Supreme Court Grants Enhanced Access to Justice for Victims of Cyberbullies

On September 27, 2012, the Supreme Court of Canada released its decision in *A.B. v. Bragg Communications Inc.*, an important constitutional case at the intersection of defamation law and children’s rights.

A.B., the anonymous plaintiff, is the victim of cyberbullying. In March 2010, she discovered that someone had posted a fake Facebook profile using her picture, a slightly modified version of her name, and other identifying particulars. The Facebook profile made unflattering commentary about A.B.’s appearance and included sexually explicit references. At the time, A.B. was 15 years old.

A.B.’s father, on her behalf, sought disclosure of the IP address used to post the Facebook profile. A.B. intended to sue the cyberbully for defamation. She asked the court to permit her to sue anonymously and to ban publication of the fake Facebook profile. The *Halifax Herald* and Global Television opposed her request on the grounds that both of the requested privacy measures violated the freedom of the press. The Nova Scotia courts agreed. In their view, there was insufficient evidence of specific harm to A.B. that would justify a press ban or anonymous proceedings.

A.B. appealed to the Supreme Court of Canada. In a unanimous judgment, the court granted A.B.’s request to sue anonymously and banned publication of any identifying details from the fake Facebook profile.
The open courts principle and the freedom of the press are protected by the Canadian Charter of Rights and Freedoms. In order to grant a publication ban that would impair this hallmark right, the court had to be persuaded that A.B.’s interests justified that infringement. In this case, the court identified two such interests: privacy and the protection of children from cyberbullying.

A.B.’s privacy interest was tied to both her age and the nature of the victimization she sought protection from (which the court described as “relentlessly intrusive humiliation of sexualized online bullying”). The court found that, based on reason, logic, and common sense, A.B. would suffer objective harm if her identity was disclosed given the “psychological toxicity” of cyberbullying.

Further, declining the confidentiality order in this case would also harm children generally and the administration of justice, given that a bullied child may not pursue “responsive legal action.” As the court concluded:

> If we value the right of children to protect themselves from bullying, cyber or otherwise, if common sense and the evidence persuade us that young victims of sexualized bullying are particularly vulnerable to the harms of re-victimization upon publication, and if we accept that the right to protection will disappear for most children without the further protection of anonymity, we are compellingly drawn in this case to allowing A.B.’s anonymous legal pursuit of the identity of her cyberbully.

The decision is a modest step forward for the court as Canadian law continues to adapt to the challenges presented by the Internet and social media. It is a useful and prominent reminder for clients that courts will routinely grant orders to disclose customer information where there is sufficient evidence linking an IP address to defamatory Internet material. The case is also an important reminder that material posted on the Internet is never truly anonymous and that great care should be taken when making the decision to publish or post material online—particularly, when the subject of any published material is a young person or that published material might be defamatory. Finally, this case is an important victory for children’s rights advocates in that it empowers children to use legal means to combat cyberbullying.

[Editor’s note: Jeffrey Leon and Ranjan Agarwal were counsel to UNICEF Canada, interveners in the appeal before the Supreme Court of Canada in support of A.B.]
Tagging You: Guidelines for Facial Recognition in Canada and the United States

Introduction

In October, the U.S. Federal Trade Commission (“FTC”) issued a staff report entitled “Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies.” Organizations operating in Canada and the U.S. should consider carefully the guidance in the FTC Staff Report. They should also have regard to earlier guidance, “Data at Your Fingertips,” issued by the Office of the Privacy Commissioner of Canada (“OPC”) regarding the collection of biometric information, including facial information.

This article examines some of the privacy issues that facial recognition technologies present and compares and contrasts the U.S. and Canadian guidelines on the use of these technologies.

A question of liberty and control

The Supreme Court of Canada has held that privacy is at the heart of liberty: “[R]estraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.” Very recently, the Supreme Court of Canada reiterated that the underlying values of dignity, integrity, and autonomy are fostered by protecting a biographical core of personal information from the state.

Private sector privacy advocates may argue that those same values require that individuals have the right to protect (and control) a biographical core of personal information from private sector organizations should they choose to do so.

