Blake, Cassels & Graydon LLP October 2010

Blakes Bulletin

Intellectual Property–Social Media Series

Privacy and Social Media: Challenges to Business

WENDY MEE

The privacy practices of many social media website operators have been, and continue to be, the subject of criticism from privacy regulators and the general public. In early 2010, the heads of the data protection authorities in 10 different countries, including Canada, sent a public letter to Google Inc. to express their concerns about privacy issues related to GOOGLE BUZZ, the company's then newly released social networking application.

More recently, the Canadian federal Privacy Commissioner, after completing an investigation commenced in 2008 into the privacy practices of Facebook, Inc., announced another investigation. The most recent investigation relates to the "Like" button on FACEBOOK. The "Like" button allows users to indicate which products, articles and other content on the Internet they like. Many users click on this button without realizing that their personal preferences will be distributed over the Internet for the purposes of attracting Internet traffic to the "Liked" site.

This article does not analyze the current privacy practices of social media website operators, which the Privacy Commissioner has acknowledged are "presenting ongoing challenges to privacy regulators around the globe". Rather, it considers privacy issues faced by organizations that use social media to promote their businesses, such as blogs for consumer feedback and company pages on third-party-operated social networking websites, and suggests ways to address these issues.

This article focuses on the privacy principles set out in the Canadian federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). Organizations that operate in Alberta, British Columbia or Quebec will also have to consider the private-sector privacy statutes in those provinces, which impose similar, though not identical, requirements as PIPEDA.

KNOWLEDGE AND CONSENT

One common criticism of social media website operators is that they collect, use and disclose personal information of users without their knowledge and consent. For example, one of the concerns raised by privacy regulators regarding GOOGLE BUZZ was that it "automatically assigned users a network of 'followers' from among people with whom they corresponded most often on GMAIL, without adequately informing GMAIL users about how this new service would work or providing sufficient information to permit informed consent decisions".

PIPEDA requires that personal information only be collected, used and disclosed with the knowledge and consent of the individual, subject to certain limited exceptions. In order for consent to be meaningful, individuals must be informed about how their personal information is collected, how it will be used by the organization, and to whom it may be disclosed.

While providing this information in a publicly available privacy policy or statement is required pursuant to PIPEDA's openness principle, this may not be sufficient in and of itself for the purposes of obtaining meaningful consent. The purposes for which the information is to be used should be brought to the attention of individuals at the time personal information is collected and consent obtained.

For example, if an organization requires users to register as a condition of the use of an interactive website or interactive section of its website, the purposes for which information provided during registration will be used and to whom it may be disclosed should be clearly explained at the time of registration.

In some circumstances, it may be appropriate to require users to read through a privacy policy or statement and to indicate their consent to the collection, use and disclosure of their personal information as described in such policy or statement, for example, by clicking an "I Accept" button, before permitting the user to participate in the social media platform.

Typically, consent should be obtained at the time of collection. However, if an organization makes material

CONT'D ON PAGE 2

©2010 Blake, Cassels & Graydon LLP

CONT'D FROM PAGE 1

changes to its personal information handling practices and would like to use and disclose personal information it has already collected for different purposes not previously identified, affected individuals should be notified and, where appropriate, a new consent obtained. Simply posting a revised privacy policy on an organization's website may not be sufficient where material changes are made.

LIMIT USE AND DISCLOSURE

Another common criticism of organizations generally, which may have particular relevance in the social media context, is that they often require individuals to consent to a use or disclosure of their personal information that is not necessary for the purposes for which the information is provided.

PIPEDA prohibits organizations from requiring individuals to consent to collection, use or disclosure of their personal information beyond what is necessary for the purpose for which the information was provided. Accordingly, care should be taken to ensure that any proposed use or disclosure of personal information that is not directly necessary to fulfil the social media purposes for which the personal information is being provided is clearly optional.

In relation to the example of registering on a website, if an organization would like to use the registration information for marketing purposes or to share email addresses of registered users with affiliates or other third parties, this should be made clearly optional, for example, by including an opt-out box on the registration page.

LIMIT COLLECTION

Organizations may only collect personal information that is necessary to fulfill the specific and legitimate purposes that are identified at the time of collection. A common complaint is that organizations require individuals to provide more personal information than is necessary to fulfill the identified purposes.

