The Limits of the Application Game - Why Employee Privacy Matters

By Dan Michaluk

Introduction

“Do our employees have privacy rights?” This simple question, which we are often asked, is rarely a simple one to answer.

In some cases, clear privacy rights govern the employment relationship. There is a clear statutory requirement, for example, that restricts employers from using employee social insurance numbers as unique identifiers without express written consent. In other cases, privacy rights are less clearly defined but are real nonetheless. Labour arbitrators regularly recognize that unionized employees have implied privacy rights, for example.

There are yet other cases in which there is a clear employee privacy issue but not a clear employee privacy right. Given that no privacy legislation applies directly to Ontario-regulated employment relationships and given that common law (or court-based) privacy rights are yet to be firmly recognized, this is a common situation facing non-unionized employers in Ontario. To put it plainly, there is an apparent privacy rights gap in Ontario employment law.

There are two basic ways employers manage the gap. Some non-union employers, in the name of employee relations, follow a best practices approach in managing privacy issues. Others take a more aggressive approach and rely on the fact that their employees do not have a practical means of forwarding a privacy complaint – that is, they “play the application game.”

In this paper we describe the various sources of employee privacy rights in five parts: (1) rights in privacy statutes; (2) human rights and privacy statutes; (3) privacy regulation in other statutes; (4) contractual privacy rights; and (5) the privacy tort. Our intent is to illustrate that privacy rights are rooted in many sources, that there

---

1 Income Tax Act, R.S.C. 1985, c. 1 (5th Supp), ss. 239(2)(b) and (2.3).
are risks of newly-developing sources of employee privacy rights and, overall, that employee privacy does matter.

Rights in Privacy Statutes
Privacy statutes are often referred to by their acronyms. In Ontario, the relevant statutes are:

• **Personal Information Protection and Electronic Documents Act (PIPEDA)**;  
• **Personal Health Information Protection Act, 2004 (PHIPA)**;  
• **Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)**;  
and

• **Freedom of Information and Protection of Privacy (FIPPA)**.

In this part, we describe how PIPEDA, PHIPA, MFIPPA and FIPPA apply to employees in Ontario. As you will see, PIPEDA contains the only statute-based privacy code that regulates employees working in Ontario, but it only applies directly to employees who work for federally-regulated employers.

**PIPEDA**

PIPEDA regulates employment in banks, telecommunications companies, inter-provincial transport companies, airlines and other federally-regulated employers. These employers must abide by PIPEDA and its ten privacy principles, including the principle that collections, uses and disclosures of employee personal information be based on informed (express or implied) consent, and the principle that personal information should only be collected, used and disclosed as necessary for a reasonable purpose.

**PIPEDA** does not apply directly to employers regulated by Ontario employment law. Generally speaking, employees who work for these employers do not enjoy the protection of a statute-based privacy code.

---

2 S.C. 2000, c. 5.  
3 S.O. 2004, c. 3, Sch. A.  
6 *PIPEDA*, Principle 3.  
7 *PIPEDA*, section 5(3), Principle 4 and Principle 5. As this paper is providing an overview of privacy issues facing employers, throughout this paper we have provided a simplified description of the statutory requirements.
There is still some debate about whether PIPEDA can apply indirectly to Ontario-regulated employers who outsource functions to commercial service providers because PIPEDA applies to personal information that is collected, used and disclosed “in the course of commercial activity”. On one theory, when an employer outsourcers an employment administration function (e.g. payroll administration), an agency relationship exists and there is no “disclosure” that attracts the application of PIPEDA. On another theory, the outsourcing of employment administration functions by Ontario-regulated employers is regulated by PIPEDA because outsourcing requires employee personal information to be disclosed and used “in the course of commercial activity” between the employer and the service provider.

This issue is far from certain, and prudent employers will keep in mind PIPEDA’s privacy principles when engaging third party commercial service providers to process or otherwise handle employee personal information.

**PHIPA**

PHIPA is significant to Ontario employers, but has limited application to employers who do not provide health care to their employees.

