Health information is generally regarded as among the most sensitive types of personal information. Even members of the Millennial Generation, who regularly share details of their personal lives on social media, are troubled by the thought of strangers accessing the intimate details of their health histories.

There has been a string of data breaches in the health sector recently: some breaches due to employee carelessness, some due to intentional employee behaviour, and some due to malicious cyber-attacks. What recourse does an Ontario patient have when his or her personal health information is unlawfully accessed or distributed? The answer used to be clear that a patient whose privacy rights were violated had no immediate access to the courts, but the patient could make a complaint to the Information and Privacy Commissioner of Ontario (the “Privacy Commissioner”). For the first time, a case now pending before the Ontario Court of Appeal raises the question of whether a patient who is a victim of a privacy breach can access the Ontario courts as well as the mechanisms provided in Ontario’s health sector privacy legislation.
Ontario now recognizes a cause of action for breach of privacy. In 2012, the Ontario Court of Appeal released its decision in *Jones v. Tsige* and explicitly recognized a common law tort for breach of privacy in Ontario. Prior to that decision, there had been no common law cause of action for invasion of privacy recognized in Canadian law. Other provinces, such as Nova Scotia, have left the door open to follow Ontario’s lead. In contrast, the courts of British Columbia have explicitly stated that there is no common law tort of invasion of privacy in that province. This leaves citizens in British Columbia to rely solely on statutory rights of action.

While it may seem like just an esoteric legal question whether one’s right of action is based on the common law or statute, the answer to this question actually has very real, practical implications for patients, health care providers, and the insurers of health care providers in Ontario.

This article provides an overview of privacy litigation in Ontario and examines the important questions that are pending in Ontario today with respect to privacy violations in the health care sector.

The Tort of Intrusion upon Seclusion

Traditionally, in Ontario, there was no private cause of action for breach of privacy. A person who alleged breach of privacy was restricted to following the statutory procedures enacted in privacy legislation.

The Ontario Court of Appeal changed the law of privacy in that province in 2012 when it confirmed in *Jones v. Tsige* that “intrusion upon seclusion” is a valid cause of action. In this case, the plaintiff, a bank employee, alleged that her privacy rights had been breached by another bank employee. The issue before the Court of Appeal was whether Ontario law recognized a right to bring a civil action for damages for the invasion of personal privacy, or whether the plaintiff’s only remedy was to bring a complaint to the Office of the Privacy Commissioner of Canada under the *Personal Information Protection and Electronic Documents Act* [*PIPEDA]*.
In *Jones v. Tsige*, the Court of Appeal expanded the common law and recognized the existence of a right of action for privacy violations that involve “intrusion upon seclusion”. To establish intrusion upon seclusion, three key elements must be satisfied:

1. The defendant’s conduct must be intentional, which includes acts of recklessness.
2. The defendant must have invaded, without lawful justification, the plaintiff’s private affairs or concerns.
3. A reasonable person would regard the invasion causing distress, humiliation, or anguish as highly offensive.

Notably, proof of actual loss flowing from the breach is not an element of the cause of action for intrusion upon seclusion. This is important because, generally, to sustain a lawsuit in Ontario, a claimant needs to assert the breach of a recognized legal right or obligation and demonstrate that he or she has suffered a quantifiable loss as a result of the breach. Not so for intrusion upon seclusion. The Court of Appeal held that a victim of invasion of privacy could collect monetary damages without having suffered a quantifiable loss. Because damages will be for “moral” harm, the Court of Appeal capped the amount of damages at $20,000 but left open the possibility of awarding aggravated or punitive damages in exceptional cases.

Ontario’s recognition of the tort of intrusion upon seclusion has made Ontario a key jurisdiction in which to launch class actions for data breaches. For instance, if the personal information of 50 people is improperly accessed, a class of those 50 people can launch a class action and possibly recover a million dollars (not taking into account aggravated or punitive damages) just by proving the invasion of privacy, with no requirement to prove individual losses to class members. In fact, a class action has already been certified in the banking context for intrusion upon seclusion. In *Evans v The Bank of Nova Scotia [Evans]*, the Ontario Superior Court of Justice certified a class action lawsuit where a rogue bank employee accessed personal banking information from 643 of the bank’s clients for fraudulent purposes.