Facial recognition technologies create new challenges for privacy protection. In public spaces, there is, of course, the possibility that people might recognize you. However, one of the features of urban spaces is that an individual can often move around in a way that is relatively anonymous.

Advanced facial recognition technologies have the potential to match images across platforms. Pervasive private sector passive security video surveillance, facial recognition in digital signage, and photos and videos uploaded to social media could, in theory, be combined and crossmatched. The ability to control the use of one’s own image and the expectation of being able to move around in relative anonymity could, in theory, be lost. Moreover, the collection of and crossmatching of facial information by the private sector could be combined with public sector data from government-issued identification and licensing activities, leading to concerns of mass surveillance. The data need not even be conscripted by the government if it is available publicly or provided to the government voluntarily.

In Canada, we have already had some experience with the potential use of combining private sector data with public sector databases for law enforcement purposes. Following a riot in Vancouver, the Insurance Corporation of British Columbia (“ICBC”) (a Crown corporation subject to private sector privacy legislation in British Columbia) offered its facial recognition technology to assist police in comparing images of individuals alleged to have participated in the riot with images in its database of drivers. ICBC is the provincial insurer for drivers in British Columbia. ICBC wasn’t being entirely selfless. Having paid out on insurance claims, it was subrogated to its insureds for claims against rioters who caused the damage. The plan was to take images contained on surveillance video and images uploaded to social media and compare them using facial recognition technology with those in ICBC’s database of driver photos. The Office of the Information and Privacy Commissioner of British Columbia (“IPC”) responded with an investigation that concluded that ICBC did not provide adequate notice of this potential use to citizens and that it must receive a warrant, subpoena, or court
order before using facial recognition software to assist law enforcement.\(^5\)

Notwithstanding the concerns raised by the IPC in British Columbia, it is easy to be drawn into being overly critical of the use of facial recognition. As the dissenting Commissioner, J. Thomas Rosch, stated in an appendix to the FTC Staff Report there is, as yet, little evidence that facial recognition technologies are being systematically “misused.”\(^6\) In Commissioner Rosch’s view, the Staff Report was, among other things, premature.

It is also important to acknowledge that reasonable people may disagree on a number of the values underlying suspicion of facial recognition technology. Some may be sceptical as to whether facial recognition technologies present any material threat to liberty. Others may be sceptical about whether the relative anonymity that urban life affords has anything to do with liberty. Reasonable people may also differ in the extent to which they are prepared to submit to surveillance for the purposes of public safety.

Moreover, when critiquing facial recognition technologies, it is important to acknowledge that not all facial recognition technologies are the same and not all uses have the same degree of intrusion on an individual’s ability to be “left alone” in relative anonymity. As the FTC Staff Report notes, there is a spectrum of technological sophistication and a spectrum of uses.\(^7\) Facial recognition technologies may simply detect and locate a face in an image. Other technologies and uses may be able to identify demographic characteristics, moods, or emotions of the person to deliver targeted advertising.

**FTC: Technological Neutrality but Greater Transparency and Choice**

For the most part, the FTC Staff Report is neutral with respect to the use of facial recognition technologies in consumer settings. The FTC acknowledges that facial recognition can be used “in ways that benefit consumers by providing them innovative products and services, such as the ability to try beauty products by uploading their faces to the Web, the ability to target search results, and the ability to organize and manage photos.”\(^8\) Facial recognition technology can also be used to enhance privacy protection. The technology can be used for authentication of mobile devices and to blur images of individuals captured in video.\(^9\)

However, the FTC is also concerned about potential erosions of privacy in ways that are unfair to consumers. In providing guidance, the FTC has organized its analysis around three core principles:

1. “Privacy by Design: Companies should build in privacy at every stage of product development.”\(^10\)

The FTC Staff Report states that the transmission of facial information should be encrypted or secured to protect against intrusion from a hacker who could view the images in real time.\(^11\) Organizations should also attempt to prevent unauthorized scraping of images.\(^12\) If images are retained, there should be reasonable data security protection in place, and the images should be subject to destruction once they are no longer necessary for the purpose for which they are collected.\(^13\)

2. “Simplified Consumer Choice: For practices that are not consistent with the context of a transaction or a consumer’s relationship with a business, companies should provide consumers with choices at a relevant time and context.”\(^14\)

The FTC considers a consumer’s face to be a persistent identifier in the sense that it can’t simply be changed in the way that other identifiers can be, such as a credit card number or a tracking cookie.\(^15\) Accordingly, it is critical that there be meaningful and informed choice.

