

Employee Privacy Breaches – Do They Warrant Discipline?



In 2012 the Ontario Court of Appeal first established the tort of intrusion upon seclusion to Canadian law in [Jones v Tsige](#). Apart from the obvious impact of this case on those who are the victims of a privacy breach, the case has raised interesting questions in the field of labour and employment law. Namely, it places strong pressure on an employer to ensure prompt and sufficient discipline against employees who breach privacy rules in an effort to mitigate potential tort claims. The salient issue is how this new source of liability weighs against traditional labour and employment law concerning discipline. In other words, when does an employee's breach of a rule merit discipline and what discipline is warranted? While most cases thus far are in a labour context, these same general themes could be equally applied to non-unionized employees.

Privacy is serious business in certain industries

Arbitrators generally agree that confidentiality of certain records, particularly medical and banking records, is critically important. For that reason, many arbitrators have upheld the dismissal of employees for what may seem at first glance to be fairly minor breaches. While there is general consensus that privacy breaches are serious, outcomes begin to diverge when the adjudicator turns to the issue of mitigation: the reason why the snooping occurred, whether or not the employee was aware of a confidentiality policy, whether there is remorse, and whether the snooping is likely to happen again. Even where mitigation favours reinstatement, arbitrators impose lengthy unpaid suspensions. The issue is taken very seriously.

Especially the medical context

Most arbitrators find that there should be a zero tolerance standard when looking at confidential information in the medical context:

...I again wish to stress that the 'zero tolerance' standard should be the norm and that only in compelling circumstances should termination not be the result of deliberate breaches of the Act, Standard or confidentiality policies. ...

That quote is from Arbitrator Rayner in *Bluewater Health and O.N.A. (Hardy) (Re)*,

2010 CLB 33129. The arbitrator said that the vulnerability of patients to the misuse of their medical records by employees with access to those records is obvious. But 'zero tolerance' does not always mean discharge is the only disciplinary response.

In the Bluewater matter, there were two grievors: one, a part time nurse with two years' service, accessed the medical records of four patients she had no connection to for very short periods – a matter of seconds. The grievor characterized this as 'accidental access'. The other grievor, a 15-year employee with a good work record, accessed the medical records of two patients – her daughter and her father. Her reason? She testified that she accessed her daughter's records because her daughter suffered from severe cerebral palsy and she was the primary caregiver. She said that she accessed her father's records because she wanted to explain and discuss what she discovered about his condition with him. In both cases, neither grievor had obtained consent, either express or implied, to access the patient records that they did. Arbitrator Rayner upheld the discharge of the first grievor, rejecting her *de minimis* argument and focusing on the fact that she failed to report any "accidental access" required by the policy. With the second grievor, he found that mitigation justified reinstatement without compensation, but with no loss of seniority.

In *Timmins & District Hospital and O.N.A. (Peever)* (2011), 208 LAC (4d) 43, Arbitrator Marcotte agreed with Arbitrator Rayner that "zero tolerance" is the norm. In *Timmins*, the grievor was a registered nurse, with 22 years' service who was discharged for breach of confidentiality after accessing the clinical mental health records of a patient. Her reason? The patient whose records she accessed had been married to her son who was embroiled in a custody dispute with the patient. Arbitrator Marcotte was unable to find any compelling circumstances to mitigate the penalty of discharge saying that, based on his conclusions that she knowingly accessed the information in violation of the employer's ethics and confidentiality policies and applicable privacy legislation without remorse, there was no assurance that her actions would not reoccur.

A very recent decision, released in March 2014 out of British Columbia, found compelling circumstances that favoured mitigation of a dismissal. In *Vancouver Coastal Health Authority and HSA BC (Gamache), Re*, (2014) 118 CLAS 104, the arbitrator was faced with a 24-year employee of the health authority who was dismissed for accessing and emailing contents of a patient's medical records. The employee had emailed this information to a friend of hers whose sister had recently separated from the patient. The employee claimed not to have known of the recent separation, but in any event, she had no consent to access the records. A three-month suspension without pay was substituted in lieu of dismissal. The arbitrator noted that despite a zero tolerance policy, the employer must still consider the unique facts of the case and that "extremely compelling" circumstances can justify penalties short of dismissal. The mitigating circumstances in this case included a lack of malice in disclosing the information, the employee's candid and sincere admissions of wrongdoing, her blemish-free record of employment and significant stressors in her life at the time.

Sometimes, discipline short of dismissal may be appropriate despite a "zero tolerance" policy due to mitigating factors.

Arbitrators in Canada recognize a well-known, well-understood and all-encompassing fundamental obligation on health care employees to maintain the confidentiality of patient information.

But lately, privacy isn't just restricted to health care settings; it's about trust

[Steel v Coast Capital Savings Credit Union](#) will be of interest to non-union employers

who place a high expectation on their employees to ensure privacy and confidentiality of clients. This decision is also reviewed in Preparing for the office snoop: protect employee privacy and limit your liability. Ms. Steel's job description required that she "Respect the privacy and confidentiality of all customer and staff information at all times". In her job, Ms. Steel could access personal folders of employees when she was assisting with technical problems. Her access, however, was restricted by protocol: (a) the employee whose personal folders were to be accessed had to provide consent; or, (b) the VP of corporate security had to authorize it. Nevertheless, Ms. Steel, who had signed off on the employer's Acceptable Use Policy, Code of Conduct Policy and Information Confidentiality Policy, accessed a spreadsheet in a co-worker's personal file that contained confidential employee information including pay grades and seniority dates. After an investigation by the employer, Ms. Steel was terminated for cause. The court agreed that the employer had cause, saying:

Ms. Steel occupied a position of great trust in an industry in which trust is of central importance. In her position [she] was given the ability to access confidential documents. The employer established clear policies and protocols known to Ms. Steel at the relevant time that were to govern access to confidential documents.

The court found that the 'trust' fundamental to Ms. Steel's position was broken beyond repair.

What this means for employers

The outcome of an arbitration or court case can never be 100 per cent predictable because of the large role that individual facts play. What is predictable is that privacy breaches will continue, whether as a result of human curiosity or snooping. Nonetheless, employers are equipped with strong guidance from arbitrators as well as the courts. Decision makers are saying that in some industries, 'zero tolerance' is the standard and unless there are sufficient mitigating circumstances, dismissals are appropriate even for seemingly minor violations. Even in cases where mitigation does play a role, arbitrators are saying lengthy unpaid suspensions are warranted. Employers, whether unionized or non-unionized, in the health care, banking or any other sector where confidentiality is an expected condition of employment, should continue to educate employees through codes of conduct or confidentiality policies and should clearly say discipline will follow when these policies are violated. As in all cases, policies and discipline must always be consistent and equally applied. Hillary Clinton summed it up best when she said:

We count on the space of trust that confidentiality provides. When someone breaches that trust, we are all worse off for it.