LABOUR AND EMPLOYMENT

COMPUTER SURVEILLANCE BY EMPLOYERS: FINDING THE BALANCE BETWEEN BUSINESS INTERESTS AND EMPLOYEE PRIVACY RIGHTS

by W. Eric Kay and Andrew J. Skinner

As the use of computers and computer activity becomes more pervasive in the workplace, employers are facing new challenges. Generally speaking, greater network connectivity should be welcomed by employers. However, the use of company technical devices in the workplace can give rise to "inappropriate activity". In these circumstances, an employer must balance the privacy of its employees, and the surveillance of employees as a good business practice to monitor employees using company technology.

When Does Employer Surveillance Cross the Line?

Canadian courts and adjudicators have recognized that employers have a legitimate interest in monitoring the workplace, whether it is for security reasons, economic reasons, or simply to promote productivity. However, there are limits placed on these legitimate interests in the context of upholding employee privacy rights in the workplace. Privacy commissioners and arbitrators have developed various tests to evaluate on any given set of facts whether employee monitoring is acceptable. While there is no established universal test, if the employer can demonstrate a justifiable causal link between the information obtained and the employee's actions, it is likely that the legitimate interest of the employer will outweigh the employee's privacy concerns. In this regard, factors to consider include the seriousness of the allegations, the probative value of the evidence and the degree of invasion on the privacy of the individual.

In *R v. Cole*, 2012 SCC 53, the Supreme Court of Canada noted that although employees may have a legitimate expectation of privacy when using workplace computers, in some cases the seriousness of an offence and workplace computer policies are sufficient to override the privacy rights of an individual. The Court did state, however, that the decision to delve into an employee's browsing history on their work computer represents an intrusion into their privacy that must be reasonably justified.

If authorized by law, including by necessary implication from a statutory duty, an employer has a reasonable power to seize and search a digital device if it has reasonable grounds to believe that the device contains evidence of "serious" misconduct. Generally, arbitrators have also allowed employers to use monitoring data as evidence of employee misconduct which is considered to be reasonable in the particular circumstances.

While an employer has a right to direct and monitor employee behaviour and performance in the workplace, employers should be aware that the Ontario Court of Appeal has recognized the employee right to privacy in tort in *Jones v. Tsige*, 2012 ONCA 32. In that case, Justice Sharpe recognized employment as a category of information which should be protected from deliberate and significant invasions of personal privacy. Based on *Jones v. Tsige*, employees may now allege that unreasonable monitoring constitutes an "intrusion upon seclusion" under the common law. Employers need to be aware that significant invasions into employee personal information without justification, and particularly disclosure of that information to third parties, will open up the employer to potential liability in tort.

Practical Issues

If employers allow employees to have access to technology and to use it for personal use (which can often be inferred even when a policy exists), then employers should expect that the employee has an implied right to a reasonable expectation of privacy within that equipment. If an employer plans to monitor an employee's usage, such as their computer email or browsing history, it is recommended that the employer obtain the employee's written consent in advance, or provide notice in the employment contract, collective agreement or terms of employment at hire. Arguably, where the employer has established policies related to the use of work computers and work emails, there will be a reduced expectation of employee privacy unless the employer fails to enforce their policies or does so selectively.

Employers may rely on information obtained through routine searches or audits to discipline an employee. However in the event of litigation, arbitrators and courts may review the employer's authority for conducting the search. Arbitrators and courts will likely explore the "totality of circumstances" in evaluating whether an employee's reasonable expectation of privacy was breached in obtaining the information and deciding whether it may be relied upon as evidence in the case of discipline.

Staying alert to and recording suspicious employee behaviour can help prevent potentially damaging results. Companies should consider adopting policies with respect to employee technology monitoring, including conducting regular audits of employee usage which may disclose impropriety. At the point of employee departure, a checklist can be utilized with a view to protect vulnerable data that may be unknowingly or intentionally transferred during the departure.

Outlook

While technology will continue to give employers insight into the personal use of the employee devices, employers must be cognizant of the potential human resources issues that come with using such information. Even when an employer may be within their legal or collectively bargained right to use and rely on this information to discipline an employee, the impact on workplace morale may be more important than the legal ramifications.

Although the Court has yet to provide a straightforward answer as to how much employers may monitor their employee's technological usage, there are steps that employers should take to prevent issues from arising if they intend to monitor employee's usage:

- Obtain written consent or provide notice to the employee in advance of monitoring
- Create an acceptable use policy for all technological devices, which explains what an employee can and cannot do and the disciplinary consequences of violating the policy
- Ensure the employee handbook makes employees aware of employer monitoring.
- Conduct regular audits of employee usage

This Client Alert is published by Dickinson Wright LLP to inform our clients and friends of important developments in the field of labour and employment law. The content is informational only and does not constitute legal or professional advice. We encourage you to consult a Dickinson Wright lawyer if you have specific questions or concerns relating to any of the topics covered in here.

FOR MORE INFORMATION CONTACT:

W. Eric Kay is a partner in Dickinson Wright's Toronto Office and can be reached at 416.777.4011 or ekay@dickinsonwright.com

Andrew J. Skinner is a partner in Dickinson Wright's Toronto Office and can be reached at 416.777.4033 or askinner@dickinsonwright.com