The FTC Staff Report suggests that “walk-away choice” is sufficient if (a) the technology is being used to gather demographic information (age and gender), (b) images are not stored, and (c) the organization has been sufficiently transparent about its activities.\(^16\)

By contrast, using facial recognition technologies for identification purposes requires affirmative express consent.\(^17\) Similarly, using an image in a ma-
terially different way (for example, a new use) would require affirmative express consent.\textsuperscript{18}

3. “Transparency: Companies should make information collection and use practices transparent.”\textsuperscript{19}

The FTC is concerned that the public is not well educated in the uses of facial recognition technology. For example, the FTC is of the view that facial recognition technologies in digital signage would not be consistent with reasonable consumer expectations.\textsuperscript{20} Therefore, it is important to provide prominent notice so that consumers have a meaningful choice as to whether they want to come into contact with these types of technologies.\textsuperscript{21}

The FTC Staff Report states that a notice should be prominently placed at the entrance to the store or at the entrance to the area of the store in which the technology is being used.\textsuperscript{22} When used with digital signage or other novel applications, a notice should be placed near the digital signage or area of novel use.\textsuperscript{23} The notice should state the purpose of the technology and how consumers can find out more information about the technology and the practices of the company operating the signs in that venue.\textsuperscript{24}

If facial recognition is used on images submitted in social media, the operators of those social networks should provide consumers with an easy-to-find, meaningful choice and the ability to turn off the feature and delete biometric data.\textsuperscript{25}

**Canada’s Focus on Proportionality**

The Canadian guidance from the OPC contains similar themes. Individuals should be informed that facial recognition is being collected.\textsuperscript{26} If facial information will be used for other purposes than those disclosed at collection, additional consent will be required.\textsuperscript{27}

However, unlike the U.S. approach, the Canadian approach by the OPC requires that organizations be prepared to justify the use of facial recognition. In part, this is probably because subs. 5(3) of the Personal Information Protection and Electronic Documents Act [PIPEDA]\textsuperscript{28} provides that “[a]n organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances” [emphasis added].

In determining what is reasonable, the OPC encourages organizations to apply a four-part test:

1. Is the use of the technology demonstrably necessary to meet a specific need?
2. Is the use of the technology likely to be effective in meeting that need?
3. Would the loss of privacy be proportionate to the benefit gained?
4. Is there a less privacy-invasive way of achieving the same end?\textsuperscript{29}

The application of this test means that technologies such as facial recognition are not to be employed simply because they are efficient, convenient, or cost effective.\textsuperscript{30} Instead, the OPC suggests that facial recognition should be “essential for satisfying [a particular] need.”\textsuperscript{31} Any loss of privacy must be proportional to the benefit obtained from the technology. If the benefit to the organization of using facial recognition is minor, then it will be difficult to justify the loss of privacy from technologies that may be used to identify individuals. By contrast, technologies that are being deployed for privacy-enhancing purposes (such as blurring faces in photos) or that are based simply on sensing that there is a person facing a digital signage may be much easier to justify in comparing the cost to an individual’s privacy to the benefit to the organization from the technology.

**Implications of the Philosophical Difference**

The Canadian focus on the contextual reasonableness of facial recognition technologies is an important philosophical difference in approach with practical implications. In particular, it may be necessary in Canada to more carefully calibrate the use of facial recognition technologies in consumer settings to a clearly defined need.

Although the use of facial recognition technologies may be more restricted in Canada, they can be used
in privacy-enhancing ways, as demonstrated by the experience in Ontario casinos.