In *Jones v Tsige*, Jones did not sue the employer bank, just the rogue employee. However, the plaintiff in *Evans* seeks to impose vicarious liability on the employer for invasion of privacy by one of its employees. When the case goes to trial, at issue will be whether the employer bank took adequate precautions to protect clients’ personal information from misuse by the bank’s employees. Specifically, the court will be called upon to consider the standard of care that is owed by a bank to its clients with respect to safeguarding personal information from wrongful access by employees. This question gives rise to an interesting privacy conundrum with which the court will have to grapple: any obligation on an employer to protect personal information by monitoring its employees is likely to quickly bump up against an employer’s corresponding obligation not to breach the reasonable expectations of privacy of the employees themselves.

**Expanding the Tort of Intrusion upon Seclusion to the Health Care Sector**

Recently, the media has reported a string of violations of personal information held by health care facilities in Ontario. As a result (as one would expect in the wake of *Jones v. Tsige*), the health care facilities have come into the sights of plaintiffs’ class action lawyers.

In *Hopkins v. Kay*, patients from the Peterborough Regional Health Centre (the “Hospital”) launched a $5.6 million class action lawsuit against the Hospital, alleging that approximately 280 patient records were intentionally and unlawfully accessed and disseminated to third parties without the patients’ consent.

The Hospital, in response, brought a motion to strike the plaintiffs’ claim on the basis that it did
not disclose a cause of action. The Hospital argued that the claim was precluded by the *Personal Health Information Protection Act, 2004* [PHIPA],⁸ because the legislature intended *PHIPA* to be a comprehensive code that displaces any common law cause of action, including intrusion upon seclusion. Accordingly, the Hospital’s contention is that the plaintiffs’ only recourse is to bring a complaint to the Privacy Commissioner.

The Ontario Superior Court of Justice dismissed the Hospital’s motion to strike, concluding that it was not plain and obvious that the claim disclosed no reasonable cause of action. Its decision is under appeal, with the Court of Appeal expected to hear argument on December 15, 2014.

**Ontario’s Personal Health Information Protection Act**

*PHIPA* is Ontario’s privacy legislation that sets out the requirements that health information custodians must follow when collecting, using, and disclosing personal health information.

Part VI of *PHIPA* creates a comprehensive administrative scheme for the enforcement of the Act. Where a person believes that someone has breached a provision of *PHIPA*, the person may bring a complaint to the Privacy Commissioner. *PHIPA* gives the Privacy Commissioner discretion to determine whether or not to investigate the complaint. Upon completing an investigation (if the Privacy Commissioner chooses to investigate), the Privacy Commissioner may issue an order directing the person(s) who contravened *PHIPA* to take a variety of steps, including requiring a health information custodian to cease or implement certain practices.

*PHIPA* also creates a statutory right of action. Under *PHIPA*, a person may start a civil proceeding for damages for actual harm that the person has suffered as a result of the contravention of *PHIPA*, but only after the Privacy Commissioner has issued a final order. *PHIPA* gives the court the jurisdiction to hear the claim and make a damages award, limiting damages for mental anguish to $10,000. The statutory right of action has three important elements when compared to the test for the tort of intrusion upon seclusion:

1. The complainant must have suffered “actual harm” (whereas proof of harm is not required for the common law tort).
2. The right of action only exists after the Privacy Commissioner has issued a final order (whereas there is no such prerequisite to starting an action for the common law tort).
3. Mental anguish damages are limited to $10,000 (whereas the Ontario Court of Appeal contemplated damages up to $20,000 for reasonable distress, humiliation, or anguish).

