CANADIAN PRIVACY LAW REVIEW

Volume 11 • Number 8 July 2014

In This Issue:

LexisNexis®

Unions and Privacy: Employer Must Disclose to Union Its Employees' Personal Information

Robert Boyd
Associate
McMillan LLP

Unions may take heart in two rulings recently handed down by the Supreme Court of Canada recognizing that the protections afforded in respect of fundamental rights and personal information may not unduly restrict a union in the exercise of its activities.

Indeed, in November 2013, in an Alberta matter,[1] the Supreme Court held that the Alberta privacy statute could not prohibit a union from filming, and taking photographs of, strikebreakers. The provisions of the statute struck down by the Supreme Court provided that an organization could not collect, use or disclose personal information without the consent of the interested parties. By recognizing the importance of protecting freedom of expression in a labour dispute, the Supreme Court held that the right of a union to express itself, including by publicly denouncing strikebreakers, should take precedence over the purposes sought to be achieved by the legislator in the matter of protection of privacy.

In the same vein, the Supreme Court of Canada has just held in the matter of *Bernard v. Canada (Attorney General)*,[2] a case involving the federal public service, that an employer was required to disclose to the union the home contact information of all the employees that were members of its bargaining unit, in order to enable it to communicate with the employees quickly and efficiently. This matter contains an interesting analysis of the protection of personal information in the context of labour relations.

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)

Facts

Elizabeth Bernard was a federal public service employee who was included in the bargaining unit. However, she was not a union member. In accordance with the "Rand Formula", she paid union dues, was covered by the benefits of the collective agreement, and was entitled to representation by the union, just like all the other employees in the bargaining unit.

The dispute originated from the refusal by the employer to provide the union with the home contact information of bargaining unit members. After a complaint for unfair labour practices had been filed, the parties agreed that the employer would, on a quarterly basis, provide the union with an updated list of the home mailing addresses and home telephone numbers of the bargaining unit members, on the condition that the union undertook to ensure the security and privacy of the information, to provide it only to the appropriate union officials and not to use the information for any purpose other than union activities. In addition, the parties undertook to notify the employees of the nature of the information that would be disclosed to the union.

This agreement was approved by the Public Service Labour Relations Board (the "Board").

When she found out that her personal information had been provided to the union, Ms. Bernard initiated legal proceedings to have the decision of the Board voided. According to her, the disclosure by the employer of her personal information breached her right to privacy and her freedom of association protected by s. 2(d) of the *Canadian Charter of Rights and Freedoms* (the "Charter"), because, she argued, such freedom implied the right not to associate with the union. Finally, Ms. Bernard alleged that the disclosure of her personal information amounted to a search and seizure in breach of s. 8 of the Charter.

After numerous legal proceedings, the Board found that disclosure of personal information did not breach Ms. Bernard's fundamental rights. The Board also added two additional conditions to the disclosure of information: (1) that it was to be provided to the union only on an encrypted or password-protected basis, and (2) that expired home contact information was to be appropriately disposed of after updated information was provided.

Ruling

The Supreme Court dismissed the arguments by Ms. Bernard that disclosure of her personal information to the union breached her fundamental rights.

First of all, the Supreme Court recalled the context in which the employer disclosed the personal information. The union is the exclusive representative of all the members of its bargaining unit. While an employee who is a member of the bargaining unit is free not to join the union, according to the "Rand Formula", such employee cannot opt out from the collective labour relations scheme. He or she must pay union dues and may not choose not to be represented by the union.

On the issue of the disclosure of personal information, the Supreme Court shared the Board's opinion that the union must have access to the personal contact information of the employees in order to be able to fully exercise its representation duties incumbent on it by law. As far as collective labour relations are concerned, such exchanges cannot be limited to the workplace because the union must be able to fully exercise its representation duty. In this respect, the Supreme Court reiterated the principles set out by the Board in order to justify such disclosure of the employees' personal contact information to the union:

- it is not appropriate for a bargaining agent to use employer facilities for its business;
- workplace communications from bargaining agents must be vetted by the employer before posting;
- there is no expectation of privacy in electronic communications at the workplace; and
- the union must be able to communicate with employees quickly and effectively, particularly when they are dispersed.[3]

The Supreme Court then pointed out the tripartite relationship between the employee, the union, and the employer. In this context, it is normal that information would be shared to a certain extent. However, due to such tripartite nature, disclosure of personal information cannot be equated with disclosure of personal information to the public. The Supreme Court, therefore, stated that there was some disclosure duty upon the employer:

> To the extent that the employer has information which is of value to the union in representing employees, the union is entitled to it.[4]

The Supreme Court also found that the Board was well founded in holding that by disclosing personal information to the union, the employer did not breach the *Privacy Act*.[5] Paragraph 8(2)(a) of said Act reads as follows:

> **8**. [...]
>
> (2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed
>
> (a) for the purpose for which the information was obtained or compiled by the institution or **for a use consistent with that purpose** [emphasis added];

The Supreme Court held that disclosure by the employer of personal information to the union represented a "use consistent" with the purposes for which personal information was obtained—that is, the proper management of the employment relationship.

Ms. Bernard's argument regarding her fundamental right not to associate with the union was also dismissed. In accordance with its prior rulings handed down on the topic, the Supreme Court reiterated its position that the right not to associate, if it exists, does not mean that an employee may withdraw from the scheme of collective labour relations in order to avoid paying union dues and refuse representation by the union.

Finally, as regards the argument based on a breach of privacy, according to the Supreme Court, there could be no question of reasonable expectation of privacy relating to the information disclosed.

Comments

Although the matter occurs in the context of the federal public service, the Supreme Court relied on

general principles applicable to collective labour relations, also applicable under provincial legislation in Quebec as well as in other Canadian provinces.

Thus, the Supreme Court held that the employer must disclose to the union the addresses and personal telephone numbers of the employees because it requires such information to exercise its duty of representation owed to all the employees of the bargaining unit. By way of example, the Supreme Court argued that the union must be able to contact the employees to notify them of the conduct of a strike vote or a vote on the latest management proposals.

The Supreme Court, in a relatively succinct manner, dismissed the argument regarding privacy. In this respect, its finding that Ms. Bernard could not have an expectation of privacy with respect to her personal contact information may appear surprising. That said, the steps taken in this case to ensure that the information of the employees would remain protected by the union and would be used for the sole purpose of labour relations, in our opinion, provide an adequate protection to those employees who are concerned about the disclosure of their information in the course of labour relations. These protective measures might be used as benchmarks for the courts called upon to rule on a similar issue in other provinces. Thus, it should be recalled that personal contact information of the employees must be disclosed to the union, among others, on the following terms:

- encrypted and password-protected transmission
- disclosure only to authorized union officials
- prohibition against using information for purposes other than to exercise its representation duty
- duty to destroy obsolete information

As regards the application of privacy laws, the Supreme Court acknowledged that the statute applicable to the federal public service authorized such a disclosure of personal contract information because it was a use consistent with the purposes for which such information was obtained.

However, an issue arises as to the effect that this ruling will have in those provinces where the applicable privacy statute does not appear to authorize such disclosure of information by the employer without the employee's consent.

In particular, this is the case of *An Act Respecting the Protection of Personal Information in the Private Sector*[6] applicable in Quebec. Thus, upon reading of such statute, it appears that an employer in a private sector in Quebec may not disclose personal information to a union without having first satisfied a number of strict conditions.[7]

The employee's consent to the disclosure of his or her information to the union might also be required in accordance with the *Personal Information Protection and Electronic Documents Act*,[8] a statute applicable to federal works, undertakings, or businesses.[9]

Consequently, some legislative amendments may have to be made in order to comply with the principles established by the Supreme Court of Canada in the matter of *Bernard v. Canada*.

In the meantime, there is no doubt that unions will rely on this matter to claim their right to access personal contact information of the employees. As regards labour relations, we should recall that such information may have strategic value for a union, especially where a raiding campaign is imminent, and where a union may wish to contact employees outside the workplace. For those employees who object to the disclosure by their employer of their personal contact information to the union, it will certainly become more difficult to continue to do so now that the judgment in *Bernard v. Canada* has been handed down.

[*Editor's note*: The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on

this material alone. Rather, specific legal advice should be obtained. © McMillan LLP 2014]

---

1 *Alberta v. U.F.C.W.*, [2013] S.C.J. No. 62, 2013 SCC 62.

2 [2014] S.C.J. No. 13, 2014 SCC 13.

3 *Ibid.*, para. 25.

4 *Ibid*., para. 26.