The Ontario Lottery and Gaming Authority (“OLG”) facial recognition program is instructive. OLG maintains a voluntary self-exclusion program for persons who do not want to be admitted to gaming sites. In collaboration with the Information and Privacy Commissioner and the University of Toronto, the OLG developed a facial recognition program that uses biometric encryption. A biometric pointer key is created from a sample image. The sample is then discarded. The identity of the person can only be unlocked by the biometrically encrypted pointer key derived from a person’s live image. Images that do not unlock a self-excluded gambler’s photograph are discarded, thereby protecting the privacy of the general public visiting the casino. If a likely match is identified, staff will check identification, which eliminates false positives.  

Conclusion

Facial recognition technologies won’t be going away. They are novel, useful, and fun for consumers. However, developers should consider engaging in a privacy impact assessment with respect to any deployment of these technologies for new uses and applications.

---

7. Ibid. at pp. i–ii.
8. Ibid. at p. 7.
9. Ibid.
10. Ibid. at p. 2.
11. Ibid. at pp. 13 and 17.
12. Ibid. at p. 17.
13. Ibid. at pp. 11–12.
14. Ibid. at p. 2.
15. Ibid. at p. 19.
16. Ibid. at pp. 15–16.
17. Ibid.
18. Ibid.
19. Ibid. at p. 2.
20. Ibid. at p. 15.
21. Ibid.
22. Ibid.
23. Ibid.
24. Ibid. at p. 19.
25. Ibid.
26. Supra note 2 at p. 3.
27. Ibid.
29. Supra note 2 at p. 6.
30. Ibid. at p. 7.
31. Ibid.
32. For more information see: Ann Cavoukian and Tom Marinelli, “Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept” (Toronto: Information and Privacy Commissioner, November 2010), supra note 2.
When “Private” Isn’t Private: Discovery in the Age of Facebook

Parties to litigation cannot hide behind Facebook privacy controls during the discovery process according to a recent decision of the British Columbia Supreme Court. In *Fric v. Gershman*, the plaintiff in a motor vehicle accident claim was ordered to review and produce thousands of photos depicting her travelling and participating in social and sports activities, including those from her private Facebook account.

In its ruling, the court addressed several key issues that define the developing area regarding disclosure of information on social networking sites such as Facebook.

First, courts have held that the information contained on Facebook must be relevant to an issue in dispute. In *Fric*, the court held that the plaintiff had put her physical functioning and activity level in question by claiming damages for loss of amenities of life, loss of mobility, and diminished earning capacity as the result of pain and fatigue. Photos depicting the plaintiff, a recent law school graduate, travelling or engaging in social and sports activities, such as an inter-university competition known as Law Games, were relevant to her claims for physical impairment and social withdrawal.

However, mere proof of the existence of a Facebook profile does not entitle a party to gain access to all information in the profile. Courts will not grant “fishing expeditions” simply because an individual’s general health, enjoyment, and employability are at issue. Courts have granted production where the plaintiff has acknowledged the existence of relevant information in his Facebook profile or where the public portion of a Facebook profile contains relevant information that suggests it is likely the private part of the profile contains similar information.

In *Fric*, the plaintiff gave evidence at her examination for discovery that she had posted photos of herself travelling and participating in events such as Law Games on her Facebook profile. As her physical and social capacity were relevant, an order was granted requiring her to produce photos where she is participating in Law Games and on vacation.

Privacy concerns also arise from the production of information stored on Facebook. For instance, courts have held that while a party may be required to produce information from their Facebook profile, they are not required to give up their username and password to the opposing party. Third-party privacy rights must also be given special attention. The plaintiff in *Fric* was allowed to edit her photos to protect the privacy of her friends and others appearing in her photos. Similarly, commentary associated with the plaintiff’s photographs posted on Facebook was not ordered to be produced. The probative value of Facebook commentary was outweighed by the interest in protecting the private thoughts of the plaintiff and third parties.

Two key themes emerged from the decision. Firstly, in the age of digital media, the courts are mindful of the proportionality of requiring parties to disclose potentially thousands of photos versus the benefit of such disclosure. Where production would require the review of hundreds of documents and potentially delay trial, courts have declined to order production. However, in *Fric*, the court dismissed the plaintiff’s concern that the court’s order would require her to review over 12,000 photographs, in addition to several hundred more on her Facebook profile.

Secondly, where there is a real and legitimate concern that information could be permanently deleted...
from Facebook, courts may issue an injunction or preservation order until the information has been produced.