**When Does a Statutory Scheme Foreclose a Common Law Right of Action?**

The issue before the Court of Appeal in *Hopkins v. Kay* will be whether *PHIPA* precludes a private right of action for the tort of intrusion upon seclusion—that is, whether the complainant must use the mechanism in *PHIPA* and only that mechanism.⁹

This case offers the Court of Appeal the opportunity to grapple with the age-old question of how to balance the role of the legislature with the role of the judiciary. It is uncontested that a role of the legislature is to make laws, while a role of the judiciary is to interpret legislation and enforce it. That said, courts also have the jurisdiction to adapt the common law in a manner consistent with the changing needs of society. The issue for the Court of Appeal will be whether the legislative intention underlying *PHIPA* is for *PHIPA* to provide the only remedies for data breaches of personal health information, or whether extending the scope of the tort of intrusion upon seclusion to cover data breaches of personal health information constitutes an appropriate step in the development of the common law in Ontario.
PHIPA and Intrusion upon Seclusion: Can They Coexist?

Brian Beamish, the Acting Commissioner, has said that the Office of the Commissioner will appear as an intervenor before the Court of Appeal and will argue that PHIPA does not prevent courts from hearing cases related to personal health information violations.

While it remains to be seen what the Court of Appeal will decide, it seems that the enforcement scheme in PHIPA can exist simultaneously with the tort of intrusion upon seclusion. When the purpose and the provisions of PHIPA are examined as a whole, it does not appear that the legislature’s intent was to displace the common law, particularly when we consider the state of the common law at the time of the enactment of the statute. PHIPA came into effect on November 1, 2004—eight years before the Court of Appeal’s decision in Jones v. Tsige. When the legislation was originally enacted, there was no common law tort for breach of privacy. Accordingly, the legislation did not take away any rights otherwise existing at common law. Rather, the legislation was additive in the sense that the legislature gave complainants a remedy where none existed at common law.

A statutory claim under PHIPA is quite different from a claim that can be brought for intrusion upon seclusion. To recover damages under PHIPA, a complainant must be able to prove that he or she suffered actual harm. If the court determines that the breach of PHIPA was willful or reckless, the court may include damages for mental anguish, capped at $10,000.

In contrast, proof of harm is not an element of the common law action for intrusion upon seclusion. The claimant only has to show that 1) the defendant’s conduct was intentional; 2) the defendant invaded, without lawful justification, the person’s private affairs or concerns; and 3) a reasonable person would regard the invasion as highly offensive.

If these three elements can be established, the plaintiff is entitled to damages of up to $20,000 and may be able to recover aggravated or punitive damages in exceptional circumstances.

What Are the Ramifications of Expanding the Scope of Intrusion upon Seclusion to the Health Care Sector?

The outcome of the pending appeal of the motion to strike the common law claim in Hopkins v. Kay will set a legal precedent for future data breaches involving personal health information. There are currently at least two other cases involving improperly accessed patient information that are waiting on the Court of Appeal’s decision. A $412 million class action lawsuit has been launched against the Rouge Valley Health System after parents alleged that their personal information was sold to a third party by two hospital employees. Similarly, a data breach occurred at the Sault Area Hospital when an employee inappropriately accessed patients’ medical records.

If the action is allowed to proceed to trial on the common law tort, the outcome of Hopkins v. Kay may have sweeping implications for the vicarious liability of employers for their employees’ actions. The issue of vicarious liability was not dealt with by the court in Jones v. Tsige because the plaintiff directly sued the employee, not the employer bank. In Hopkins v. Kay, the plaintiff class members have named both the hospital and the employees as defendants. As mentioned above, the issue of vicarious liability for privacy breaches committed by employees is also at issue in Evans. Whether one or both of these cases proceed to trial, and in which order, remains to be seen. Both of these cases ask the court to consider the steps an employer should take to prevent an intentional or reckless privacy violation.