5 R.S.C. 1985, c. P-21.

6 C.Q.L.R., c. P-39.1.

7 *See* ss. 22 and 23 of *An Act respecting the protection of personal information in the private sector*. See also *Centre financier aux entreprises Desjardins Grandes-Seigneuries—Vallée-des-Tisserands and Canadian Office and Professional Employees' Union, Local 575*, SOQUIJ AZ-50507770, D.T.E. 2008T-715, [2008] R.J.D.T. 1349.

8 S.C. 2000, c. 5.

9 On this topic, *see* Éloïse Gratton and Lyndsay Wasser, *Privacy in the Workplace*, 3rd ed. (CCH, 2013), 346–347.

The Fight for the Right…to Be Forgotten

Grant McGlaughlin
Partner
Goodmans LLP

David Coll-Black
Associate
Goodmans LLP

A recent decision of the European Court of Justice overrides the interests of internet users in protecting the privacy rights of individuals whose personal information is retrievable online.

Background

On May 5, 2010, Mr. Costeja Gonzalez filed a complaint with the Spanish Data Protection Agency ("SDPA") against La Vanguardia Ediciones S.L. ("Vanguardia"), a Spanish daily newspaper publisher, and Google Spain and Google Inc. Mr. Gonzalez complained that when internet users searched his name, they retrieved links to two Vanguardia announcements from 1998 regarding a real estate auction connected to recovery of social security debts owed by Mr. Gonzalez.

Mr. Gonzalez requested that (1) Vanguardia remove or alter the relevant pages on their website so that his personal information would not be publicly available, and (2) Google cease to include his personal data in search results. Mr. Gonzalez argued that the articles were no longer relevant because the situation had been fully resolved.

On July 30, 2010, the SDPA rejected his claim against Vanguardia, finding that Vanguardia had legally published the articles in 1998. However, the SDPA upheld Mr. Gonzalez's claim that his personal data no longer be included in Google search results. The decision was based on the SDPA's authority to require search engine operators to remove or exclude data that compromises the fundamental right to data protection and the dignity of persons. The SDPA considered that the obligation on search engine operators was separate from any obligation of the initial publisher. Thus, the requirement to remove or exclude data could be imposed on search engine operators, even when the information legally remained on a website.

Following an appeal by Google to the National High Court of Spain, the question of what obligations are owed by search engine operators to protect personal data of persons who do not want their personal information to be located, indexed, and made available to internet users was referred to the European Court of Justice (ECJ), the highest court in the European Union in matters of European Union law.

The Right to Be Forgotten

The ECJ decided that a person may make a request for information removal directly to the search engine operator. The search engine operator must assess the merits of the request and accept or deny the

request. If the search engine operator denies a request, the requesting party can bring the matter before a supervisory or judicial authority for determination.

The ECJ analyzed the need to access data for legitimate interests in the face of a person's right to privacy—a European Charter–protected fundamental right and freedom. In its analysis, the ECJ stated that a fair balance should be sought in determining the legitimate interests of an internet user and a person's fundamental rights. As a general rule, the ECJ specified that the interests of the person whose data is in question will override the interests of an internet user. However, the determination ultimately depends on (1) the nature of the information in question, (2) the degree of how personal or sensitive the information is to a person's private life, and (3) the interests of the public in having the information—in particular, the person's role in public life. It may therefore be more difficult for politicians to have personal information relevant to their profession removed from search results.

The Right to Be Forgotten in Canada

While Canadians' rights to privacy are not enshrined in our Charter, as is the situation in Europe, we enjoy some protections under our federal and provincial privacy laws.

As concerns mount that the right to be forgotten will open the door to large-scale self-censorship in Europe, pitting freedom-of-speech advocates against the defenders of privacy, the status quo in Canada may not last long. Google is currently building an infrastructure that will allow internet users to request the removal of personal information relating to them from search results. A test case in Canada is likely on the horizon.

Managing the Privacy Side Effects of Rx (and other) Customer Loyalty Programs

Lydia Wakulowsky, C.S.
McMillan LLP

Introduction

On April 10, 2014, the Alberta College of Pharmacists prohibited pharmacists from offering customers inducements for the purchase of prescription drugs, blood products, or professional services (collectively, "Rx drugs"), stating that

> [i]nducements cloud decisions that should be based solely on the best healthcare.
>
> Providing inducements [for Rx drugs] is disruptive to:
>
> - impartial decision-making,
> - the coordination and continuity of care, and
> - the effective operation of health teams and Alberta's health system.[1]

Currently, seven other provinces have rules in various forms that prohibit or restrict pharmacists' use of such inducements. In response, the "Coalition of Consumer Choice"—a group of retail grocers, consumer associations, and patient advocates—are opposing the prohibition through an "I Earned It" petition calling on the provincial government to overturn it. Some have said that Rx loyalty programs build stronger bonds between patients and their pharmacies and encourage better patient adherence to prescription medication.

