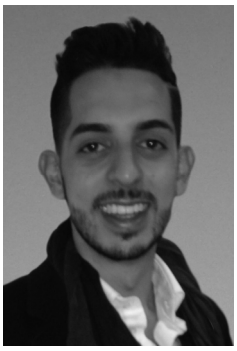
CANADIAN PRIVACY LAW REVIEW

Volume 11 • Number 11 October 2014

In This Issue:

Limited Protection of Dependents' Personal Information in Group Insurance Matters



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

Christian Abouchaker
Student-at-Law
McMillan LLP

A group insurance policy often involves several parties—namely the insurance company, the employer (or association/affinity/creditor), the third-party administrator, and the insured employee (or "member" of the plan), who rarely has any negotiating power in this regard. In addition, it is often the case that a member's dependents are eligible for benefits under the policy.

Administering a group insurance plan requires the disclosure and communication of various types of personal information that can be quite sensitive in nature. The information that must be submitted in order to be eligible for the benefits generally consists of medical information and, potentially, in the case of a member's dependents, of other personal information that they might be reluctant to disclose to the member. An example would be when a teenage girl elects to take contraceptives but doesn't want her father, the member, to learn about it, or when a dependent's spouse doesn't want the member to know that he or she is being treated for a sexually transmitted disease, or for depression.

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: $265.00 (print or PDF)
$405.00 (print & PDF)

Under both the federal statute on the protection of personal information (*i.e.*, the *Personal Information Protection and Electronic Documents Act* [*PIPEDA*][1] and the various substantially similar provincial privacy statutes, the basic underlying principle is that every person must have the opportunity to consent to the collection, use and disclosure of personal information. In this regard it is interesting to note that in two recent decisions—one by Quebec's access to information commission, the *Commission d'accès à l'information du Québec* (the "CAI") and the other by the Office of the Privacy Commissioner of Canada (the "OPCC")—limits were placed on the level of privacy that is afforded to a dependent in the context of group insurance.

Quebec Decision

In Quebec, the CAI recently took the position[2] that an insurance company could disclose personal information that is necessary for the administration of the group insurance plan, without having to obtain the dependent's consent, to a member, in connection with a claim made by that member's dependent.

In the matter in question, the plaintiff alleged that without his consent, the insurance company had disclosed his personal information to his common law spouse, a member of the group insurance plan. The plaintiff considered this disclosure to be a violation of his privacy rights—particularly because under *An Act respecting prescription drug insurance*,[3] he was, as a dependent, obliged to obtain coverage under his spouse's group insurance, thereby forfeiting his coverage under the public drug insurance plan. In its defense, the insurance company argued that the information disclosed was necessary for the member to properly administer her insurance plan, particularly with respect to co-insurance and the application of the amount of the deductible. The insurance company pointed out that it had to verify several details before approving a claim, including eligibility, the amount of the deductible, the extent of coverage, *etc*. It should be noted that in this case, the insurance policy provided that reimbursement of the claim was to be paid directly to the member.

In Quebec, *An Act respecting the protection of personal information in the private sector* (the "Quebec Privacy Law")[4] provides that any information concerning an individual that allows that person to be identified is personal information. Thus, the information about the plaintiff appearing on the reimbursement statement sent to the member constituted personal information of the dependent as understood by the Quebec Privacy Law. That legislation also provides that no one may disclose personal information contained in a file maintained in respect of an individual to a third party, or use such information for purposes unrelated to the reason the file is being maintained, unless the individual in question consents or such disclosure is required by the Quebec Privacy Law. Moreover, consent to the disclosure must be "manifest, free, and enlightened, and must be given for specific purposes".[5]

The contract with the insurance company in this case was on behalf of the member, not the plaintiff. Thus, while the CAI sympathized with the plaintiff's objection to the disclosure of his personal information to the member, it concluded that his case was not well founded. The insurance company had simply disclosed (to the member) information that was necessary for the administration of the contract, and did not contravene the Quebec Privacy Law.

Decision under *PIPEDA*

At the federal level, the approach taken by the OPCC appears to be similar. In a recent Report of Findings[6] pursuant to *PIPEDA*, the OPCC dismissed the case of a young woman who, as a dependent under her father's group health insurance plan, contested the plan administrator's policy of requiring her to submit claims through her father.

