Intrusion Upon Seclusion: Is an Employer's Request for Employee Medical Information an Invasion of Privacy?

Emma Phillips
Sack Goldblatt Mitchell LLP
June 2013

In a landmark decision last year, the Ontario Court of Appeal endorsed for the first time the right to bring a civil action for damages for the invasion of personal privacy in *Jones v. Tsige*, 2012 ONCA 32 (CanLII). This recognition of the tort of invasion of privacy cements an already clear direction in the common law towards recognizing that there must be some form of redress where the conduct of one party breaches another party's ability to control the collection and dissemination of his or her personal information.

Such a change in the landscape of privacy law could potentially have a significant impact on the law of the workplace, in particular in relation to the scope of the employer's right to access, use and disclose an employee's private medical information to determine fitness for work, accommodation requirements, or to administer health benefits. As such, this paper explores the first of the arbitral decisions to apply the findings in *Jones,* and what indications these cases give about how the tort of invasion of privacy may impact on employer obligations with respect to sensitive employee health information.

Two cases in particular, *Alberta and A.U.P.E. (Violation of Employee Privacy Rights) (Re)* (2012) 111 C.L.A.S. 98 (Sims) and *Complex Services Inc. and O.P.S.E.U., Local 278 (2011-0278-0015) (Re)* (2012) 110 C.L.A.S. 49*,* give a helpful indication of whether, and how, the newly recognized tort of "intrusion upon seclusion" affects established principles about when and how an employer

can view sensitive employee medical information. But while one case, *Alberta and A.U.P.E.,* stands for the proposition that employers have a positive obligation to safeguard private employee information and that a failure to do may give rise to liability, the second case, *Complex Services Inc.,* confirms the limits of employee privacy rights: so long as employers have a legitimate basis for seeking access to employee medical information, there is no "intrusion upon seclusion" and no compensable injury. As such, *Jones* appears not to change the existing law establishing when it is legitimate for the Employer to seek employee medical information; but it may give employees added recourse where employers step outside the bounds of what is reasonable and appropriate.

Jones v. Tsige and the Changing Landscape of the Common Law of Invasion of Privacy

In *Jones v. Tsige,* the parties, Sandra Jones and Winnie Tsige, were both employees of the Bank of Montreal. In 2009, Jones discovered that Tsige had been surreptitiously looking at her banking records. The two women did not know each other, but Tsige had formed a common-law relationship with Jones' former husband. Over a period of four years, and contrary to the Bank's policies, Tsige had viewed Jones' banking records at least 174 times. Jones asserted that her privacy interest in her confidential banking information had been "irreversibly destroyed" and claimed damages for invasion of privacy and breach of fiduciary duty, as well as punitive and exemplary damages.

In assessing Jones' claim, the Court adopted the approach of American jurisprudence which has recognized four separate branches to the tort of invasion of privacy:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

If upheld, the Court found, Jones' claim would fall into the first category of "intrusion upon seclusion", which captures the conduct of one who "intentionally intrudes, physically or

otherwise, upon the seclusion of another or his private affairs or concerns…if the invasion would be highly offensive to a reasonable person" (para. 19).

The Court noted that the question of whether the common law should recognize a cause of action in tort for invasion of privacy—including any of the four branches described above—has been debated for at least 120 years, but that there has been no clear acceptance by Canadian appellate courts of a distinct right of action for breach of privacy. Ultimately, the Court of Appeal found that given the evolution of Canadian law, including recognition by the Supreme Court of Canada of the value of privacy and its constitutional protection, it is now appropriate to acknowledge the tort of intrusion upon seclusion in Ontario (para. 65). The Court left open the possibility that the other three branches of the tort of invasion of privacy should be similarly recognized, since these were not at issue on the facts before it. The Court upheld Jones' claim, but limited her damages to $10,000.00, given that she had not suffered any pecuniary loss as a result of the wrong.

In coming to this finding, the Court found that there was a clear trend in the common law towards recognizing a tort of invasion of privacy and that a number of trial judges in Ontario had already refused to strike pleadings for invasion of privacy for disclosing no cause of action. In particular, the Court commented with approval on the case of *Somwar v. McDonald's Restaurants of Canada Ltd.*, in which an employee successfully sued his employer for breach of invasion of privacy after the Employer conducted a credit bureau check on the employee without his consent.