**What Is It All Worth in the End?**

Individuals required to disclose photos from their Facebook account depicting them as physically active and socially engaged should not despair however. Courts are reluctant to place much weight on mere snapshots of an individual's life. In *Guthrie v. Narayan*, the court held Facebook photos of the plaintiff's recent Las Vegas trip were of “limited usefulness,” noting the plaintiff was “seeking compensation for what she has lost, not what she can still do” and that “she should not be punished for trying to get on with her life.”

As *Fric* and recent cases have demonstrated, where there is evidence of information relevant to an issue in dispute, an order for production will likely be granted, regardless of the level of Facebook privacy protection. However, “fishing expeditions” are still prohibited, and production may be subject to conditions to protect privacy interests, including those of third parties. In the end, the weight such information has at trial may be as fleeting as a Facebook status update.

© McMillan LLP 2012

---


---

**Supreme Court Recognizes Employee Privacy in Workplace Computers**

The prevalence of computers in the workplace and employees’ increased use of them gives rise to questions about the existence of privacy rights in materials stored, accessed, or transmitted using employer-owned hardware and network systems. In tension with assertions of privacy, employers claim that the misuse of workplace computers to view or send inappropriate, illegal, or even merely distracting material interferes with their duty to provide a safe and productive workplace and with their right to protect the integrity of their business operations. These concerns have led to the implementation of a range of monitoring measures targeting employee e-mail and Internet activities.

The Supreme Court of Canada (the S.C.C.) addressed these competing interests in the context of workplace computers in its *R. v. Cole* decision on October 19, 2012. The Supreme Court held that Canadians may reasonably expect privacy in information contained on workplace computers where personal use is permitted or reasonably expected. The court described such information as “meaningful, intimate, and touching on the user’s biographical core.” While computer and data ownership, workplace policies and practices, and technologies in place for monitoring network activity may diminish an employee’s expectation of privacy, such “operational realities” will not extinguish the expectation of privacy in its entirety.
Legal Landscape prior to Cole

Before Cole, there was limited Canadian jurisprudence on employee privacy rights on workplace computers, particularly at the appellate level. In France (Republic) v. Tfaily, Justice Simmons recognized a reasonable expectation of privacy in personal electronic data stored by professors on university-owned computers. This aspect of the ruling was based on the terms of the collective agreement governing the employment relationship. In Poliquin v. Devon Canada Corp., the Alberta Court of Appeal allowed an employer’s application for summary dismissal of a lawsuit for wrongful termination, in part, on the grounds that the employee at issue had no reasonable expectation of privacy in his workplace computer. Emphasizing an employer’s right to protect the professional, ethical, and operational integrity of its business operations, the court held that “… an employer is entitled not only to prohibit use of its equipment and systems for pornographic or racist purposes but also to monitor an employee’s use of the employer’s equipment and resources to ensure compliance.”

American court decisions and Canadian labour arbitration decisions demonstrate a similar reluctance to recognize employee privacy rights on workplace computers. Recent American cases such as Falmouth Fire Fighters’ Union Local 1497 et al. v. Town of Falmouth et al. and People v. Kent suggest that a reasonable expectation of privacy will be found only where an employer has provided positive assurances or recognition of the confidentiality of materials accessed, transmitted, or stored using an office computer. In the earlier and oft-cited decision of Smyth v. Pillsbury Co., the court reached a more extreme result in denying privacy protection for employee communications transmitted over workplace networks notwithstanding assurances from the employer that such communications would remain confidential and privileged.

In the labour context, arbitrators have regularly declined to recognize a reasonable expectation of privacy on workplace computers, emphasizing employer ownership of computer hardware and network systems. Employers instituting acceptable use or electronic monitoring policies benefit from the generous criteria for the unilateral adoption of workplace rules set out in KVP Co. v. Lumber & Sawmill Workers’ Union, Local 2537 (Veronneau Grievance). Under these criteria, a rule must be clear, reasonable, and not inconsistent with the collective agreement. Further, the employer must notify employees affected by the operation of the rule and must enforce the rule consistently from the time that it is introduced.

