CANADIAN PRIVACY LAW REVIEW

Volume 10 • Number 6 May 2013

In This Issue:

LexisNexis®

Security Breach Notification Soon Becoming Mandatory in Canada

Éloïse Gratton
Partner and National Co-chair, Privacy
McMillan LLP

Businesses are not protected from such incidents as forgetting documents or devices containing personal information in a public place, sending business correspondence to the wrong destination, insecurely storing material containing personal information by a service provider mandated to destroy it, or suffering from loss and theft of confidential documents. Security breaches leading to loss of personal information or to unauthorized access, use, or disclosure may be triggered by a problem in the information technology system of an organization, by a simple error, or human negligence.

With security breaches being on the rise, the requirement to have organizations notify the relevant privacy commissioners and affected individuals upon a security breach taking place is becoming increasingly important. Individuals, once notified, will be in a better position to address the potential risks of harm resulting from such breaches. For instance, if they are aware of the fact that their financial information has been compromised or disclosed to an unauthorized third party, they will ensure to monitor their banking statements and credit scores.

In Canada, the federal *Personal Information Protection and Electronic Documents Act*[1] sets out ground rules for how private-sector organizations may collect, use, and disclose personal information in the course of commercial activities. The federal government may exempt organizations or activities in provinces that have their own data protection laws if they are substantially similar to the federal law. The provinces of British Columbia, Alberta, and Quebec have enacted their own provincial data-protection laws, which have been recognized as substantially similar to *PIPEDA*. Therefore, these provincial data-protection laws operate in place of *PIPEDA* in those three provinces for intraprovincial matters.

Canadian Privacy Law Review

The **Canadian Privacy Law Review** is published monthly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Suite 700, Markham, Ont., L3T 7W8, and is available by subscription only.

Web site: www.lexisnexis.ca

ISBN 0-433-44417-7 ISSN 1708-5446
ISBN 0-433-44418-5 (print & PDF)
ISBN 0-433-44650-1 (PDF)
ISSN 1708-5454 (PDF)

Subscription rates: $255.00 (print or PDF)
$395.00 (print & PDF)

So far, Alberta is the only Canadian jurisdiction that has made general purpose security breach notification mandatory. However, it seems like things are about to change in other Canadian jurisdictions. In Quebec, the Commission d'accès à l'information du Québec ("CAI") in its 2011 Quinquennial Report entitled *Technology and Privacy, in a Time of Societal Choices*[2] recommends to include mandatory security breach reporting in both its public sector and private sector data protection laws.

At the federal level, a first attempt in proposing to amend *PIPEDA* to include a breach notification obligation was initially introduced through Bill C-29 in May 2010. However, this bill died when the election was called in spring 2011. Bill C-12, which was identical to C-29, was then introduced in September 2011 but has not been moved forward.

Thankfully, an even better proposal, which has received the support of various industry players such as Openmedia.ca, the Union des consommateurs, and the Canadian Internet Policy and Public Interest Clinic ("CIPPIC"), has now been introduced by NDP Member of Parliament Charmaine Borg last February. The private member's Bill C-475, *An Act to amend the Personal Information Protection and Electronic Documents Act (order-making power)*,[3] adds clear and mandatory security breach disclosure requirements to the federal law *PIPEDA* along with new order-making power backed by significant penalties for compliance failures.

Under such proposed Bill C-475, an organization having personal information under its control would have to notify the Commissioner of any incident involving the loss, disclosure of, or unauthorized access to, personal information, where a reasonable person would conclude that there exists a possible risk of harm to an individual as a result of the security breach. The notification would have to be made without unreasonable delay after the discovery of the breach. Upon the receipt of the notification, the Commissioner may require the organization to notify without unreasonable delay affected individuals to whom there is an appreciable risk of harm as a result of the breach (although nothing would preclude an organization from notifying affected individuals of the breach on a voluntary basis). The notification to the affected individuals of the loss, disclosure of, or unauthorized access to their personal information would have to include a report of the risk of harm as it pertains to the affected individuals as well as instructions for reducing the risk of harm or mitigating that harm.