The conflict-of-interest debate is not new for health professionals practising in a retail environment. It has become increasingly complex, particularly with interprofessional collaboration. Historically, the debate has concerned pharmacists selling Rx drugs (and medical devices), opticians and optometrists selling corrective lenses, and physicians having a

business interest in pharmacies and other for-profit ventures. The debate will continue to engage health professionals practising in team settings.

This article reviews customer loyalty programs from a different perspective. Privacy considerations should be top of mind when developing and implementing Rx (and other) customer loyalty programs, particularly in light of new sophisticated data mining technologies and increasing cross-border transfers of personal information.

Privacy Considerations

Pharmacies may very well have the altruistic goal of encouraging patient adherence to prescription drugs. But stores generally launch customer loyalty programs to gain a bigger share of revenue by rewarding individuals for shopping at their store. The more money a customer spends, the greater the rewards. Often, customers can accumulate points that they redeem for "free" goods; sometimes, they can accumulate extra points when they purchase specific goods. Plastic loyalty cards with a magnetic strip or barcode contain a unique identification number. They enable the store to monitor a customer's transactions. When a purchase is made, data about the purchase (*e.g.*, the product, place of purchase, and date) is recorded. Over time, a customer's behavioural information gathered through the loyalty card can be substantial. And often, that data is collected and mined as part of a larger business intelligence initiative. The store can use the mined data to predict trends, refine marketing approaches, and potentially sell aggregated data and insights to third parties.[2] As data aggregation and mining has evolved, its impact on privacy has become increasingly complex and controversial. The main privacy concern is that profiles of individuals can be created. Once created, they can be disclosed inadvertently upon a security breach taking place.

Privacy Best Practices

Before a pharmacy embarks on an incentive program involving Rx drugs in those jurisdictions where it is allowed, the following matters (among others) should be diligently considered and addressed.

The terms and conditions for the customer loyalty program should clearly describe the program's collection and use of Rx drug data, including how the collected data will serve the program's purpose and any secondary purpose. Shoppers Drug Mart collects data from Optimum members for very broad purposes such as to communicate with the member, to better understand the member's shopping and information needs, and to offer the member relevant information, products, services, and rewards to meet those needs. If a pharmacy were to collect Rx drug data, what use would be made of it? Would a pharmacy inform a customer buying insulin of community diabetes clinics? This might prove to be a valuable service to the customer. But would the pharmacy also predict future healthcare needs of participating customers (or family members) when genetic health issues are involved? Would individuals learn of their own predicted future healthcare needs from their pharmacy?[3] What action would be taken on the basis of Rx drug data gleaned from a data mining program? Personal health information is considered to be sensitive and, under most privacy regimes, would require a customer's express consent. Query whether valid express consent can be obtained under a long terms of use agreement, which many customers do not typically read and/or understand.

Another significant issue concerns Rx data that can be accessed from a Canadian pharmacy in the U.S. The terms and conditions of the program should clearly discuss the implications, and the Canadian pharmacy should ensure that it is in compliance with legal requirements pertaining to the cross-border transfers of personal information (some jurisdictions, such as Quebec, have stringent legal requirements for the transfer of personal information to foreign jurisdictions). In one situation, the U.S. Drug Enforcement Agency subpoenaed records from the database of a supermarket chain, looking to see whether certain individuals had

purchased large quantities of plastic bags commonly used in drug transactions.[4] Consider the case of the disabled Canadian woman who was denied entry to the U.S. because Homeland Security accessed a database that showed she had been hospitalized for clinical depression.[5] If data is accessed or stored in the U.S., Homeland Security would have access to all customer loyalty program members' Rx drug histories. Customers should be made aware of this and, as participating members, be informed that they can opt out of having their pharmacy record their Rx drug data in the program database. Pharmacies should also consider whether some Rx drug data is too sensitive to be collected for purposes of the program (*e.g.*, psychotropic, HIV/AIDS drugs) and limit their collection appropriately.

