CANADIAN
Employment Law Today
A Carswellbusiness Publication ■ www.employmentlawtoday.com

CURRENT NEWS AND PRACTICAL ADVICE FOR EMPLOYERS

ISSUE NO. 522 • NOVEMBER 19, 2008

CASE IN POINT: PRIVACY

Privacy vs. policy: Personal use of company equipment

Employees often use electronic equipment at work for personal reasons and employers should be careful when trying to keep it in check

BACKGROUND

'Privacy is dead, deal with it'

The words of Sun Microsystems chairman Scott McNealy in 2000 may be a little disconcerting for some, but with the prevalence of electronic devices in everyday life, especially in the workplace, it is difficult to dispute.

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

It's usually a good idea for employers to have a policy governing the use of technology in the office such as computers, phones, voicemail, text messages, e-mail, servers, internet access, software, printers and output devices, scanners and input devices and other related equipment. However, having a policy in itself doesn't mean much if an employer doesn't give proper notice of the policy and doesn't consistently enforce it, especially if the employer is monitoring employees' use of the technology.

Keith Burkhardt of Sherrard Kuzz LLP discusses the important points of implementing an IT use policy and the legal considerations that accompany it.

By Keith Burkhardt

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 information technology (IT) is both expensive and necessary and 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 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 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 employees are given appropriate notice of its implementation 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, and consistently enforced, and its implementation and discipline for 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*. 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.

Surveillance of employee in a public place

In *Amalgamated Transit Union Local No. 569 v. Edmonton*, a unionized employee filed a grievance alleging the employer's off-duty surveillance of his activities while on a leave of absence violated his rights under the charter. The Alberta Court of Queen's Bench affirmed that the charter did apply to the City of Edmonton and its employees

Continued on page 5

CASE IN POINT: PRIVACY

Employer should clarify boundaries and consequences

...continued from page 4

were provided 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 employee had no reasonable expectation of privacy when the surveillance took place.

Reasonable expectation of privacy

A recent Court of Appeal ruling in the United States, on the other hand, found an employee had a reasonable expectation of privacy in a text message sent from a government-issued cell phone. The court held that the employer could not read the contents without a warrant or consent from the employee. In *Quon v. Arch Wireless Operating Co. Inc.*, an employee 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 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 and ruled obtaining the text messages resulted in the employee being the subject of an unlawful search. The court also found although the employer had an electronic resources policy which applied to pagers and could have authorized the employer to review the text messages, it was not routinely or consistently enforced. As well, contrary to its scope, employees had also been told text messages would only be audited in certain specific situations. In these circumstances, the employee had a reasonable expectation of privacy with 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.

Tips for employers

A prudent employer might consider the following tips relating to the creation and implementation of an IT use policy.

Legal Advice. Even an employer's best intentions can accidentally run afoul of the law. Before implementing an IT use policy, employers should consult with experienced counsel who will help in understanding the employer's 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, the employer should explain the purpose of the policy, what types of technology will be covered, how the policy will apply, when the policy will take effect, how the information collected will be used and the consequences for breaching it, up to and including dismissal for cause.

Notice to Employees. In order for the policy to have teeth, notice to employees should mean more than merely posting it 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 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.

Ownership and Expectation of Privacy. An IT use policy should state in clear language the employer owns all workplace information technology and 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 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 the downloading of seemingly harmless programs such as games and music can cause serious damage to information technology operating systems, punch a hole through security or drain away precious memory capacity. A "no downloading" policy should be considered.

Enforcement and Compliance. Once in place, the policy should be enforced consistently. In *Quon*, the employer 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 it and subsequently set out a different and contradictory informal policy. This led the court to conclude a reasonable person would believe 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 it to be diligent and clear in its efforts to ensure compliance. CELT

For more information see:

- *A.T.U., Local 569 v. Edmonton (City)*, 2004 CarswellAlta 435 (Alta. Q.B.).
- *Quon v. Arch Wireless Operating Company*, 529 F.3d 892 (9th Cir. 2008).

ABOUT THE AUTHOR

Keith Burkhardt

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 or at www.sherrardkuzz.com.