion that it is reasonable to infer that content on a person’s public profile is similar to content on a private profile, and that where a user only has a private profile, it is reasonable to infer from the purpose of social media such as Facebook that users will take advantage of the service to make personal information available to others. The court based its decision to allow disclosure of the plaintiff’s Facebook pages on the high likelihood that they contained content relevant to the issue of how the plaintiff had been able to lead his life since the motor vehicle accident at issue.

There have also been numerous criminal cases involving voluntary disclosure to police of subscriber information by Internet Service Providers (ISPs). The general rule is that such

---

<sup>34</sup> 2007 CarswellOnt 9439; 67 C.P.C. (6th) 245.

<sup>35</sup> 2009 CarswellOnt 843, 308 D.L.R. (4th) 353, 73 C.P.C. (6th) 323.

disclosure is permitted under PIPEDA and the Canadian Charter of Rights and Freedoms if subscriber agreements permit disclosure. There is no reasonable expectation of privacy in this context. While no specific cases exist on this issue with regard to social media sites, the same reasoning is likely to apply. For example, based on the ISP cases, the following provision in the Terms of Service of a Facebook app would likely allow disclosure:

“We may be required to disclose user information pursuant to lawful requests, such as subpoenas or court orders, or in compliance with applicable laws. We do not reveal information until we have a good faith belief that an information request by law enforcement or private litigants meets applicable legal standards. Additionally, we may share account or other information when we believe it is necessary to comply with law, to protect our interests or property, to prevent fraud or other illegal activity perpetrated through the Facebook or using the Facebook name, or to prevent imminent bodily harm. This may include sharing information with other companies, lawyers, agents or government agencies.”<sup>36</sup>

In contrast, it is not clear whether the following Google Terms of Service provision would authorize disclosure:

“We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent or otherwise address fraud, security or technical issues, or (d) protect against harm to the rights, property or safety of Google, its users or the public as required or permitted by law.”<sup>37</sup>

In the above provision, the meaning of an “enforceable governmental request” that would trigger a PIPEDA disclosure exception is unclear.

It seems, therefore, that courts are not going to pay much attention to “privacy” if it impacts on providing full disclosure, finding the truth or being fair to both parties. Where the production right is questionable and information is very sensitive, privacy may be one factor of many to be considered in determining proportionality of request for information. In most cases, personal information made available on social media sites will be produced.

---

<sup>36</sup> Terms of Service, “My Arabic Name” Facebook App. Available at: <http://apps.facebook.com/myarabicname/privacy.php>. Accessed on: August 25, 2010.

<sup>37</sup> Privacy Policy, Google.com. Available at: <http://www.google.com/privacypolicy.html>. Accessed on: August 25, 2010.

To avoid professional negligence, lawyers would be well advised to look at social media sites in any case where character or activities of an individual party could prove relevant, and to seek production of such content if information is not forthcoming. Additionally, lawyers must advise clients that relevant portions of web sites relating to them must be listed in documents affidavits in the context of a proceeding.

A strong understanding of the scope and impact of privacy rights in the social media context is clearly important for the protection of individual users of social media, given the still-uncharted territory that is privacy in the context of social media. However, establishing and understanding the line between the public and private sphere is also important for business clients who wish to use social media as a tool to enhance their commercial activities and protect their brand. They need to know what the privacy risks of doing so entail, in order to make informed decisions about the extent and the way in which they establish a presence in the online social media world.

### **3. Privacy, Social Media and Business Clients: Rewards versus Risks**

The advent of the Internet has meant both increased opportunities for businesses and increasing competition among them. In order to compete in the online world, businesses must rely more than ever on the reputation of their brand. When speaking of a company's "brand," we refer not only to the visual design elements of its logo or product, but also to the ideas and ideals associated with the company and its reputation for quality customer service, products, deals and value. The overall brand is a valuable asset that takes a long time to develop but is very easy to lose or have depreciate.

As a result, in order to maintain their competitive edge, businesses must be very careful how their brand is used, represented and treated in the online as well as the physical world. As a result of its widely accessible and mostly unchecked nature, social media can be both a useful brand protection tool and a source of risk for businesses.

#### **3.1 The Rewards – why clients should use social media**

A client's brand can easily be affected by unauthorized uses of any brand elements in various forms of social media. Whether in the context of a page claiming to represent the company, a blog purportedly disclosing the best ways to obtain deals on the client's products or

the unauthorized association of the client's logo with an unendorsed product, unauthorized social media uses of a client's brand can seriously affect (often negatively) the customer perception of the brand, and thus its value. As a result, clients must try to understand the ways in which unauthorized uses of their brand in the context of social media can affect it, as well as the ways they can themselves use social media to prevent or mitigate such effects.