The pharmacy should consider whether it will aggregate data and sell it to third parties. If so, the pharmacy should inform its customers of this and obtain their prior consent. While customers do not, generally, have privacy rights over aggregated data, this information might impact the validity of their knowledgeable, informed consent. Another issue that could impact informed consent is the ability of a pharmacy to change the program's terms and conditions, including changes that devalue conversion rates.[6] When a customer weighs the benefits and the risks of joining an Rx drug program, the value of the points might be a consideration, and informed consent might be negated.

The pharmacy must put appropriate privacy protections into its systems. Consider CVS's 50-million-member ExtraCare loyalty program, which had a potential security problem. Anyone with a member's card number, ZIP code, and last name could access information concerning a member's over-the-counter drug and family planning purchases because CVS did not password protect this information. Access to a customer's ExtraCare number was simple. It is printed on all CVS receipts and is readable on keychain cards (which may be accessed by parking valets). Upon becoming aware of this security flaw, CVS pulled Internet access to the data. The access was restored after CVS added security to the site.[7]

The pharmacy must consider the result if a customer withdraws from a loyalty program. Will all information pertaining to the customer, including the purchase history, be removed from the loyalty program records permanently? The intent should be clearly set out in the terms and conditions.

A thoughtful legal and policy analysis at the commencement of a data aggregation and mining program (or a program that might appear to the public to have data mining potential) is worthwhile to avoid scrutiny from the public and privacy advocates once an Rx drug loyalty program is underway. It might be wise to bring in the appropriate privacy experts at the developmental stage to get input. It is certainly wise to consult with qualified legal counsel in developing the privacy framework for the program.

---

1 Alberta College of Pharmacists, *Inducement for Drugs and Professional Services: A Basis for a Prohibition*, p. 3, <pharmacists.ab.ca/Content_Files/Files/Inducements_paper_apr18.pdf>. The prohibition came into effect on June 10, 2014.

2 Shoppers Drug Mart, as part of its Optimum rewards program, has a Very Important Baby program for new and expectant mothers. Identified members receive targeted newsletters on health and nutrition.

3 Consider the situation involving Target in the U.S.: Target was able to figure out that a teenage girl was pregnant before her father did. By data mining the pregnant teenager's purchase history, Target was able to know that she was pregnant because she purchased various items that were highly predictive of pregnancy.

4 Privacy Rights Clearinghouse Fact Sheet #15: What Personal Information Should You Give to Merchants, quoting Robert O'Harrow, "Bargains at a Price: Shoppers' Privacy", *Washington Post*, December 31, 1998, <https://www.privacyrights.org/what-personal-information-should-you-give-merchants>.

5 Valerie Hauch, "Disabled Woman Denied Entry to U.S. after Agent Cites Supposedly Private Medical Details", *Toronto Star*, November 28, 2013, <http://www.thestar.com/news/gta/2013/11/28/disabled_woman_denied_entry_to_us_after_agent_cites_supposedly_private_medical_details.html>.

6 Note that in July 2010, Shoppers Drug Mart announced a new conversion rate for its points. To get $1 in merchandise,

customers would need 800, instead of 700, Shoppers Optimum points. In 2010, Option Consommateurs initiated a class action lawsuit against Shoppers Drug Mart, which operates in Quebec as Pharmaprix. Option Consommateurs alleged that the company broke Quebec's consumer protection laws when it changed the conditions of the chain's Optimum loyalty program, increasing the number of points necessary for savings, and impacting the 1.4 million Quebec residents who use the cards. In March 2012, a Québec Superior Court judge agreed to hear the case.

[7] Barry Berman, "Developing an Effective Customer Loyalty Program", *California Management Review* 49, no. 1 (Fall 2006): 123–148.

The Tort of Intrusion upon Seclusion Meets Class Action Certification

Roland Hung
Associate
McCarthy Tétrault LLP

In *Evans v. Bank of Nova Scotia* [*Evans*],[1] the Ontario Superior Court of Justice (the "Court) certified a class action proceeding for allegations concerning a breach of privacy rights through the tort of intrusion upon seclusion. This decision set a precedent for the low bar of certification in class actions concerning breaches of information privacy, which may be of some concern to organizations that handle personal information.

The Case

Justice Smith heard a motion in *Evans* to certify class proceedings by plaintiffs claiming that the Bank of Nova Scotia (the "Bank") was vicariously liable for the actions of an employee who surreptitiously disseminated the private and confidential information of customers for fraudulent and improper purposes.