Even where the terms of an employer policy on computer and network use are not made clear to an employee, Briar v. Canada (Treasury Board) [Briar] and Consumers Gas v. C.E.P. suggest that a “common sense” test may be applied in assessing the employee’s conduct. The arbitrator in Briar, Taylor, Q.C., said at para. 74, “even if it could be said that [the grievors] were unaware of the policies, they distributed material which common sense dictated was inappropriate to distribute at a workplace and, in particular, at a correctional facility where they are supposed to set an example of socially acceptable behaviour.”

Supreme Court of Canada’s Decision in Cole

Cole concerned a teacher who was criminally charged with possession of child pornography following the discovery of nude, sexually explicit photographs of a female Grade 10 student on the hard drive of his school-owned laptop. The photos were found by a computer technician employed by the school board. The technician was responsible for ensuring the integrity of the network system. The laptop, compact discs containing the photos, a screenshot of the laptop including the file path and thumbnail pictures, and temporary Internet files pulled from the teacher’s browsing history were ultimately provided to the police who proceeded with a warrantless search. The teacher challenged the search and sought to exclude the evidence based on an alleged violation of his right to be free from unreasonable search and seizure under s. 8 of the Canadian Charter of Rights and Freedoms.
The S.C.C.’s decision, while set in the context of a criminal case, outlines the scope of an employee’s reasonable expectation of privacy for personal information on workplace computers. The court confirmed the Ontario Court of Appeal’s finding that Canadians do, in fact, have a reasonable expectation of privacy on workplace computers, at least where personal use is permitted or reasonably expected.

Referring to the 2010 decision in *R. v. Morelli*, Justice Fish, for the unanimous court on this issue, said that any computer used for personal purposes contains “… information that is meaningful, intimate, and touching on the user’s biographical core,” including financial, medical, and personal information. The court recognized that, in particular, computers used for Internet browsing reveal specific interests, likes, and propensities about the user.

While workplace policies and practices can diminish an employee’s reasonable expectation of privacy, the court held that these policies are not sufficient to extinguish the privacy expectation. This “diminished expectation of privacy” is equally protected by s. 8 of the Charter. The same reasoning was applied with respect to school board ownership of the teacher’s laptop computer, as well as the technology in place at the school to monitor network activity.

To determine the existence and extent of the expectation of privacy, the court said one must look to the totality of the circumstances. In *Cole*, the nature of the information at issue and the fact that the accused was permitted to use his computer for personal use, both pursuant to policy and in practice, weighed in favour of a reasonable, although diminished, expectation of privacy.

The court found that the actions of the police in conducting a warrantless search violated the teacher’s s. 8 Charter rights. However, Fish J., for the majority, concluded that the admission of evidence would not bring the administration of justice into disrepute. In part, because the impact of the breach was decreased by the teacher’s diminished privacy interest in the laptop materials and because of the ultimate discoverability of the evidence based on the existence of reasonable and probable grounds to search.

**Conclusion**

The Supreme Court of Canada’s decision establishes that, where the employer permits or condones personal use of workplace computers, employees will have a reasonable expectation of informational privacy. That said, it remains to be seen what impact *Cole* will have on the admissibility of evidence and the employer’s ability to prove just cause in civil actions for wrongful dismissal.

Although *Cole* emphasizes that employer policies and practices will diminish rather than extinguish the expectation of privacy in workplace computers, it remains advisable for employers to implement clear and unambiguous technology and privacy policies and monitoring conventions with respect to the acceptable use of workplace computers. Employers should also ensure that monitoring policies comply with applicable privacy legislation, including employee notification of the purposes of monitoring and collection of information contained on workplace computers, as well as the use that will be made of information collected.

[Editor’s note: The authors wish to acknowledge the contribution of John Mather, Student-at-Law.]

4 Ibid. at para. 49.
12 Ibid. at paras. 2 and 58.
Balancing Rights of Privacy with Accommodation of Invisible Disabilities: Employers Have Rights and Employees Also Have Obligations

An employer’s duty to accommodate employees with disabilities to the point of undue hardship is well known and particularly challenging when it comes to accommodating employees with invisible disabilities, such as mental illness. What has been less thoroughly canvassed are the obligations of employees seeking accommodation, particularly when it comes to the disclosure of medical information that would otherwise be private. A recent arbitration board decision Complex Services Inc. (c.o.b. as Casino Niagara and Niagara Fallsview Casino Resort) v. Ontario Public Service Employees Union, Local 278 thoroughly and thoughtfully considers these very thorny issues and how they must be balanced.