How Employers Can Mitigate the Risk of a Data Breach by Their Employees

Employers should ensure that employees are properly trained on governing privacy legislation.
and internal data security policies and that such policies are enforced and continually reinforced. However, it is uncertain whether policies and training will be sufficient to protect an employer from vicarious liability in the event that a data breach occurs. Organizations should use encryption and other advanced technologies where possible. They should have strict access controls, which only allow those in the category of “need to know” to access sensitive records. A data breach vulnerability audit can be commissioned to point out a particular facility’s vulnerabilities and recommend practices and technology to address identified vulnerabilities. Cyber-liability insurance may be one way to cover losses arising from data breach. However, an insurance company will certainly perform an audit before providing coverage to make sure the employer is taking appropriate steps to reduce the chances of the insurer having to pay out on the cyber-liability policy. As well, reckless behaviour will no doubt have the insurer invoking an exclusion in the cyber-liability policy to deny coverage.

© 2014 Davis LLP

4 The following provinces have provincial statutory privacy torts: British Columbia (Privacy Act, R.S.B.C. 1996, c. 373, ss. 1(1)); Saskatchewan (The Privacy Act, R.S.S. 1978, c. P-24, s. 2); Manitoba (The Privacy Act, C.C.S.M. c. P125, ss. 2(1) and 2(2)); Newfoundland and Labrador (Privacy Act, RSNL 1990, c. P-22, ss. 3(1)).
5 PIPEDA, S.C. 2000, c. 5.
8 PHIPA, S.O. 2004, c. 3, Schedule A.
9 Note that the question comes before the Court of Appeal from a decision on a motion to strike for disclosing no reasonable cause of action, not from a trial on the merits or a summary judgment motion. Accordingly, it is possible for the Court of Appeal to avoid a full examination of the question by simply agreeing that it is not plain and obvious that PHIPA precludes a common law right of action, without providing a thorough analysis of the interaction between the statutory right and the tort.

Security Breach Involving Personal Information: What Type of Harm Can Lead to Damages Being Awarded?

Class actions triggered by security breaches involving personal information are growing in popularity. The recent decision rendered by the Honourable Justice André Prévost in the matter Sofio v. Investment Industry Regulatory Organization of Canada [IIROC]¹ clarifies what would be the necessary burden of proof in respect of the damage suffered by applicants at the authorization stage of a class action, in the event that there is no evidence that personal information was misused following the security breach.

The Facts Leading to the IIROC Decision

In February 2013, an employee of the Investment Industry Regulatory Organization of Canada (“IIROC”), which monitors all trading activity across the country, lost a laptop containing the personal information of approximately 50,000 customers of brokerage firms.² Soon after, a motion for authorization to institute a class action was filed on behalf of persons forming part of the following class—namely, all the individuals and legal persons that have fewer than 50 employees, whose personal information was lost in Quebec by IIROC or one of its employees in 2013 (the “Members”).
The laptop, which was never found, contained only one level of protection (password), not two levels (which would include a password as well as data encryption) as provided for by the IIROC policies. The plaintiff argued that IIROC, by its negligence, lost the personal information of the Members who were belatedly informed, and needed to take steps to mitigate the consequences of the breach, such as measures to prevent identity theft and to protect access to their bank accounts. However, the plaintiff was unaware of any cases where the personal information of the Members was used maliciously (for example, used for identity theft or other fraudulent activities).

**Damages Following a Security Breach**

There are usually two types of harm that may result from a security breach involving personal information: (1) a more objective type of harm such as financial harm, which would include fraud and identity theft, or which may include the time spent by the affected individuals to verify their banking information and statements, monitor their accounts, modify their passwords, and subscribe to credit watch services; and (2) a more subjective type of harm, which has an emotional component and can be summarized as stress, anguish or humiliation following the security breach. This latter type of harm may also involve the fear of affected individuals that their personal information may be misused or used for fraudulent purposes. The IIROC decision made clear the courts’ tendency to award damages only if one can prove that there were, in fact, fraudulent activities involving personal information following the security breach.