In recognizing a stand-alone tort of invasion of privacy, the decision in *Jones* goes a long way towards cementing an already clear direction in the common law towards recognizing that the law must provide some form of redress where the conduct of one party breaches another party's ability to control the collection and dissemination of his or her personal information. Of particular interest in the employment context is the Court's support for the reasoning in the *Somwar* case, in which an employer's misuse of an employee's personal information was found to be actionable. While *Jones v. Tsige* arose out of a relationship between two co-workers, and

not between an employer and employee, the Court's reliance on *Somwar* indicates that an illegal "intrusion upon seclusion" can also arise where an employer unreasonably uses or views an employee's private information without the employee's consent. Given this development in the law, the premise that employees do not enjoy an inherent right to privacy in the workplace is arguably no longer tenable, although that right must be assessed having regard to all of the circumstances, such as the employer's operational interests.

The Impact of *Jones v. Tsige* on an Employer's Access to Medical Information: Is a Request for Access to Sensitive Information an Intrusion Upon Seclusion?

Thus far, few labour arbitrators have addressed how the decision in *Jones v. Tsige* affects the rights of employees in organized workplaces. As noted, *Jones v. Tsige* does not arise in the context of a relationship between employer and employee or relate to private information collected by an employer from an employee. However, two recent cases apply the principles developed in *Jones* to the employment context, and may provide helpful insight into the impact of *Jones* on employer access to employee sensitive medical information.

In *Alberta and A.U.P.E. (Violation of Employee Privacy Rights) (Re)* (2012) 111 C.L.A.S. 98 (Sims), the arbitrator confirmed the positive obligation on employers to safeguard private employee information, and the liability of the employer for breaches of employees' right to privacy in their personal information. Following the discovery that fraudulent program cheques were being passed through a government program, an over-zealous investigator retained by the employer conducted credit checks on all employees in a particular department to see if any of the employees was experiencing "financial difficulties" and therefore would be more susceptible to carrying out a scheme to defraud the program (the investigation ultimately revealed that the scheme was being conducted from outside the organization and not by any employee). The investigator conducted the credit checks without the employees' consent and by using private employee information which had previously been submitted to the employer for an unrelated purpose.

The employer conceded there had been a violation of Alberta's *Freedom of Information and*

Protection of Privacy Act. The arbitrator held that an employer in possession of employee personal information has an obligation to "protect that information and ensure its use for only legitimate purposes" and that the misuse of such information, based on the principles set out in *Jones*, constituted a breach of invasion of privacy. However, given that the resulting unauthorized credit checks were not distributed further, only modest damages of $1250.00 were awarded to each employee affected.

While this decision does not arise in the context of employer access to medical information, the decision confirms that employers may only use private employee information in their possession for legitimate purposes (and arguably only for the purposes for which the information was collected), and that the misuse of private employee information may result in damages for invasion of privacy. As such, where an employer misuses or mishandles private employee medical information in its possession, it could be liable for damages for breach of invasion of privacy.

An example of such a misuse of medical information was described in a 2010 decision of the Federal Privacy Commissioner, in which the Commissioner found that the Ministry of Veterans Affairs had breached the federal *Privacy Act* in relation to its handling of the personal medical information of the complainant, a veteran who had been actively advocating for veterans' rights.[1] The Commissioner's investigation determined that the volume and sensitivity of personal information, including medical information, contained within two briefing notes to the Minister was excessive and went far beyond what was necessary for the stated purpose of the briefings. In particular, one of the notes was prepared in order to brief the Minister on the complainant's participation in a Parliament Hill press conference to discuss issues related to veterans. In addition to briefing the Minister on the complainant's advocacy activities, the note contained considerable sensitive medical information including, diagnosis, symptoms, prognosis, chronology of interactions with the department as a client, amounts of financial benefits received, frequency of appointments, and recommended treatment plans, all of which

[1] See *Findings Under the Privacy Act*, October 7, 2010: http://www.priv.gc.ca/cf-dc/pa/2010-11/pa_20101006_e.asp

had been viewed by numerous departmental officials who would normally require only very limited or no access to medical information in fulfilling their duties. The complainant had originally provided this information to the Ministry in relation to an application for veterans' benefits and had no expectation that this information would be widely viewed or used for any other purpose.

While this case arose before the decision in *Jones v. Tsige* was rendered and the complainant did not pursue any damages for the invasion of his privacy, and while the relationship between the Ministry and the veteran was not an employment relationship (although it bore some of the same elements), these are precisely the kinds of circumstances in which the *A.U.P.E.* decision indicates an employee might be able to rely on *Jones* to seek damages for the inappropriate use of his or her medical information by the employer. If medical information is provided to the employer for one purpose—for example so that the employee can apply for short-term disability benefits—and it is handled without appropriate restrictions such that it is viewed broadly within the organization and by individuals who have no need to access the employee's personal medical information, the employer could be liable for a breach of invasion of privacy.