At issue in the case were two competing grievances: a union grievance alleging discrimination and harassment in the accommodation process including the employer’s imposition of an unpaid medical leave of absence and an employer grievance alleging failure on the part of the grievor to provide medical evidence to support her accommodation demands. The grievor, a security associate, claimed two disabilities: one physical with respect to which the employer had implemented accommodation requirements and one mental that was the source of the dispute. The grievor advised the employer of the accommodation she required for her mental illness (which included certain shift times and days worked and “to only deal with one matter at a time” with respect to certain managers only and with union representation present), but, in no uncertain terms, refused to provide medical documentation in support for confidential medical privacy reasons.

In a unanimous decision, the chair of the arbitration panel, George Surdykowski, succinctly sets out each party’s respective rights and obligations in the accommodation process. His findings include the following:

- In the purely technical sense of the term, an employee has an ‘absolute’ right to keep her confidential medical information private. But if she exercises that right in a way that thwarts the employer’s exercise of its legitimate rights or obligations, or makes it impossible for the employer to provide appropriate necessary accommodation, there are likely to be consequences, because an employee has no right to sick leave benefits or accommodation unless she provides sufficient reliable evidence to establish that she is entitled to benefits, or that she has a disability that actually requires accommodation and the accommodation required. Although an employer cannot discipline an employee for refusing to disclose confidential medical information, the employee may be denied sick benefits, or it may be appropriate for the employer to refuse to allow the employee to continue or return to work until necessary such information is provided. [para. 86]

- [T]he Human Rights Commission’s Policy indicates the employee has an obligation to ask for accommodation and to provide sufficient information, including necessary otherwise private confidential medical information, to establish the accommodation required, and to participate in and facilitate both the search for and implementation of accommodation—whether or not the accommodation available is ‘perfect’ from the grievor’s subjective perspective. The employer has a legitimate need for sufficient information to permit it to satisfy its accommodation obligations. An employee can neither expect accommodation if she withholds the information to establish that she requires it, nor dictate the accommodation required. [para. 88]

- Accommodation is a matter of equal treatment required by the Code. It is not intended to be, and no employee is entitled to, a superior working arrangement merely because that is what she wants or thinks is best. [para. 89]
The cases demonstrate that the following otherwise confidential medical information will generally be required for accommodation purposes:

1. The nature of the illness and how it manifests as a disability (which may include diagnosis, particularly in cases of mental illness).

2. Whether the disability (if not the illness) is permanent or temporary, and the prognosis in that respect (i.e. the extent to which improvement is anticipated, and the time frame for same).

3. The restrictions or limitations that flow from the disability (i.e. a detailed synopsis of what the employee can and cannot do in relation to the duties and responsibilities of her normal job duties, and possible alternative duties).

4. The basis for the medical conclusions (i.e. nature of illness and disability, prognosis, restrictions), including the examinations or tests performed (but not necessarily the test results or clinical notes in that respect).

5. The treatment, including medication (and possible side effects) which may impact on the employee’s ability to perform her job, or interact with management, other employees, or customers. [para. 95]

It is in cases of invisible disability, particularly mental illness, that questions most often arise about an individual’s request for particular accommodation and the adequacy of supporting information. The employer is entitled to seek confirmation or additional information from an appropriate medical health professional to obtain further information if there is a reasonable and bona fide basis for doing so. … Although an [Independent Medical Examination] is a resource of last resort, there are cases in which one is necessary and appropriate. An employee who exercises her right to refuse the incontestably intrusive IME when one is objectively justified may find herself unable to continue or return to the work. [para. 118]

The decision is a balanced consideration of what is required to make the accommodation process succeed in cases of invisible disabilities. To the extent that it thoroughly outlines both the employer and the employee’s role in this process, it provides welcome guidance for employers.