In the ordinary course, the only section of PHIPA that regulates the employment relationship is section 49. This section effectively requires employers to collect information for their employment-related purposes based on express written consent and to use and disclose that information strictly within the limits of the written consent.\(^8\) An employer’s ability to ask an employee for his or her consent is not directly regulated by PHIPA, but PHIPA does require health care practitioners to assess the necessity of the employer’s request.\(^9\)

Employers who provide health care to employees are fully regulated by PHIPA in undertaking this activity – that is, they are bound by all elements of the PHIPA privacy code.

The definition of health care is critical for employers to understand because their obligations vis-à-vis employee medical information are very different depending the reason the records were generated. Although health care is defined broadly, it likely does not include occupational assessments.\(^10\) Therefore, employers who employ or retain medical professionals to wear “two hats” (by providing health care and

\(^8\) PHIPA, section 49.

\(^9\) PHIPA, sections 29 and 30.

performing occupational assessments) should be particularly careful in keeping their health care and assessment processes and records separate.

**MFIPPA and FIPPA**

There are two public sector freedom of information and privacy statutes: the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* and the *Freedom of Information and Protection of Privacy (FIPPA)*. Both MFIPPA and FIPPA include a very broad exclusion for employment-related records.¹¹ In light of a significant 2001 decision on the exclusion by the Ontario Court of Appeal,¹² the Commissioner herself has acknowledged that the privacy of public sector employees in Ontario is not protected under the statutes. In lobbying for an amendment to the exclusion, she has stated, “Public sector employees are currently precluded from obtaining access to most employment-related records about themselves, and from filing a privacy complaint if they feel that their personal information has been improperly collected, used, disclosed or retained”.¹³

**Human Rights Legislation and Privacy**

An employee has an obligation to provide an employer with medical information that is *reasonably necessary* to the administration of the employment relationship, including (1) to determine the validity of an absence, (2) to determine eligibility for an income protection benefit, (3) to develop accommodation plans and proposals and (4) to ensure that employees can safely return to work.

Employers who do not respect the reasonable necessity requirement in managing employees who suffer from disabilities or perceived disabilities do, however, expose themselves to potential human rights liability. In fact, human rights claims that arise out of a failed accommodation process often involve disputes about the necessity of an employer’s request for information – essentially a matter of individual privacy. The Alberta Court of Queen’s Bench recently noted the link between human rights and privacy rights in *Kellogg Brown & Root*:

> … some may argue that [an anti-discrimination right] should not do the work of privacy rights. However, equality rights, human rights and privacy rights do not exist in compartments. In Law the Supreme Court stated that a primary purpose of equality rights is the protection of the essential human dignity of each individual. The Act identifies human dignity and equality as fundamental principles to

---

¹¹ *MFIPPA*, section 52(3) and *FIPPA*, section 65(6).


be cherished and protected in Alberta... Human dignity is therefore at the core of both privacy rights and equality rights. To extend the protection of perceived disability to individuals who test positive on this type of drug test within this type of policy promotes the protection of human dignity and strengthens rather than dilutes anti-discrimination norms.¹⁴

Privacy Regulation in Other Statutes
There are also privacy rights and restrictions scattered throughout the federal and provincial statute books. We cannot list all such provisions, but we have identified the most significant statutory provisions in an Appendix to this paper.

Contractual Privacy Rights
Currently, for Ontario-regulated employers, the implied contractual obligations of unionized and non-unionized employers differ.

Unionized Employers and Collective Agreement Rights
Although collective agreements rarely contain express privacy protections, arbitrators have willingly protected unionized employees’ privacy rights by relying on clauses that specify that work rules must be reasonable,¹⁵ by recognizing implied restrictions on management rights,¹⁶ and by recognizing a right of privacy based on the “common law of the unionized workplace”.¹⁷ Based on the prevailing arbitral case law, employers have a fairly limited ability to raise successful preliminary objections to privacy complaints by arguing that there is no right in the collective agreement that has been violated.