Until these proposed amendments are incorporated in the current Quebec public and private sector data protection laws and *PIPEDA*, both jurisdictions have adopted security breach guides. More specifically, the Quebec CAI has made available on its website a document entitled *Que faire en cas de perte ou de vol de renseignements personnels?*,[4] and the federal Office of the Privacy Commissioner has also adopted a guide entitled *Keys Steps in Responding to Privacy Breaches*,[5] which provides guidance for businesses on how to handle these breaches.

Mandatory security breach reporting is crucial, as it can serve to strengthen public confidence in the public bodies and businesses that hold personal information and can allow the respective privacy commissioners to better play their oversight roles. Notification can also be an important mitigation strategy that has the potential to benefit both the organisation and the individuals affected by a security breach.

---

1 S.C. 2000, c. 5 [*PIPEDA*].

2 <http://www.cai.gouv.qc.ca/documents/CAI_RQ_2011_res_eng.pdf>.

3 <http://parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=6000116>.

4 *Loss or Theft of Personal Information: How Should You React?*, <http://www.cai.gouv.qc.ca/documents/CAI_FI_vol_rens_pers_citoyen_eng.pdf>.

5 <http://www.oipc.ab.ca/Content_Files/Files/Publications/Key_Steps_in_Responding_to_a_Privacy_Breach.pdf>.

Social Media Background Checks in Canada: Do the Risks Outweigh the Rewards?

Lyndsay A. Wasser
Partner
McMillan LLP

Background checks are an important tool for employers to assess the suitability of candidates for employment opportunities within the organization. Social media checks, in particular, can provide a lot of useful information respecting whether a candidate (1) presents himself or herself professionally, (2) is a good fit for the company's culture, (3) has the right qualifications for the position, and (4) is generally a well-rounded person.

If social media checks provide such useful information, why is the number of employers performing such checks decreasing instead of increasing?[1]

The decline in social media checks on prospective employees may reflect an increased awareness of privacy laws and other legal risks associated with such activities. In Canada, there are four jurisdictions that have specific privacy legislation that restricts the ability of employers to perform background checks on employees or prospective employees (collectively the "Privacy Statutes"):

Federally regulated employers	The *Personal Information Protection and Electronic Documents Act*[2]
Employers in Alberta	The *Personal Information Protection Act*[3]
Employers in British Columbia (B.C.)	The *Personal Information Protection Act*[4]
Employers in Quebec	*An Act Respecting the Protection of Personal Information in the Private Sector*,[5] the *Civil Code of Québec*,[6] and the *Charter of Human Rights and Freedoms*[7]

There are differences between the Privacy Statutes; however, they contain some common features that have the effect of restricting or prohibiting social media checks. For example, the Privacy Statutes require that organizations (1) provide notice or obtain consent prior to collecting an individual's personal information; (2) limit their collection of personal information to that which is necessary for reasonable purposes; and (3) take reasonable steps to ensure that information collected is accurate, complete, and up to date. Although some exemptions exist in the Privacy Statutes for "publicly available" information, this term is specifically, narrowly defined[8] and would not cover much of the information that would be collected via a social media search.

An employer may be able to satisfy the first requirement listed above (notice/consent); however, the other two requirements are likely to be problematic in most cases. First, social media checks reveal a wide variety of information about the job candidate and third parties (such as Facebook "friends," Twitter "followers," or persons who have a name similar to the candidate). Unlike with traditional background checks, it is difficult, if not impossible, to control the amount of information collected to only reasonable and necessary facts. In addition, information available on the Internet may be incorrect, falsified, or outdated, impacting the organization's ability to ensure that all information collected is accurate, complete, and up to date.