Again, with reference to the example of website registration, the registration form should not require a user to provide his/her telephone number or mailing address if all that is required to participate in an interactive website is an email address. However, provision of this information may be made optional, for example, if the individual opts-in to receiving marketing communications via these channels.

TERMS OF USE

One of the significant challenges faced by an organization engaged in social media is that it has little or no control over the information that gets posted on its page on another website, such as FACEBOOK. This has many legal implications, including from a privacy perspective.

Social media sites are governed by terms of service (TOS), which may also be referred to as terms of use, a user agreement or legal notice. The TOS should prohibit users from posting personal information of third parties and should allow the organization to remove material that may offend privacy legislation or the organization's privacy policy.

One key advantage to an organization of using its own social media platform, such as an interactive section on an organization's primary website or its own free-standing site, is that the organization has some control over the content posted and control over the TOS to ensure that the foregoing issues are addressed.

If the organization uses a social media platform provided by a third party, such as a corporate FACEBOOK page or TWITTER account, the organization will be governed by the third party's TOS and privacy policy. In such case, the organization should review the platform operator's TOS to ensure that the organization has some ability to remove or edit, or request the operator to remove or edit, offensive material. This may not be the case with all third-party social media platforms.

The privacy practices of many social media platform operators continue to be criticized by the general public and by privacy regulators around the world. Accordingly, an organization should ensure that it is comfortable with the personal information practices of third-party platform operators, and that these practices do not conflict with the organization's own policies and practices.

The foregoing is not intended to provide a comprehensive overview of the privacy issues raised by the use of social media. In order to minimize the risk that an organization will be identified in the press or be the subject of an investigation by a regulator based on a violation of privacy, it is important to think about these and other privacy issues that may be raised by an organization's use of social media.

©2010 Blake, Cassels & Graydon LLP

Blakes Bulletin
October 2010
Intellectual Property–Social Media Series

Employee Use of Social Media – Addressing the Risks

KATE MACARTNEY

There is no doubt that social media are very powerful tools in shaping an organization's image. Given the ability to share information quickly and with a wide audience, businesses are increasingly embracing social media by, for example, creating FACEBOOK pages to advertise products and to interact directly with their customers or clients, or using TWITTER to engage in public relations campaigns. However, organizations are not the only ones using social media.

By mid-2010, almost 50% of all Canadians were participating in FACEBOOK. Many of those users are also employees of businesses and other organizations. There are also numerous other social networking sites and other types of social media sites which allow employees to join, post, blog, comment, contribute and otherwise share information.

Given the ubiquitous nature of social media and the ease with which information can be created and shared, social media have provided employees with a greater ability to tarnish the reputation of employers and to expose employers to additional risks, whether the employees intend to or not.

RISKS OF EMPLOYEE SOCIAL MEDIA USE

In a 2009 survey of United States employees and companies, 74% of the employees surveyed agreed that it is easy to damage a company's reputation in social media.

However, 27% of employees said that they do not consider the ethical consequences of posting comments, photos or videos; 37% rarely or never consider what their boss would think; and 34% rarely or never consider what their customers would think. Moreover, 15% agreed that, if their employer did something with which they did not agree, they would comment about it online.

These employee attitudes can place the reputations of organizations, not to mention their confidential information, at risk. This risk is compounded by the fact that employees may believe that their personal social network pages or blogs to which they contribute are private and protected from public view. However, this is often not true.

In cases that have come before Canadian courts and tribunals where employees posted material online that could or did damage their employers' reputations, some of the employees were genuinely surprised to discover that their comments were available to the public at large. The employees often believed that their postings were only shared among a few close friends, which caused them to be more reckless in posting comments than they might otherwise have been.

ADDRESSING EMPLOYEE SOCIAL MEDIA RISKS

Given these risks, some employers may be tempted to simply block access to all social media sites so that employees cannot use them during work time. However, this is unlikely to be a workable solution for a number of reasons.

First, new sites are constantly being created and can be accessed from multiple devices, including hand-held devices, so it would be extremely difficult to block them all through all access points. Second, employees are able to access social media away from work and can post damaging material just as easily at home.

Furthermore, blocking access may have a damaging effect on employee morale as it sends a message that the employer does not trust its employees to use this increasingly important form of communication responsibly.

Instead, employers should develop and implement clear policies that specifically address their expectations of employees when they use social media and set out any limitations or restrictions on that use.