By contrast, where an employer handles such information with appropriate restrictions, it remains clear that legitimate demands for employee private medical information will not be considered a violation of the right to privacy. In a recent decision by Arbitrator Surdykowski, *Complex Services Inc. and O.P.S.E.U., Local 278 (2011-0278-0015) (Re)* (2012) 110 C.L.A.S. 49, the arbitrator determined that *Jones* did not stand for the proposition that asking an employee for information for a legitimate purpose (such as substantiating an absence) or as permitted by legislation or the collective agreement violated the right to privacy.

In *Complex Services*, the grievor sought medical accommodation for both a physical and apparently mental illness, but refused to provide certain medical records sought by the Employer, or to submit to an Independent Medical Exam. She insisted on her absolute right to privacy over her medical information. In the course of the hearing, Arbitrator Surdykowski

requested submissions from the parties with respect to *Jones v. Tsige* and its application to the grievance arbitration.

Ultimately, Arbitrator Surdykowski found that *Jones v. Tsige* did not "alter or add to the analysis" in the case (para 91). While the arbitrator agreed with the Union that "*Jones v. Tsige* reinforces the premium value of privacy in Canadian society", he found that the decision does not establish "an additional premium or value" [emphasis added] (para. 92). In other words, in the context of a unionized workplace, *Jones v. Tsige* does not alter the existing legal landscape with respect to when an employer is permitted to seek sensitive medical information from employees:

> …I agree with the Employer that whatever *Jones v. Tsige* actually stands for in terms of the non-legislated or non-contractual right to privacy, it does not stand for the proposition that asking for or even demanding that an employee disclose confidential medical information for a legitimate purpose constitutes an improper or actionable intrusion on the employee's right to privacy. *Jones v. Tsige* does not posit any absolute right to privacy.
>
> (para 93)

As such, Arbitrator Surdykowski held that it remains the case that an employer is entitled to request and receive an employee's confidential medical information to the extent necessary to answer legitimate employment related concerns, or to fulfill its obligations under the collective agreement or legislation; nothing in *Jones* alters the employer's right to manage its workplace, or to obtain confidential medical (or other) information as required or permitted by legislation or the collective agreement, or which it reasonably requires for a legitimate purpose.

Arbitrator Surdykowski emphasized, however, that the employer is only entitled to the confidential information necessary for the legitimate purpose. And even in such circumstances, the employee is entitled to refuse to disclose her confidential medical or other information, although if she does she must accept the consequences: that refusing to allow access to necessary confidential medical information may justify the employer's refusal to allow the

employee to continue or return to work, implement requested accommodations, result in the loss of disability benefits, or even lead to the loss of employment.

These same principles were reiterated by Arbitrator Surdykowski in two further cases, *Canadian Bank Note Co. and I.U.O.E., Local 772, Re* (2012) 112 C.L.A.S. 38 and *Hamilton International Airport Limited. V. Canadian Union of Public Employees, Local 5167,* 2012 CanLII 7445 (ON LA), namely that employer access to employee confidential medical or other information is limited to the exercise of the employer's legitimate rights or obligations and that *Jones v. Tsige* has no impact on this analysis.

Conclusion: The Impact of *Jones v. Tsige* on Employer Access to Employee Medical Information

In recognizing for the first time a stand-alone tort of invasion of privacy, *Jones v. Tsige* goes a long way towards settling the debate about whether employees have a "right" to privacy in the workplace. For those arbitrators who continued to maintain that no such right exists absent some jurisprudential foundation in the common law (or a negotiated right in the collective agreement), *Jones v. Tsige* now clarifies that a generalized right to privacy *does* exist in the common law, and can provide the basis upon which arbitrators can ground the principle that employees have a right to privacy in the workplace.

As applied in the *A.U.P.E.* case*, Jones* also appears to stand for the proposition that employers may be liable for the tort of intrusion upon seclusion where they have misused private employee information, even if that information was originally provided to the employer for a legitimate purpose. If the employer uses the information for a purpose other than which it was intended, and without legitimate foundation, it exposes itself to liability. While the *A.U.P.E.* case arose out of the context of an employer's illegal credit check, such circumstances could foreseeably arise with employee private medical information given to the employer for one purpose, but misused for another. Similarly, where employee medical information is handled inappropriately and viewed by individuals who have no operational need to know the information, this also may give rise to liability.

However, at least according to one Ontario arbitrator, *Jones v. Tsige* does not affect the contours of when employers can seek employee medical information and under what circumstances. Assuming the employer's request for medical information is *bona fide* and meets the established tests, there is no intrusion upon seclusion and *Jones* does not limit the employer's entitlement to access sensitive employee medical information in order to carry out its obligations under the collective agreement, the Ontario *Human Rights Code*, and other legislation.