The plaintiff alleged that the insurance company's refusal to process her claims directly and its disclosure of personal information concerning her to her father constituted a breach of *PIPEDA* Principle 4.3.3 set out in Schedule 1 of that statute, which provides that an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill explicitly specified and legitimate purposes. In its analysis, the OPCC took into account the rights and responsibilities of plan members and their dependents.

The members of a group health insurance plan often bear sole responsibility for all claims made and are accountable for errors, abuse, or fraud stemming from those claims. The OPCC noted that the insurance company's practice of refusing to deal directly with a member's dependent thereby compelling the disclosure of the dependent's personal information to the member complied with Principle 4.3.3. In the OPCC's view, because a dependent under the plan has none of the same responsibilities as the member has in respect of the plan, dependents cannot expect absolute protection of their personal information and must consent to its disclosure to the plan member. While it recognized the legitimacy of the complainant's concerns, the OPCC, in concluding that the dependent's complaint was not well founded, also took into account the plan's structure and other practical considerations.

Conclusion

These two decisions are welcome news for employers: They impose only limited obligations with regards to dependents in group insurance matters, allowing employers to manage claims through the intermediary of a single person (*i.e.*, the member) and authorizing them to disclose personal information regarding the member's dependents to the member if the information is deemed necessary for the administration of the group insurance plan, without having to obtain the dependent's consent. However, the effect of these decisions is to provide

only limited protection to the personal information of a member's dependents. While this may cause some inconvenience to the dependents who wish to keep their purchases of medication private, this limitation on their privacy rights has now been deemed acceptable by two Canadian privacy commissioners when personal information must be disclosed to a member for claims management purposes.

---

1 S.C. 2000, c. 5.
2 *X. et La Capitale assurance et gestion de patrimoine*, Commission d'accès à l'information du Québec, June 21, 2013.
3 CQLR c. A-29.01.
4 CQLR c. P-39.1.
5 *Ibid*., s. 14.
6 *PIPEDA* Report of Findings # 2013-012, *Adult daughter required to submit insurance claims through her father and consent to disclose personal information to her father upon claiming benefits from his private health insurance plan*, Office of the Privacy Commissioner of Canada, 2013 CanLII 92363 (OPCC).

Europe Not Yet Satisfied with Adequacy of Quebec's Privacy Law

Timothy M. Banks
Partner
Dentons Canada LLP

On June 4, 2014, the Article 29 Working Party ("WP 29") issued a report[1] to the European Commission ("EC") regarding an application by the Province of Quebec, Canada, for status as a jurisdiction providing an adequate level of protection for the purposes of transfer and processing of personal data from the European Union. WP 29 is made up of representatives of European Union member states. The report is significant not only because WP 29 questioned the jurisdictional scope of the Quebec legislation but also because it has raised concerns regarding certain limitations in Quebec's scheme of protection for personal information.

Jurisdictional Dispute

WP 29's first concern was regarding the territorial scope of Quebec's *An Act respecting the protection of personal information in the private sector* (the "Quebec Act").[2]

In an attempt to thwart a constitutional challenge, the federal *Personal Information Protection and Electronic Documents Act* [*PIPEDA*][3] contains a mechanism[4] to cede jurisdiction over an organization in favour of provincial legislation if that province enacts legislation that is declared to be substantially similar to *PIPEDA*. The Quebec Act was declared substantially similar in 2003, resulting in a constitutional détente (although there remains an outstanding judicial proceeding regarding the constitutionality of *PIPEDA*).[5]

Even though the Quebec Act has been declared substantially similar, there is some uncertainty regarding the effect of that declaration. On one interpretation, provincial legislation, such as the Quebec Act, applies only to the collection, use and disclosure of information *within* the province. Collection, use and disclosure across provincial borders, or internationally, remain to be subject to *PIPEDA*. However, another interpretation, which was adopted by the Commission d'accès à l'information du Québec in its application for recognition, is that organizations must comply with both statutes if the collection, use or disclosure of personal information cross provincial boundaries.

WP 29 noted the apparent disagreement regarding the scope of the Quebec Act and stated that further clarification was required.

Substantive Concerns

WP 29 also raised substantive concerns with the adequacy of the Quebec Act. In doing so, WP 29

compared and contrasted the Quebec Act with *PIPEDA*. WP 29's concerns seem to reflect a preference for more precise legal drafting rather than any concern regarding how the Quebec Act is interpreted and applied in practice by the Commission d'accès à l'information du Québec.