In jurisdictions other than those listed above, there are fewer restrictions upon an organization's ability to conduct social media background checks on employees or prospective employees. However, all individuals have some privacy rights in every Canadian jurisdiction. In the recent case of *Jones v. Tsige*,[9] the Ontario Court of Appeal created the tort of "intrusion upon seclusion," as follows:

> One who intentionally [or recklessly] intrudes, physically or otherwise, upon the seclusion of another or his [or her] private affairs or concerns, is subject to liability to the other for invasion of his [or her] privacy, if the invasion would be highly offensive to a reasonable person.[10]

Although there is no case law on this issue to date, it is likely that a simple Google or Facebook search on a job candidate, revealing information that is not restricted or password protected, would not satisfy this test. However, employers that take more invasive or deceptive actions (*e.g.*, by demanding candidates' social media passwords, attempting to circumvent password protections to hack into candidates' accounts, or misrepresenting themselves in order to be accepted as a "friend") could face claims of "intrusion upon seclusion."

Furthermore, in all Canadian jurisdictions, social media searches increase the risk of human rights complaints. Human rights legislation across the country prohibits discrimination on the basis of the following characteristics: social condition, source of income, political beliefs, criminal conviction, mental or physical disability (including drug/alcohol addiction), family status, marital status, gender identity/expression, sexual orientation, pregnancy/childbirth,

sex/gender, age, religion/creed, nationality/citizenship, national/ethnic/place of origin, ancestry, and race/colour.

A social media search has a high probability of revealing information about one or more of these protected characteristics. If a candidate is not hired after this type of information has been collected, the candidate could allege that the organization's decision to refuse employment was based, at least in part, on the protected characteristic. Even if the allegation is false, the organization will be put into the position of having to defend its decision as well as incurring the costs and inconveniences of defending against a human rights complaint.

Given the risks associated with social media background checks, employers would be well advised to carefully consider whether such searches are necessary to achieve their goals. In many cases, the information needed to assess a candidate's suitability for employment can be obtained through more traditional means, such as interviews, reference checks, and criminal background checks. Although there are also laws applicable to traditional types of background checks (which should be taken into consideration before the checks are undertaken), these checks generally give employers more control over the amount and type of information they collect.

For federally regulated employers and employers in Alberta, B.C., and Quebec, it would be prudent to avoid social media checks altogether due to the difficulty of ensuring compliance with the Privacy Statutes.

In other jurisdictions, employers that feel the need to conduct social media checks should take the following steps to minimize the risks:

- Obtain candidates' prior consent to the check or at least provide advance notice.
- Conduct the check only after a conditional offer of employment has been made.
- Limit the check to information that is available to the public and do not demand or attempt to circumvent passwords.
- Ensure that hiring managers/human resources persons are properly trained on human rights laws as well as how they should conduct the checks and use the information obtained to make sure they limit the checks as much as possible to what is reasonable in the circumstances and consider only the information relevant to assessing a candidate's suitability for the position (without consideration of any characteristic protected by applicable human rights laws).
- Document the reasons for not hiring a candidate.
- Retain the information (securely) for the time period necessary to respond to access requests, intrusion upon seclusion claims, or human rights complaints.

These steps may not eliminate the risk of a human rights or privacy complaint; however, they can put the employer in a better position to defend against such claims.

At the end of the day, employers must weigh the risks of social media checks against the potential rewards to determine if it is worthwhile for such checks to form a part of their hiring processes.

[*Editor's note*: This article was prepared for a presentation at the Canadian Corporate Counsel Association (CCCA) Spring Conference in April 2013.]

---

1 Nancy Messier, "Survey: Thirty-Seven Per Cent of Your Prospective Employers Are Looking You Up on Facebook," *The Next Web*, April 18, 2012, <http://thenextweb.com/socialmedia/2012/04/18/survey-37-of-your-prospective-employers-are-looking-you-up-on-facebook/>.