In assessing the validity of the cause of action for the breach of information privacy, the Court relied on the test for the tort of inclusion upon seclusion set out in *Jones v. Tsige* [*Jones*],[2] as follows:

1. The defendant's conduct must be intentional (which could include recklessness).
2. The defendant must have invaded the plaintiff's private affairs or concerns without lawful justification.
3. A reasonable person would regard the invasion as highly invasive, causing distress, humiliation, or anguish.

The *Jones* test does not require proof of damage, widening the availability of the common law tort of intrusion upon seclusion as a basis of action in certain provinces. In *Evans*, the Court found that the plaintiffs established that their claim against the Bank for vicarious liability for its employees' tort of intrusion upon seclusion would not be plainly and obviously unsuccessful. Though the Court noted that the law in this area is unsettled, it chose to affirm the test in *Jones*, declining to consider decisions by courts in British Columbia and New Brunswick, which have recently chosen not to recognize this common law tort.

Significance

The availability of the tort of intrusion upon seclusion as a class action matter should concern retailers and other consumer-facing businesses because of the following:

- The elements of proving this tort do not require proving damage.
- The threshold for class action certification is low, given that class action statutes are structured to promote access to justice and to make efficient use of judicial resources through the consolidation of common claims that may otherwise not be litigated.

However, the common law tort of inclusion upon seclusion per *Jones* is not recognized in all Canadian provinces. Plaintiffs may not always have an option

to base a class proceeding on this tort claim. For instance, the Supreme Court of British Columbia held in *Demcak v. Vo* that there is no common law tort of invasion of privacy.[3] Instead, B.C., along with three other provinces,[4] has a statutory tort for the invasion of privacy. While the B.C. statutory provisions outlining[5] this tort are similar to those elements in *Jones*, it is possible that the existence of a statutory cause of action will preclude courts from seriously considering the common law tort followed by the Court in *Evans*.

Despite the fact that the tort of inclusion upon seclusion is not available in B.C., the Supreme Court of British Columbia has recently certified a class action against Facebook (a massive estimate class of 1.8 million people) regarding alleged violations of the British Columbia *Privacy Act*. This action arose from Facebook's "Sponsored Story" advertisement that uses an individual's Facebook portrait image and name to indicate to friends in the individual Facebook network that he or she follows a brand or product on Facebook. It was alleged that Facebook violated s. 3(2) of the *Privacy Act* by using portrait images and names of users in the "Sponsored Stories" without explicit and informed consent.

The debate in Canada is clearly far from over. It will be interesting to see whether other jurisdictions (1) adopt a common law cause of action and allow certifications of class proceedings (as in Ontario), or (2) enact a statutory cause of action and allow certifications under the statutory regime (as in B.C.), or do both.

---

1 *Evans v. Bank of Nova Scotia*, [2014] O.J. No. 2708, 2014 ONSC 2135.

2 *Jones v. Tsige,* [2012] O.J. No. 148, 2012 ONCA 32, para. 71.

3 *Demcak v. Vo*, [2013] B.C.J. No. 1058, 2013 BCSC 899.

4 Saskatchewan, Manitoba, and Newfoundland and Labrador.

5 *See* the British Columbia *Privacy Act*, R.S.B.C. 1996, c. 373, s. 1.

Guidelines on the Collection of Personal Information and Leases

Alexandra Nicol
Lawyer
Borden Ladner Gervais LLP

The Commission d'accès à l'information ("CAI"), Quebec's privacy commissioner, has recognized a landlord's rights to personal information. However, by virtue of *An Act respecting the Protection of Personal Information in the Private Sector*,[1] the information requested by the landlord must be necessary and indispensable to the evaluation and management of a leasing application.

In order to ensure that the personal information requested remains within the permissible framework, the CAI has established a set of guiding principles (summarized below) that should be considered prior to disclosing personal information.

Personal Information That May Be Requested by a Landlord

1) *Personal information establishing the identity of the future tenant*. The landlord may request the full name and current address of the applicant. In order to ensure the accuracy of such information, the landlord may require the applicant to present a valid piece of identification. However, the landlord is forbidden from retaining any information contained on the identification, and, therefore, no photocopy may be produced by the landlord.

2) *Personal information establishing behavioural traits*. In order to establish the behavioural traits of an applicant, the landlord may request only the name or contact information of the current/previous landlord. Alternatively,

the applicant may present a letter of recommendation signed by the previous landlord.