- **Transparency.** The Quebec Act, unlike *PIPEDA*, does not provide for the disclosure of the contact information of a person who is accountable for the privacy practices of the enterprise, frequently referred to as a Privacy Officer. WP 29 recommended that the contact details of the person carrying on an enterprise be disclosed to the person from whom information is being collected in order to satisfy the transparency principle.
- **Access Rights.** WP 29 was concerned that access to personal information in Quebec may be limited. WP 29 noted that art. 39 of the *Civil Code of Quebec* permits the withholding of access and the refusal to correct where the enterprise has a serious and legitimate reason for doing so or if the information is of a nature that may seriously prejudice a third person. In contrast, *PIPEDA* requires an organization to grant an individual access to his or her personal information except in very limited circumstances.
- **Onward Transfers.** WP 29 was concerned that the Quebec Act did not require contractual provisions as a mandatory requirement to protect personal information transferred to third parties, even though the Quebec Act provides that an enterprise shall take all reasonable steps to protect the information. It would appear that WP 29 was concerned that this could be interpreted as a standard permitting transfers without binding provisions to ensure a comparable level of protection to the Quebec Act.
- **Sensitive Information.** WP 29 also raised concerns regarding the absence of a specific definition of sensitive data. WP 29 noted that *PIPEDA* also lacks a definition of sensitive data. The Canadian approach is to assess the sensitivity of information by reference to the context in which it is collected, used and disclosed. Data may be more or less sensitive depending on how it is used and combined with other information. Evidently, WP 29 would prefer greater specificity around what constitutes sensitive information.

The WP29's report is now before the EC. Given the overall state of flux in Europe as the member states consider the proposed European Data Protection Regulation, we are unlikely to see further action on the Quebec application in the near term.

---

1 The Article 29 Working Party, *Opinion 7/2014 on the Protection of Personal Data in Quebec*, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp219_en.pdf>.
2 CQLR, c. P-39.1.
3 S.C. 2000, c. 5.
4 *Ibid*., s. 26(2)(*b*).
5 *PIPEDA, Organizations in the Province of Quebec Exemption Order*, SOR/2003-374.

Evans v. The Bank of Nova Scotia: Another Case of Intrusion upon Seclusion Is Certified as a Class Action

Erica Maidment
Associate
Gowling Lafleur Henderson LLP

The new tort of "intrusion upon seclusion" that provides a cause of action to those whose privacy has been breached was given new teeth this month by the certification of a class action against The Bank of Nova Scotia (the "Bank") and its

employee, Richard Wilson in *Evans v. The Bank of Nova Scotia* [*Evans*].[1]

Facts

The central allegations are that Mr. Wilson, a Mortgage Administration Officer employed by the Bank, decided to print out and give his customers' confidential information to his girlfriend. His girlfriend then distributed this information to individuals who used it to commit identity theft and fraud. The scam was exposed by the Calgary Police in May 2012 when the police found profiles belonging to the Bank's customers in the course of executing a search warrant against individuals suspected of fraud in Alberta. Mr. Wilson confessed to improperly accessing and printing personal customer profiles for individuals who applied for mortgages from November 2011 until the end of May 2012 and to delivering them to third parties.

The Bank identified 643 customers whose files were accessed. The Bank gave those customers notice that it was possible that there had been unauthorized access to their confidential information and offered free credit monitoring and identity theft protection. As of the date of the hearing, 138 of those customers had notified the Bank that they have been the victims of identity theft or fraud, and the Bank provided them with compensation for their pecuniary losses.

The 643 customers, known as the "Notice Group", sued the Bank and Mr. Wilson for damages in negligence, breach of contract, breach of fiduciary duty, breach of good faith, and under the new tort of intrusion upon seclusion, claiming damages for emotional suffering, hardship, inconvenience, and waiver of tort. The Ontario Superior Court of Justice (the "Court") certified the Notice Group's class action for intrusion upon seclusion and waiver of tort, in addition to the Bank's alleged breach of contract with those customers and negligent supervision of its employee.

Intrusion upon Seclusion

Jones v. Tsige [*Jones*][2] established a tort in Ontario for the intentional or reckless invasion of the privacy of another individual without lawful justification. The harm from such an invasion of privacy must be such that "[a] reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish."[3] The Court of Appeal in *Jones* indicated that "a modest conventional sum"[4] of damages would be appropriate and that the appropriate range of damages would be up to $20,000. In *Jones*, the plaintiff, Jones, and the defendant, Tsige, were two employees of Bank of Montreal, working at different branches. Tsige became romantically involved with Jones's ex-husband and began probing Jones's financial information by way of her access as an employee of the bank. Jones was granted summary judgment against Tsige for $10,000.