Non-Unionized Employers and Constructive Dismissal Claims
The best way of describing the position of non-unionized employees of Ontario-regulated employers is that they have no practical means of asserting a privacy

¹⁵ See e.g. Re United Food and Commercial Workers Union, Local 1000A and Janes Family Foods (Surveillance Grievance), [2006] O.L.A.A. No. 611 (Trachuck) (QL).
complaint unless their employer has created some policy or other express contractual basis for making such a complaint. In theory, if these employees have privacy complaints that amount to a “fundamental breach” of the employment relationship, they may quit and claim constructive dismissal. However, this option has not yet proven to be appealing, and we are not aware of any constructive dismissal claims advanced on the basis of a privacy breach alone.

This does not mean that employers should be blind to the risk of constructive dismissal claims based on privacy claims when managing employees. The *Honda v. Keays* decision is a well-known recent case in which an employer was found to have constructively dismissed an employee who suffered from chronic fatigue syndrome by being overly-aggressive in seeking medical information about the employee’s condition.¹⁸ Although the *Keays* decision does not use the language of privacy to express why the employer breached its contract of employment and constructively dismissed Mr. Keays, the interest protected by the Court in *Keays* is analogous to a privacy interest.

**The Privacy Tort**

The traditional view of the common law is that there is no tort of invasion of privacy. For example, in the case of *Euteneier v. Lee*, the Ontario Court of Appeal made the following comments:

> But [the respondent] properly conceded in oral argument before this court that there is no ‘free-standing’ right to dignity or privacy under the *Charter* or at common law. For example, although respect for human dignity underlies many of the rights and freedoms in the *Charter*, it is not a principle of fundamental justice under s. 7 of the *Charter*.¹⁹

However, over the years, common law courts in Ontario have grappled with whether such a tort does, or at least should, exist. In one recent claim, an employee claimed that his employer committed the tort when the employer conducted a credit check without notice or consent. The employer brought a motion to strike the claim as not disclosing a reasonable cause of action. In *Somwar v. McDonald’s Restaurants of Canada Inc.*, Madam Justice Stinson of the Ontario Superior Court of Justice dismissed the employer’s motion, and stated as follows:

> With advancements in technology, personal data of an individual can now be collected, accessed (properly and improperly), and

disseminated more easily than ever before. There is a resulting increased concern in our society about the risk of unauthorized access to an individual’s personal information. The traditional torts such as nuisance, trespass, and harassment may not provide adequate protection against infringement of an individual’s privacy interests. Protection of those privacy interests by providing a common law remedy for their violation would be consistent with Charter values and an “incremental revision” and logical extension of the existing jurisprudence.  

This was a preliminary motion only, but Stinson J.’s *dicta* is strong. The above paragraph was commented upon positively by another judge of the Ontario Superior Court of Justice later in 2006.\(^{22}\) Last year, a small claims court judge relied on the *Somwar* case in awarding damages for the tort of invasion of privacy.\(^ {23}\) Based on these developments, employers ought to beware of the potential for tort-based liability for privacy violations in respect of their current and former employees.\(^ {24}\)

**Conclusion**

It should be apparent from the above discussion that employee privacy rights do exist in Ontario. And while the scattering of privacy-protective provisions throughout the statute book and the nascent status of a tort of invasion of privacy leave employers with the option of managing around privacy rights and playing the application game, this approach to managing employee privacy comes with legal and practical risks. Furthermore, and as noted by the Alberta Court of Queen’s Bench in the *Kellogg Brown & Root* case, respect for human dignity is at the core of privacy rights. This view means that the availability of the application game may narrow as the law develops. In short, employee privacy matters.