In light of the case *Mustapha v. Culligan of Canada Ltd.* in which it was discussed that psychological distress (subjective harm) suffered must be more important than mere annoyance in order for this type of damage to be compensated for, Prévost J.S.C. came to a similar conclusion, holding that the damages must be serious and prolonged. In a similar breach incident involving the National Bank of Canada, which triggered a class action in *Larose c. Banque Nationale du Canada*, the Québec Superior Court had authorized the class action. In that case, the National Bank of Canada had been robbed of three laptops, one of which contained personal information of about 225,000 mortgage customers. In their motion for authorization to institute a class action, the applicants alleged, in essence, the same mistakes as those alleged in the IIROC case: negligence in the protection of their personal information and undue delay in notifying customers. The damages claimed also showed some similarity to those alleged in the IIROC case: additional delays when making credit applications, obligation to monitor bank accounts, increased vigilance in providing personal information, obligation to inform other financial institutions, loss of time, and anxiety. The court nevertheless highlighted an important fact alleged in the motion for authorization in IIROC, which clearly distinguishes that case from IIROC—namely, the evidence of identity theft. Unlike in IIROC, it was alleged that the identity of at least one member of the group had been stolen, triggering the assumption that this situation may also apply to others.

The court in IIROC also took into account the case of *Mazzonna v. DaimlerChrysler Financial Services [Mazzonna]* to determine whether authorization should be granted. In Mazzonna, a record containing personal information of DaimlerChrysler customers had been lost by a courier while delivering it to a credit agency. In its motion for authorization to institute a class action, Mazzonna criticized DaimlerChrysler in a way similar to that in IIROC. In Mazzona, because no identity theft or fraud associated with the loss of the record had been reported, the Québec Superior Court did not authorize the class action, because the damages alleged by the petitioner were, *prima facie*, the kind of ordinary annoyances and anxieties (and therefore did not constitute “compensable” damages).
While the doctrine and jurisprudence recognize that subjective harm or the type of moral damage such as stress, emotional trauma, trouble, hassle, and inconvenience can be compensated for, a great deal of discretion is awarded to the judge for the assessment of such damages. For example, in recent class actions, courts have recognized the possible existence of damages in cases involving unlawful work stoppages and unjustifiable delays in the public transport services or failure by a tour operator to meet certain of its obligations. In these cases, the non-pecuniary damages generally covered the accumulated inconveniences, such as stress or anger associated with delay or uncertainty, late appointment or work arrivals, fatigue and discomfort caused by the fact of having to walk (despite weather conditions) for a longer period than expected, feeling of dependence and humiliation of being held hostage, and discomfort and stress associated with waiting in an airport for several hours or days.

Authorization of the Class Action Dismissed

The authorization of a Class Action in IIROC was dismissed for the main reason that the criterion of authorization stipulated by art. 1003(b) of the Code of Civil Procedure of Quebec was not met: the applicant failed to prove that the facts alleged seem to justify the conclusions sought. At the authorization stage, the applicant has to establish that he appears to be entitled to the right that he is exercising. Although the claim may, in fact, ultimately fail, the action should be allowed to proceed if the applicant has an arguable case in light of the facts and the applicable law.

The applicant’s legal rationale was as follows: (1) IIROC allegedly committed wrongdoings by losing the laptop, failing to ensure maximum protection of the Members’ information contained therein, and delaying notification to the Members; (2) the Members suffered damages, including time spent doing monthly checks of bank accounts and credit cards; and (3) the damages suffered by the Members are directly related to the wrongdoings committed by IIROC.

The court considered the damages alleged by the applicant to be part of life in our 21st century society when the theft and misuse of personal information are almost daily reported in the news. Since such data are easily accessible on the Internet, monthly verifications of bank accounts and credit cards are not uncommon. Checking for irregularities in mailed statements should also be a routine. While the applicant also claimed to have suffered stress, following the incident, the request for authorization offered no details in this regard. Therefore, the court concluded that the applicant failed to prove harm or an injury for which damages may be awarded. The court also considered the fact that to date, no identity theft or fraud resulting from the loss of the laptop by IIROC had been reported. The court considered the stress of the events alleged in the motion for authorization as failing to meet the criteria set forth by s. 1003 b) of the Quebec Code of Civil Procedure and thus not to being an injury for which damages could be awarded.