2 S.C. 2000, c. 5.

3 SA 2003, c. P-6.5.

4 S.B.C. 2003, c. 63.
5 R.S.Q., c. P-39.1.
6 LRQ, c C-1991.
7 R.S.Q., c. C-12.
8 *An Act Respecting the Protection of Personal Information in the Private Sector* exempts personal information, which "by law is public" as opposed to "publicly available." There is no definition of information that "by law is public" in the statute itself, but the meaning of this term under Quebec law is also narrow.
9 [2012] O.J. No. 148 (Ont. C.A.).
10 *Ibid*. at para. 19.

Private and Confidential: *Steel v. Coast Capital Savings Credit Union*

Alison Strachan
Staff Lawyer
Stewart McKelvey

> [The employer] had to trust Ms. Steel to only access such documents as part of the performance of her duties and to follow the protocols when she did so. Such trust was fundamental to the employment relationship in relation to Ms. Steel's position.

So concludes the court in *Steel v. Coast Capital Savings Credit Union*,[1] a recent decision that will be of interest to employers who place a high expectation on employees to ensure the privacy and confidentiality of their clients.

Ms. Steel was employed by Coast Capital for more than 20 years, most recently as a Helpdesk analyst in the IT Department. Her duties included providing internal technical assistance to other employees of Coast Capital when they experienced trouble with the network. As Helpdesk analyst, Ms. Steel had access to any document or file in the organization. Her work was unsupervised, and no one monitored what documents she accessed or for what reason or purpose. Why? It would not be practical. Although the position was not managerial, the job description required that the analyst "respect the privacy and confidentiality of all customer and staff information at all times."

What Did Ms. Steel Do That Was Wrong?

Ms. Steel could access employee personal folders when assisting with technical problems. Access, however, was to be made only after the employee had given permission, or the VP of corporate security had authorized it. The Helpdesk analyst was expected to follow a specific protocol. During her annual review process, Ms. Steel acknowledged that she had reviewed, understood, and signed off on the *Acceptable Use Policy*, *Code of Conduct Policy*, and *Information Confidentiality Policy*. Yet, after this review, Ms. Steel accessed a spreadsheet in a coworker's personal file that contained confidential employee information including pay grades and seniority dates.

As a result of the investigation, Ms. Steel was terminated on a "with cause" basis. In its termination letter to Ms. Steel, Coast Capital said that the "severity of this breach of trust has led Coast Capital Savings to lose faith in [her] judgement. It has resulted in a serious loss of confidence in [her] which [they] believe has irreparably damaged the employment relationship."

What Happened Next?

Ms. Steel sought summary judgment in an action for damages for wrongful dismissal, saying that even if the employer's version of events were true, the alleged conduct did not amount to just cause for dismissal. Coast Capital agreed that the issue could be resolved at summary dismissal and that evidence Ms. Steel had provided during discovery was not in conflict with the facts giving rise to the dismissal. The court agreed that it could dispose of the matter, and it did—in favour of the employer.

What Did the Court Note Was Key?

There are some key points of this decision that should not be overlooked. If they had not existed, the employer may have had a more difficult time asserting just cause. What made this case different?

- The relationship of trust is particularly critical in the banking industry where employees are held to a higher standard of trust than employees in other undertakings.
- Employees who work with greater autonomy are held to a higher standard of trust—the greater the autonomy the employee enjoys, the more fundamental trust is in the employment relationship.

Madam Justice Ross relied on these circumstances in finding cause to dismiss, saying:

> Ms. Steel occupied a position of great trust in an industry in which trust is of central importance. In her position [she] was given the ability to access confidential documents. The employer established clear policies and protocols known to Ms. Steel at the relevant time that were to govern access to confidential documents.[2]

Ms. Steel knew that to remotely access other employee's files without first receiving specific permission to do so was forbidden. In her role, it was not practicable for Coast Capital to monitor what she accessed and for what purpose. The court noted that the "trust" fundamental to her position was broken and that her actions amounted to just cause for dismissal.