### 3.1.1 Potential Negative Effects of Unauthorized Social Media Uses of the Brand

Unauthorized social media uses of the design elements of the client's brand can affect the value of the client's intellectual property rights. Unauthorized uses of the brand word mark, logo, ad copy and other design aspects may constitute trade-mark and/or copyright infringement. In some cases, uncontrolled uses of design aspects of the brand can result in a loss of distinctiveness of the client's trade-mark, and the eventual loss of trade-mark protection.

Unauthorized social media uses of the client's brand can also communicate out of date or inaccurate information about the client's products, such as inaccurate consumer offers, or may associate the brand with unauthorized third-party goods or services, which may be inferior in quality. Such uses may mislead and confuse consumers and consumer confidence in the brand and the value attached to it may become diluted.

Diversion of corporate opportunities for the client and a loss of consumer focus are further negative results that can result from unauthorized uses of the client's brand. For example, third parties may use a business' proprietary brand information to create commercial opportunities for unauthorized resellers of the client's products, to the detriment of the client. Not only does such use contribute to consumer confusion about the source of the products, such confusion may also lead to a loss of consumer confidence, as well as potential regulatory and direct complaints on privacy and consumer protection grounds and focus consumer attention away from the brand-owner's products. Unauthorized users may also profit from their use through the sale of advertising in association with the brand.

Finally, unauthorized use of trade-marks and/or copyright material licensed by a business could expose it to third-party liability for failing to prevent the use. Similarly, businesses may be exposed to third party liability as a result of misleading advertising that can result from

unauthorized uses of their brand. For example, they may be exposed to consumer liability on the basis of their failure to prevent the unauthorized promotion of inaccurate information in conjunction with their brand. Furthermore, they may be exposed to liability vis-à-vis providers of partner goods or services, on the basis of their failure to prevent an unauthorized association between that provider's good or service and any goods or services also associated with the unauthorized user of the client's brand.

### 3.1.2 Preventing the Effects of Unauthorized Social Media Uses of the Brand

There are a number of proactive strategies that businesses may adopt to prevent and mitigate the effects of unauthorized uses of their brand in the social media sphere.

First, maintaining an active authorized online presence allows the brand owner to monitor and prevent unauthorized uses of its brand or that of its partners. Brand owners can create an official presence on social networking sites, including establishing an online presence for new products. Other potential strategies include participating on industry and consumer blogs in order to distinguish the real brand, and further establish its identity; advertising to its consumers that only sites or online presence authorized by the company should be trusted; developing and distributing various relevant apps through official channels; and ensuring that all company websites, newsletters and other online presence are consistently up to date.

In addition, brand owners may wish to adopt a "co-opt and absorb" strategy. For example, they may wish to "authorize" online use of the brand by certain third parties, thus gaining the ability to monitor and impose conditions on how the brand is used. Brand owners can purchase selected websites, businesses or software and related intellectual property rights of entities using the brand without authorization. In some cases, businesses can offer employment to individual unauthorized online distributors of content bearing the brand.

Perhaps the strongest strategy for preventing and mitigating the negative effects of unauthorized uses of a business' brand is to actively monitor the online space and identify and challenge existing unauthorized uses. For example, businesses may focus on locating cybersquatters, misspelled domain names (typosquatting), and third-party search engine ads for their word mark or logo. To prevent attracting negative regulatory, third-party or reputation liability, brand owners should familiarize themselves with and use brand protection tools

offered by social media websites. They should also take advantage of the domain ownership challenge mechanism offered through the Uniform Domain Name Dispute Resolution Policy (UDRP), or, in Canada, the Canadian Dispute Resolution Policy (CDRP). Brand owners should formally advise potential consumers of the dangers of using unauthorized social media content bearing their brand. Finally, they should seek out and address all instances of trade-marked brand keywords being sold by search engines to unauthorized users.

### 3.2 The Risks – Identifying privacy-related risks of using social media

Active engagement in the social media context by brand owners offers strong advantages in terms of better controlling and protecting their brand in the online context. However, due to the nature of social media and of the online context, businesses using social media face a certain number of privacy-related risks. A business that wishes to adopt the use of any type of social media must be aware of and address the privacy issues before doing so.

Often, users of social media – including businesses – can misunderstand and underestimate the privacy risks of involved in using social media. The primary risk relates to failures to ensure notice, consent and reasonable purpose requirements are met for any collection, use and disclosure of personal information done in the course of social media use. If a business does not understand how those obligations, found under both PIPEDA and similar provincial legislations, translate into requirements in the online social media context, it may become exposed to liability under those laws.