Takeaways for Businesses

IIROC will make it more difficult for privacy class actions to be authorized following a security breach involving personal information unless there is evidence that the identity of one of the class member was stolen and it can be proven that the damages caused were greater than the stress of verifying bank accounts and credit card statements.

Although businesses may find the IIROC decision reassuring, they should note that the breach response plan in effect subsequent to the breach, including IIROC’s reaction to the breach, were taken into account by the court when dismissing the motion for authorization to institute a class action. The fact that affected individuals were properly notified and that measures were quickly taken to protect the
individuals (free credit monitoring, fraud alerts, etc.) was taken into account by the court: a press release was published; a letter was sent to customers, informing them of the theft and asking for their vigilance; a notice of incident was reported to both Equifax and TransUnion; and the Privacy Commissioner was informed.

The class action might have been authorized if the organization had failed to take appropriate measures and/or if there had been proof of misuse of the Members’ identity. Incidentally, it should be noted that punitive damages might be granted in certain circumstances, regardless of the absence of compensatory damages. The aggregate sum granted to each class member as punitive damages may be extremely costly for organizations defending a privacy class action.

Furthermore, while not every security breach will lead to the authorization of a class action, an organization can ignore neither the costs of responding to a breach nor the reputational damages resulting from it. For instance, it has been recently reported in the Wall Street Journal that following the recent Home Depot security breach, the cost of the investigation, credit monitoring service, call center staffing, and other breach response and breach management steps amounted to approximately $62 million. As far as the reputational damages, the shares of Home Depot ended up being 0.86 per cent lower on the New York Stock Exchange upon the announcement of the breach, wiping out approximately $1 billion of Home Depot’s total market value on September 8, 2014. However, on the same day, S&P 500 was down only 0.28 per cent.

© 2014 McMillan LLP
“Objectively Reasonable” and Privacy: Recent Developments

The ubiquitous and rapidly evolving nature of technology has recently necessitated serious consideration of our “reasonable expectation of privacy”. This concept is at the core of Canadian privacy law. In particular, the concept is a key part of the Canadian Charter of Rights and Freedoms (the “Charter”) test for s. 8, the right to be secure against unreasonable search and seizure. The Supreme Court of Canada (“S.C.C.”) grappled with these questions in R. v. Cole1 and R. v. Vu,2 and more recently, in the British Columbia and Ontario Courts of Appeal, applied these Charter principles to couriered packages and USB keys in R. v. Godbout3 and R. v. Tuduce,4 respectively.

In R. v. Cole, the S.C.C. found that employees can reasonably expect some level of privacy with regard to personal information stored on work computers, but the reasonableness of their expectation is impacted by the context in which personal information is placed on an employer-owned computer and the customs of the workplace, factors that the court called “operational realities”.5

In R. v. Vu, the S.C.C. took privacy rights on personal computers one step further, finding that police must obtain prior judicial authorization for a computer search. Police must be able to satisfy the authorizing justice that they have reasonable grounds to believe that any computers they discover will contain the evidence sought.

In R. v. Godbout and R. v. Tuduce, the courts continue to grapple with finding the elusive limits of the “reasonable expectation of privacy” standard.

R. v. Godbout: Reasonable Expectations for Couriered Packages

A reversal of the trend set by R. v. Cole and R. v. Vu occurred in the R v. Godbout decision wherein the British Columbia Court of Appeal (“B.C.C.A.”) found that the consignee of a couriered package had no reasonable expectation of privacy with regard to its contents. Mr. Godbout was sent a package through the DHL courier company from a Mr. Calkins, who signed a shipping contract containing a term that the company or a government authority could search the package without notice. Mr. Godbout never interacted with DHL or agreed to the terms of the shipping contract. The company opened the box and called the police, who searched it and found illegal drugs. They repackaged and delivered it to Mr. Godbout, who opened it and was subsequently arrested on drug charges.

