CCH
a Wolters Kluwer business

Labour Notes®

December 1, 2008
Number 1368

"PRIVACY IS DEAD, DEAL WITH IT"[1]

By: Keith Burkhardt of Sherrard Kuzz LLP. Reproduced with permission.

The use of electronic resources in the workplace has become so pervasive that many employees insist that they could not survive even a day without their laptop, cell phone or personal data assistant. And while employees will use these resources to complete regular employment tasks, more often than not they will also be used for personal or non-business purposes.

The management of workplace technology can be a touchy subject. Mention the word "monitoring" and cries of invasion of privacy ring from the rafters. But it doesn't have to be this way. Most employees understand that information technology is both expensive and necessary, and that an IT use policy is a reality of employment.

A well-crafted policy outlining an employer's right and ability to monitor an employee's computer, cell phone, or other electronic resource ("IT Use Policy") can create an effective balance between business objectives and workplace harmony. The content of an IT Use Policy will vary depending upon a number of factors such as whether the workplace is unionized, the nature of the work, the workplace culture and, of course, prevailing legalities such as privacy laws and reasonable expectations.

Legal Considerations

In most **non-unionized workplaces**, an employer will be permitted to unilaterally implement an IT Use Policy. Courts can be expected to uphold a policy which is reasonable in nature provided that employees are given appropriate notice of the implementation of the policy and the change is either not considered fundamental to the terms and conditions of employment, or employees receive some form of consideration to compensate them for the change.

Unionized workplaces may operate differently. For example, a collective agreement may require consultation or agreement with the union prior to the implementation of the policy. As well, arbitrators have routinely found that employees have a reasonable expectation of privacy in certain activities that include the use of electronic resources.

That being said, if the collective agreement does not restrict management rights as they relate to the use of information technology, management may unilaterally implement an IT Use Policy. The only parameters are that the policy must be reasonable, unequivocal, consistently enforced, and its implementation, and consequences of a breach, must be brought to the employees' attention.

Government operations will need to also consider the impact of the *Charter of Rights and Freedoms*. Section 8 of the Charter protects individuals from being the subject of an unreasonable search or seizure. Courts and Tribunals have interpreted this restriction as prohibiting an employer from engaging in certain surveillance or monitoring activities if there is a reasonable expectation of privacy.

For example, in *Amalgamated Transit Union Local No. 569 v. Edmonton*, a decision of the Alberta Queen's Bench from 2004, a unionized employee filed a grievance alleging that the employer's off-duty surveillance of his activities while on a leave of absence violated his rights under Section 8 of the Charter. The Court affirmed that the Charter did apply to the City of Edmonton and that its employees were provided, under Section 8, with the general right to be free from an unreasonable invasion of their privacy. The Court concluded, however, that this right had not been infringed by the employer as the surveillance occurred in a public place and monitored activities which occurred in the public eye. As such, the grievor had no reasonable expectation of privacy when the surveillance took place.

A recent Court of Appeal ruling in the United States, on the other hand, found that an employee had a reasonable expectation of privacy in a text message sent from a government-issued cell phone and that the employer could not read the contents of the message without a warrant or consent from the employee. The case in question, *Quon v. Arch Wireless Operating Co. Inc.*, involved an employee who was disciplined after a review of text messages sent from his pager revealed a number of inappropriate or non-work related messages. The employee complained that his privacy had been unlawfully violated when the contents of these messages were disclosed to his employer by the service provider that transmitted and stored them. The Court agreed with the employee and ruled that obtaining the text messages resulted in the employee being the subject of an unlawful search. The Court also found that although the employer had an electronic resources policy which applied to pagers and which could have authorized the employer to review the text messages, it was not routinely or consistently enforced and, contrary to the scope of it, employees had *also* been told that text messages would only be audited in certain specific situations. In these circumstances, the employee had a reasonable expectation of privacy in the text messages, and the policy could not be relied upon. While this case is not binding on Canadian courts and employers, a similar result in Canada is not beyond the realm of possibility.