While the implementation of a policy cannot provide absolute protection against the risks outlined above, it will make employees aware of the effect their activities can have on the employer and that the employer expects them to act in a responsible manner when using social media.

GUIDELINES FOR EMPLOYEE SOCIAL MEDIA POLICIES

Employers should consider the following guidelines when creating and implementing a social media policy for employees:

- *Explain what social media is and what the policy covers:* The policy should make clear to employees what types of activities it applies to. The definition of

CONT'D ON PAGE 4

©2010 Blake, Cassels & Graydon LLP

CONT'D FROM PAGE 3

social media should be broad; while naming specific sites as examples can be helpful, the definition should not be limited to those sites as social media are constantly changing.

- *Remind employees about the nature of social media:* The policy should remind employees that any communication made through social media is or can become public, that the identity of anonymous contributors can often be revealed, and that postings can be difficult to rescind or delete.

- *Include non-work usages of social media:* The policy should make clear that it applies both to at-work usage, if permitted, and off-duty usage of social media. An employee's confidentiality obligations to its employer, for example, do not end as soon as the employee leaves work.

- *Remind employees that what they publish reflects both on themselves and the employer:* The policy should generally remind employees to exercise good judgment and prohibit the publishing of any comments that may negatively affect the employer.

- *Prohibit the violation of laws:* The policy should state that employees are legally responsible for their communication using social media and, as a result, should not violate any laws including those regarding human rights, defamation, copyright or other intellectual property rights, securities, financial disclosure and privacy rights, among others. Any applicable industry-specific laws should also be included in this list.

- *Prohibit the violation of employer policies:* The policy should reiterate that all other employer policies continue to apply to communications using social media. In particular, confidentiality policies and agreements apply to limit or prohibit the disclosure of certain information about the employer. The policy should also remind employees that seemingly innocuous or anonymized information could still breach confidentiality. In addition, codes of conduct and conflict of interest policies, among others, will continue to apply to limit improper behaviour.

- *Prohibit speaking on behalf of the employer:* The policy should clearly state that, unless authorized to do so, employees should not speak on behalf of the employer. Employers should also consider requesting that employees post disclaimers when they make comments in social media to the effect that their views are theirs alone and do not reflect the views of the employer.

- *Advise that revisions may be requested:* The policy should notify employees that, in appropriate circumstances, the employer may request revisions to, or the removal of, certain social media communications.

- *Consider including specific rules regarding the use of social media in a business capacity:* If the employer is considering appointing an employee or various employees to use social media on behalf of the employer, it should set out specific rules regarding this role. These rules may vary based on the employer's intended use of social media; however, any industry-specific rules, such as restrictions on disclosure or advertising, should be referenced.

- *Advise that the employer will monitor employee usage of social media while at work, if applicable:* If the employer will monitor employees' use of social media, which it may already do through monitoring employee Internet usage, the employer should disclose this to its employees and advise that they have no reasonable expectation of privacy with respect to their use of the Internet through employer systems.

- *Advise of the consequences of a breach:* The policy should provide that discipline up to and including termination of employment may result if an employee breaches this policy. A policy is only as good as its enforcement so the employer must be prepared to follow through with disciplinary action in order to ensure that its employees comply with this policy.

CONCLUSION

There is no absolute way to protect employers from the risks associated with employees' use of social media. However, an employee policy that educates employees about the nature of social media and sets out clear expectations of employee conduct when using social media can go a long way in managing these risks.

Go to **blakes.com/english/subscribe.asp** to subscribe to other Blakes Bulletins.

MONTRÉAL OTTAWA TORONTO CALGARY VANCOUVER
NEW YORK CHICAGO LONDON BAHRAIN AL-KHOBAR* BEIJING SHANGHAI* **blakes.com**
* Associated Office

Blakes periodically provides materials on our services and developments in the law to interested persons. If you do not wish to receive further bulletins, please click **here**. For additional information on our privacy practices, please contact us at **privacyofficer@blakes.com**. *Blakes Bulletin* is intended for informational purposes only and does not create a lawyer-client relationship. The transmission of this information does not suggest Blakes or any of its lawyers are practising law of any jurisdiction other than Canada. The information provided in this bulletin is summary in nature and does not constitute legal advice. We would be pleased to provide additional details or advice about specific situations if desired. For permission to reprint articles, please contact Blakes Marketing Department at 416-863-2403 or **lynn.spencer@blakes.com**.©2010 Blake, Cassels & Graydon LLP.