\(^{24}\) The risk of negligence claims for data breaches is also a possibility – see *g.* *Young v. Bella*, [2006] 1 S.C.R. 108, 2006 SCC 3 (CanLII).
## Appendix – Privacy Regulation in Other Statutes

<table>
<thead>
<tr>
<th><strong>Criminal Code, R.S.C. 1985, c. C-46 – Canada</strong></th>
<th><strong>Confidentiality – Prohibition on Wiretaps</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Prohibition</strong> against wilfully intercepting a private communication by means of any electro-magnetic, acoustic, mechanical or other device (s. 184).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Consumer Reporting Act, R.S.O. 1990, c. C.33 – Ontario</strong></th>
<th><strong>Confidentiality – Requesting Consumer Report</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Intention to use for employment purposes must be established (s. 8(1) and (2)).</td>
<td></td>
</tr>
<tr>
<td>• <strong>Prohibition</strong> against requesting or obtaining consumer reports without written notice (s. 10(2)).</td>
<td></td>
</tr>
<tr>
<td>• <strong>Notice</strong> must take specific form (s. 10(6)).</td>
<td></td>
</tr>
<tr>
<td>• <strong>Notice</strong> of adverse action must be given per the statute (s. 10(7)).</td>
<td></td>
</tr>
<tr>
<td>• <strong>Prohibition</strong> against obtaining other information without notice (s. 11(1)).</td>
<td></td>
</tr>
<tr>
<td>• Offence for any contravention up to $25,000 (individual) or $100,000 (corporation) (s. 23).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Employment Standards Act, 2000, S.O. 2000, c. 41 – Ontario</strong></th>
<th><strong>Physical Privacy - Lie Detector Tests</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Prohibition</strong> against requiring, enabling or influencing an employee to take a lie detector test (s. 70(1)).</td>
<td></td>
</tr>
<tr>
<td>• <strong>Prohibition</strong> against disclosing to an employer that an employee has taken a test and disclosing results of test (s. 70(2)).</td>
<td></td>
</tr>
</tbody>
</table>

**Permissible Disclosure - Building Service Providers**

<p>| • Disclosure of prescribed employee information to possible new provider, new providers, and owner/managers permitted (s. 77 of the Act, and s. 3 of O. Reg. 287/01). | |</p>
<table>
<thead>
<tr>
<th>• Obligation to keep confidential, use only for determining termination, severance and vacation obligations or potential obligations under Part XIX of the Act (s. 78).</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• <strong>Not an identifier</strong> - SIN not to be used, communicated or allowed to be communicated for purposes other than authorized under the Act without an individual's written consent (s. 237(2)(b)).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not an identifier (offence)</strong> – Offence to knowingly use, communicate or allow to be communicated without written consent – punishable by fine not exceeding $5,000 or imprisonment not exceeding 12 months, or both (s. 239(2.3)).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality of medical information gathered under the Act (s. 63(1))</td>
<td>• Employer shall not seek access to a worker's health record without consent (s. 63(2))</td>
</tr>
<tr>
<td></td>
<td>• Section 63 of the Act prevails despite anything to the contrary in the <em>PHIPA, 2004</em> (s. 63(6))</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mandatory Collection (Medical Surveillance Programs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Employer has duty to establish a medical surveillance program as prescribed by regulations (s. 26(1)(h))</td>
</tr>
<tr>
<td>• Worker consent required (s. 26(3))</td>
</tr>
<tr>
<td>• Programs all relate to exposure to certain designated substances</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Employee Access – Board File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worker has right to request access to the file kept by the Board “if there is an issue in dispute” and the Board does not believe the worker will be harmed by seeing the file (s. 57).</td>
</tr>
</tbody>
</table>

**Confidentiality**

- **Functional Abilities Form** – Employer and its representative prohibited from disclosing information contained in functional abilities form except to a person assisting the employer return the person to work (s. 37(4)).

- **Documents Disclosed by Board** - Employer must keep information disclosed from Board confidential (s. 59).

- **General** - Employer must not disclose health information received from a health care practitioner, hospital, health facility or any other person or organization about a worker who has made a claim for benefits unless specifically permitted by the Act (s. 181).

- **Offence** – failure to comply with the above punishable by fine of up to $100,000 (s. 150).