Mr. Godbout challenged the lawfulness of the search under s. 8 of the Charter, which protects the right to be secure against unreasonable search and seizure. In order to be protected under s. 8, one must have an objectively reasonable expectation of privacy in the object searched.

The court found that neither Mr. Calkins nor Mr. Godbout had any reasonable expectation of privacy because DHL accepted the package for delivery pursuant to the certain explicit contractual terms that allowed DHL to search the contents of the package. The court found that the contractual term “negated any objectively reasonable expectation of privacy” that either Mr. Calkins or Mr. Godbout could assert, stating, “[t]he fact that the appellant may not have known of the terms of shipment does not make his subjective expectation objectively reasonable”.6 Thus, the terms of the shipping contract ultimately governed the s. 8 rights of both Mr. Calkins and Mr. Godbout despite

Roland Hung
Associate
McCarthy Tétrault LLP
Co-author: Kimberly Macnab
Articling Student
McCarthy Tétrault LLP

122
the fact that only one of them had seen, or had any way of knowing, the terms of that contract.

This decision seems to suggest that an individual can sign away his or her privacy rights, which may affect how organizations can structure certain contracts to allow them to monitor or search its customers or employees.

**R. v. Tuduce: Reasonable Expectations for USB Keys**

In another technologically charged case, *R. v. Tuduce*, the Ontario Court of Appeal (“Ont. C.A.”) pondered the similarities between USB keys and computers with regard to whether police should require a specific search warrant and found that police required specific prior authorization before searching an electronic device. The Ont. C.A. considered the factors discussed in *R. v. Vu* that distinguish personal computers from other “receptacles” covered under search warrants and applied them to USB keys. They considered that large amount of data can be stored on USB keys, data can be left on the keys without the user’s knowledge, and the user cannot be in complete control over which files an investigator will be able to find on the key. In particular, the court found that a personal USB arguably engages a more serious privacy concern than a work computer, because it is neither owned by the employer nor is subject to the terms and conditions of use imposed by employers on work computers.7

However, the court did not discuss other storage devices or electronic “receptacles” that may or may not be provided by employers. What of the cell phones commonly provided by employers?8 Larger USB storage devices or external hard drives may be provided by employers; however, what level of privacy will be considered objectively “reasonable”? The storage capacity of USB keys has massively increased over the last decade; the courts are attempting to keep up with our ever-increasing ability to store vast amounts of personal data on devices that we fit into a pocket.

**Significance**

Most often, our highest court finds occasion to deal with these types of privacy issues in criminal law cases, where the accused objects to the procedure by which authorities have obtained evidence. However, private corporations and employers should be aware that developments in Charter jurisprudence can be important indicators of best practices and employee rights when it comes to privacy concerns. The line between personal devices and employer-issued technology becomes more and more blurred as the divide between home and office narrows. Employers must caution themselves against the potential privacy infringements enabled by superior employee-monitoring capacity and define “acceptable use of technology” policies in order to clearly delineate the lines between personal and office use on work desktops, laptops, cell phones, USB keys, and any other aids to working remotely that they may provide. Courts’ ability to keep up with changing technology will always be limited; employers must be able to proactively consider the myriad privacy issues that can arise in the context of employee devices.

© 2014 McCarthy Tétrault LLP

---

5. In a wrongful dismissal case outside of the Charter context, the Alberta Court of Appeal in *Poliquin v. Devon Canada Corporation*, [2009] A.J. No. 626, 2009 ABCA 216, found for the employer where an employee was dismissed with cause due to inappropriate use of his work computer. The court stated, “[t]he workplace is not the employee’s home; and employees have no reasonable expectation of privacy in their workplace computers [at para. 45]”.
8. The Alberta Office of the Information and Privacy Commissioner found that an employer improperly traced an employee’s personal phone calls, primarily because there was no official workplace phone use policy: *Order P2013-03*, 2013 CanLII 66186.
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