3) *Personal information establishing the payment tendencies of the applicant*. With the consent of the applicant, the landlord may (a) request information from the current or previous landlord, and (b) perform a credit check. In such circumstances, the landlord need obtain only the applicant's full name, current address, and date of birth.

   Alternatively, to establish his credit worthiness, the tenant may provide the landlord with (a) a credit certificate from their financial institution; (b) a letter of recommendation from a previous landlord; (c) any other document attesting to the applicant's adherence to his obligations (Bell, Hydro-Québec, *etc*.); or (d) pertinent extracts from his credit report.

   In order to conduct a credit history check, the landlord must first obtain the applicant's consent. Once consent is obtained, a credit history check necessitates very limited information (*i.e.*, full name, current address, and date of birth). The landlord does not need to obtain the applicant's social insurance number.

   It is important to note that the above information may also be requested by the landlord in the context of a sublease or assignment.

Personal Information That *May Not* Be Requested by a Landlord

The following information may not be requested by a landlord:

- social insurance number
- driver's licence and number
- health insurance card and number
- passport

In addition, the analysis of an application does not necessitate the applicant to mention his current employment, name and contact information of his employer, number of years working for the employer, and his salary. The same applies for all registration-related information of the applicant's personal vehicle. Finally, the applicant is not required to provide the name and coordinates of his financial institution; nor is the applicant required to provide a copy of a blank cheque.

In the event that a landlord requests personal information not specifically authorized by the Act, the applicant may file a complaint with the CAI. The CAI can provide the necessary information requested, launch an investigation, and/or recommend or order any measures deemed appropriate for the protection of the applicant's personal information. However, if the Act is contravened, the CAI, in such circumstances, does not have the authority to grant damages.

[*Editor's note*: A version of this article was originally published on the *Law of Privacy in Canada Blog*, <http://carswellprivacylaw.wordpress.com/>.]

---

[1] CQLR c P-39.1.

Will Europe's "Right to Be Forgotten" Cross the Pond to Canada?

Aaron Lemkow
Summer Student, Stewart McKelvey
Juris Doctor Candidate 2015,
Dalhousie University Schulich School of Law

The European Court of Justice's (the "ECJ") recent affirmation of the European Union's ("the EU") "right to be forgotten" has stirred intense debate and stoked fears about the future regulation of the Internet; one journalist went so far as to identify the decision as a shift towards Orwellian control over information. The case centered around

Costeja Gonzalez of Spain and his request that Google remove a link to a 36-word article from 1998, which detailed the repossession of his home to satisfy his debts.

In the aftermath of the ruling, Google has been bombarded with similar requests from thousands of individuals, ranging from ex-politicians to convicted pedophiles. This has predictably caused an administrative nightmare for Google, which is scrambling to figure out how to process these requests. Whether European courts will be similarly overwhelmed has yet to be seen, but this prospect is tempered by the irony that a requester must first air his or her dirty laundry in the most public manner imaginable before having it removed from the digital clothesline.

But what is the impact on Canada? Could a similar law pass muster in our own legal system? The decision could have far-reaching effects that could affect Canadian companies doing business in the EU. Such was the threshold used by the ECJ: data processors, whether operating inside the EU or not, fall under this law if they or their subsidiaries economically benefit in the EU from their data-processing services. But the decision leaves several unanswered questions: How directly must the data processing be tied to economic benefits before falling under this law? Must data processors remove links from searches conducted in the EU or around the globe? What about open-source software with contributors from inside and outside the EU? It may be years before the implications of this case are fully understood and appreciated.

Fears over whether a home-grown law could take shape may be unwarranted. The right to privacy is selectively protected in our *Charter of Rights and Freedoms* (the "Charter"), such as the right to be free from unreasonable search and seizure. Freedom of expression, on the other hand, has been generously interpreted and applied by Canadian courts: it is informed by listeners' interests, and courts are moving away from limiting the protection of economic expression.

And yet, a Canadian equivalent is not out of the realm of possibility; privacy concerns have been enough to sink federal bills aimed at strengthening state surveillance. Should Parliament or a provincial legislature decide to pass such a law, it would have to be saved (under s. 1 of the Charter) as a reasonable limit that can be demonstrably justified in a free and democratic society. The Charter jurisprudence indicates that courts will generally be deferential to a government faced with competing social and economic interests, and nowhere is this balancing act better illustrated than under the "right to be forgotten".

Privacy interests and freedom of speech are continuing to collide.