What Does This Mean for Employers?

If you expect privacy and confidentiality from employees, you should have and maintain policies dealing with access to information within your computer system. This is more critical in industries where trust is of central importance (*e.g.*, banking or healthcare) and particularly necessary where an employee has unsupervised access to the system. In your annual review process, review those policies and ensure there is acknowledgement by employees that they are aware of them. This issue will usually only arise when someone complains. Consider whether there are proactive ways to monitor access (*e.g.*, by way of routine audits or by requiring a log book to be submitted each day, detailing access and providing consent information for that access). In many workplaces, it will be impractical to impose such a system. There is no doubt that if you are going to take privacy and confidentiality seriously, any report of questionable access should be properly investigated. Likewise, if an employee is determined to be in violation of your policies, apply your policy evenly and consistently when discipline is warranted.

---

1 [2013] B.C.J. No. 593 at para. 27 (B.C.S.C.).
2 *Ibid*. at para. 26.

B.C. Investigation Shines Light on Personal E-mail and Records Management

Timothy M. Banks
Partner
Dentons

On March 18, 2013, the British Columbia Information and Privacy Commissioner ("OIPBC") announced an investigation into the use of personal e-mail accounts by public servants in that province. The investigation is shining a light on problem of using personal e-mail in the public service. However, the issues identified by the OIPBC go further. They are also relevant for organizations in the private sector.

Records Management Obligations

The use of personal e-mail for business is a significant problem for records retention and privacy programs.

Communications taking place outside of the organization's e-mail records management system may not be captured in compliance with the organization's records management system. The OIPBC reminds public servants in *Guidelines on the Use of Personal Email Accounts for Public Business*[1] that personal e-mail may still be subject to the British Columbia *Freedom of Information and Protection of Privacy Act* [*FIPPA*].[2]

FIPPA applies to records in the custody or control of a public body. A record will be under the control of the organization if (a) the record relates to a departmental matter and (b) the government institution could reasonably expect to obtain a copy of the record upon request. The OIPBC's general rule is that "any email that an employee sends or receives as part of her or his employment duties will be a record under the public body's control, even if a personal account is used."[3] These records may, therefore, be subject to access to information requests even though the organization does not have possession of the e-mail record.

This is not just a public sector problem. For example, subs. 23(1) of the British Columbia *Personal Information Protection Act* [*PIPA*],[4] which applies to private sector organizations in British Columbia, provides that an organization must provide an individual with the individual's personal information under the control of the organization. There is no obvious reason why the meaning of "control" in *PIPA* should be narrower than that in *FIPAA*.

Information Security Obligations

The OIPBC also expressed concern regarding the security of personal e-mail in the Guidelines. This issue applies equally to the public and private sectors. Depending on the service used by the employees and whether copies of the e-mail are downloaded to unencrypted devices, the e-mail may be stored in an insecure environment.

Private organizations should be aware that s. 34 of *PIPA* requires the organization to protect personal information in its custody or under its control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal, or similar risks. Organizations may be faulted for turning a blind eye to the practice of employees using personal e-mail systems that do not provide for adequate security. In assessing the risk, organizations should consider whether they would have breach notification responsibilities in the event an employee's personal e-mail was compromised and that e-mail contained personal information collected by or on behalf of the organization.

Even leaving aside the possibility of a breach, organizations should consider whether employees transmitting personal information outside of the administrative, technical, and physical security controls established by organization would violate representations made by the organization in its public privacy policies.

---

1 OIPBC, *Use of Personal Email Accounts for Public Business*, March 18, 2013, <http://www.oipc.bc.ca/tools-guidance/guidance-documents.aspx> ("Guideline").

2 R.S.B.C. 1996, c. 165 [*FIPPA*].

3 Guideline, p. 2.

4 S.B.C. 2003, c. 63 [*PIPA*].