The question in *Evans* was whether the Bank was vicariously liable for Mr. Wilson's actions, which were arguably worse than Tsige's, because he disclosed the information to a third party. The Court went back to the first principles of vicarious liability from *Bazley v. Curry*.[5] The key factor that decided this issue was that the Bank created the opportunity for Mr. Wilson to abuse his power by having unsupervised access to customers' private information. It did not matter that the Bank was not itself involved in the improper conduct. It also did not matter that the damages for the tort of intrusion upon seclusion are symbolic or moral damages; the Court found that it was not plain and obvious that the Bank was not vicariously liable:

> The tort of intrusion upon seclusion has only recently been recognized by the Ontario Court of Appeal and is settled in Ontario. However, until the matter is ultimately decided at the Supreme Court of Canada, I find that the law in Canada is not settled on this issue.[6]

The cause of action has yet to be considered by the Supreme Court of Canada, and not all provinces

have established the tort as a cause of action. British Columbia courts have refused to acknowledge a tort of breach of privacy that is independent of privacy legislation.[7]

However, this is not the first time that the tort of intrusion upon seclusion has been certified as a common issue in a class action. In March 2014, the Federal Court certified a class action in *Condon v. Canada*[8] partly on the basis of intrusion upon seclusion. The case involved the loss of confidential student information on an external hard drive collected for the Canada Student Loans Program by the Government of Canada. As in *Evans*, the Federal Court determined that it was not plain and obvious that a claim on the basis of the new tort would fail.

Damages

The Bank in *Evans* challenged the plaintiffs' claim for damages for emotional distress, because the plaintiffs had not demonstrated that the harm to them rose to the level of a recognizable psychiatric illness, attempting to use the precedent of *Healey v. Lakeridge Health Corp*.[9] However, the Court found that "it is not plain and obvious that the plaintiffs who have suffered real pecuniary damages would not also have the right to claim additional damages for the emotional suffering, hardship and inconvenience they have suffered."[10]

Further, the Bank challenged the plaintiffs' claim for damages on the basis of waiver of tort, because the alleged wrongdoing had no connection to the Bank's profits. The Court agreed with the Bank that there must be a "wrongful gain" by the particular defendant for waiver of tort to succeed but disagreed that the Bank's profits were unconnected to the Bank's allegedly negligent supervision of Mr. Wilson, reasoning that inadequate supervision may save the Bank money.[11]

Conclusion

While it is not the first time that intrusion upon seclusion has been the basis of a certified class action, *Evans v. The Bank of Nova Scotia* is unlikely to be the last if employees of businesses who collect confidential information from their clients and customers lose or misuse that information. As such, until the parameters of the tort are further developed by the courts, it is advisable for businesses to supervise employee access to confidential information to ensure that it is not misused in a way that might subject them to potential liability.

[*Editor's note*: A version of this article was originally published in the *Gowlings Commercial Litigation Bulletin*, July 2014.]

---

1 *Evans*, [2014] O.J. No. 2708, 2014 ONSC 2135.
2 *Jones*, [2012] O.J. No. 148, 2012 ONCA 32.
3 *Ibid.*, para. 71.
4 *Ibid*.
5 [1999] S.C.J. No. 35, [1999] 2 S.C.R. 534, paras. 37, 41.
6 *Evans*, *supra* note 1, para. 26.
7 *Mohl v. University of British Columbia*, [2009] B.C.J. No. 1096, 2009 BCCA 249, para. 13 (leave to appeal refused, [2009] S.C.C.A. No. 340).
8 [2014] F.C.J. No. 297, 2014 FC 250.
9 [2011] O.J. No. 231, 2011 ONCA 55.
10 *Evans*, s*upra* note 1, para. 52.
11 *Ibid*., para. 61.

INVITATION TO OUR READERS
Do you have an article that you think would be appropriate for *Canadian Privacy Law Review* and that you would like to submit? Do you have any suggestions for topics you would like to see featured in future issues of *Canadian Privacy Law Review*? If so, please feel free to contact Michael A. Geist
@mgeist@uottawa.ca
OR
cplr@lexisnexis.ca