Businesses using social media will inevitably collect personal information from the public. A company may choose to create an official Facebook page to promote its latest product, or create a Twitter profile to update its “followers” on upcoming savings, deals and marketing events. Through these media, the company may run contests, provide the public with an opportunity to sign up for newsletters or engage in other activities that require individuals to provide personal information. If individuals who participate in such activities provide their information without adequate notice of and consent to the purpose for which the information will be used and to whom it may potentially be disclosed, any use or disclosure of such information by the business may be in violation of PIPEDA or similar provincial laws.

Businesses may also face the risk of unauthorized or inappropriate disclosure of personal or confidential information to third parties, whether intentionally or not, through their social media page. Often, users of social media – including businesses – underestimate the scope of how much and how easily personal or confidential information can be disclosed on social media sites.<sup>38</sup> Much information posted on such services by users is freely available to the broad public; for example, any information that is posted by the owner or by members of a public Facebook page can be seen by anyone with access to Facebook. Similarly, information disclosed by individuals in the comments section of a business' blog is readily accessible and distributed – perhaps forever – to the Internet public, even though they may have been intended only for the smaller group of individuals who are members of the blog community. Once posted online, the information becomes difficult to control; third parties that would have access to it may disseminate or use it without the permission of either the poster or the business on whose social media site it is posted. Businesses receiving any personal information of individuals through the business' social media pages may thus be exposed to liability for failing to control its disclosure.

Finally, making social media part of a business' brand and marketing strategy involves risks of disclosure of personal information because of the individuals operating and monitoring the business' online activities. Businesses wishing to use the brand management and competitiveness-enhancing tools offered by social media will do so through assigning the task of setting up, monitoring and managing the business' social media presence to specific employees or teams. If such teams are not adequately educated and aware of the potential for unlawful collection and disclosure of personal information through social media, they may inadvertently improperly disclose information in their day-to-day operation of the social media sites.

---

<sup>38</sup> Office of the Privacy Commissioner of Canada, "Understanding Social Media Privacy Risks to Enterprises" (Power Point Presentation by Louisa Garib, Legal Services, Policy and Parliamentary Affairs). Available at: [http://www.priv.gc.ca/speech/2009/sp-d\\_20090430\\_ppt\\_e.pdf](http://www.priv.gc.ca/speech/2009/sp-d_20090430_ppt_e.pdf). Accessed on: August 25, 2010.

### 3.2.1 Managing the Risks – Navigating privacy law in the context of social media

Given the attractiveness of social media as a brand-management and business tool, companies can adopt a number of strategies to safely maximize their use of social media without engaging in conduct that could expose them to privacy-related liabilities.

*Understand the Privacy Risks.* Most importantly, businesses must ensure that they understand how the technology behind the relevant social media services works, as well as the potential privacy risks associated with their use of different social media. A company should look at whether any personal information is being or could be collected or disclosed in the course of using the particular social media service and, if so, would consent somehow be obtained from the concerned individual before this is done. As well, a business should consider whether the collection or disclosure of the expected type of information would be reasonable in the circumstances. For example, the collection of names and email addresses for a Facebook contest would likely be appropriate, as would the disclosure of the winner's name, while the disclosure of his or her email address would not.

*Obtain Informed Consent.* If personal information may potentially be collected through the company's social media presence, it should ensure that informed consent for such collection and the extent of permitted disclosure is obtained. In the example of a contest inviting potential consumers to submit personal information through the business' social media page, bringing a link to the company privacy policy to the attention of individuals providing personal information may suffice.

*Monitor for Potential Illegal Disclosure.* Due to the nature of social media, it may be inevitable that some personal information is made available on a company's social media pages, notably in the comments section of a blog or on the "wall" of a product Facebook page. In order to prevent unwanted dissemination of information that is not within the scope of any consent, the team in charge of managing the company's social media presence should engage in continuous monitoring of all its sites, in order to locate and remove any information that can be defined as "personal information". The company should create and provide to the social media team clear guidelines and best practices in this respect.

*Educate Employees.* The company's employees, in particular those that directly manage its social media presence, are key factors in mitigating any related privacy risks. To this end, the company should ensure these employees understand how all relevant social media platforms operate and the related privacy risks, in order to appropriately manage the company's social media presence. It would be appropriate for the company to implement policies setting out what can and cannot be posted on the company's social media sites, express policy guidelines on handling personal information in context of social media, as well as providing its employees with relevant social media training and detailed information about how privacy relates to social media. All policies regarding social media use by the company should be disseminated widely within the business. These policies should also be made to apply to all employees with regard to their personal use of social media while at work.

#### **4. Conclusion**

While social media services and practices continue to evolve, our understanding of privacy concerns and rules must develop at the same pace. Whether you are the operator of a social media service like Facebook, an advisor to an offline business seeking to leverage its brand and business through social media services or simply an individual user, an understanding of the challenges that online personal information use presents is crucial both now and in the future.