A Few Tips

A prudent employer might consider the following tips relating to the creation and implementation of an IT Use Policy:

Obtain Legal Advice: Even an employer's best intentions can accidentally run afoul of the law. Before implementing an IT Use Policy consult with experienced counsel who will assist you to understand your rights and obligations as an employer. If an IT Use Policy is worth having, it's worth having done right.

Purpose and Application: Explaining to employees the rationale for the policy and how the policy will apply to their work environment will go a long way towards ensuring its acceptance. In plain, straight-forward language,

CANADIAN LABOUR LAW REPORTER

Published bi-weekly as the newsletter complement to the CANADIAN LABOUR LAW REPORTER, by CCH Canadian Limited. For subscription information, see your CCH Account Manager or call 1-800-268-4522 or (416) 224-2248 (Toronto).

For CCH Canadian Limited

RITA MASON, LL.B., Senior Editor
(416) 224-2224, ext. 6275
e-mail: Rita.Mason@wolterskluwer.com

JANINE TRUELOVE, B.Sc. (Hons.), LL.B., Senior Editor
(416) 224-2224, ext. 6286
e-mail: Janine.Truelove@wolterskluwer.com

DAVID IGGULDEN, B.A., M.L.S., Associate Editor
(416) 224-2224, ext. 6369
e-mail: David.Iggulden@wolterskluwer.com

CHERYL FINCH, B.A., LL.B., Director of Editorial
Legal and Business Markets
(416) 228-6128
e-mail: Cheryl.Finch@wolterskluwer.com

JIM ITSOU, B.Com., Marketing Manager
(416) 228-6158
e-mail: Jim.Itsou@wolterskluwer.com

JANINE GEDDIE, B.A., LL.B.
Contributor

PUBLICATIONS MAIL AGREEMENT NO. 40064546
RETURN UNDELIVERABLE CANADIAN ADDRESSES TO
CIRCULATION DEPT.
330–123 MAIN ST
TORONTO ON M5W 1A1
email circdept@publisher.com

tell employees: the purpose of the policy; what types of technology will be covered (i.e. computers, phones, voicemail, text messages, email, servers, internet access, software, printers and output devices, scanners and input devices and other related equipment, etc.); how the policy will apply; when the policy will take effect; how the information collected will be used; and the consequences for a breach or breaches, up to and including dismissal for cause.

"Notice" to Employees: In order for the IT Use Policy to have teeth, "notice" to employees should mean more than merely posting the policy in the lunchroom or slipping it into an office manual. To be enforceable "notice" should include each employee receiving a copy of the written policy and being required to sign-off on a statement that confirms the employee has read and understood the policy and agrees to be bound by it. Without proper notice or agreement, an employer may have difficulty relying on the policy in the future.

Ownership and Expectation of Privacy: The IT Use Policy should include in clear language that the employer owns all workplace information technology and that employees should have no expectation of privacy as it relates to its use.

Business and Personal Use: If some limited personal use of workplace technology will be allowed, set that out in the IT Use Policy. Employees appreciate the opportunity to avail themselves of workplace technology for personal use, but also welcome guidance as to what type of usage will be considered off limits.

Degradation of Systems: Many individuals do not appreciate that the downloading of seemingly harmless programs, games, music, etc. can cause serious damage to information technology operating systems, punch a hole through security, or drain away precious memory capacity. A "no downloading" policy is therefore to be considered.

Enforcement and Compliance: Once in place, the policy should be enforced consistently. In the *Quon* decision, the employer had implemented a policy that should have eliminated any expectation of privacy relating to the contents of text messages. However, the employer failed to consistently enforce the policy and subsequently set out a different and contradictory "informal" policy. This led the Court to conclude that a reasonable person would believe that employees would be granted additional leeway in their actions. While a court may not expect an employer to discipline or discharge every employee who violates a policy, it will expect the employer to be diligent and clear in its efforts to ensure compliance.

Keith Burkhardt practices law with the management-side employment and labour law firm Sherrard Kuzz LLP in Toronto. Keith can be reached at 416.603.0700 (Main), 416.420.0738 (24 Hour) or by visiting www.sherrardkuzz.com.

Notes:

[1] Sun Microsystems Chairman Scott McNealy in 2000