FTR Now

Ten Questions and Answers about Computer Use Policies

Date: January 23, 2012

It's January 2012. Last year the Court of Appeal for Ontario recognized that an employee had a reasonable expectation of privacy that arose out of his personal use of a work computer. As discussed in a companion *FTR Now* called *How the New Privacy Tort Will Affect Employers*, this month the Court of Appeal recognized a new "intrusion upon seclusion" tort. Have you looked at your computer use policy lately? This *FTR Now* sets out ten questions and answers to help guide that exercise.

1. WHAT SHOULD EMPLOYERS DO TODAY TO ENSURE THEIR COMPUTER USE POLICIES EFFECTIVELY MANAGE THE IMPLICATIONS OF PERSONAL USE?

In light of recent developments, employers should ensure that their computer use policies (1) articulate all the purposes for which management may access and use information stored on its system and (2) make clear that engaging in personal use is a choice employees make that involves the sacrifice of personal privacy.

2. WHAT ARE THE MOST COMMON PURPOSES FOR EMPLOYER ACCESS?

Consider the following list: (a) to engage in technical maintenance, repair and management; (b) to meet a legal requirement to produce records, including by engaging in e-discovery; (c) to ensure continuity of work processes (*e.g.* employee departs, employee gets sick, work stoppage occurs); (d) to improve business processes and manage productivity; and (e) to prevent misconduct and ensure compliance with the law.

3. HOW SHOULD EMPLOYERS DESCRIBE THE SCOPE OF APPLICATION OF A COMPUTER USE POLICY?

Computer use policies usually apply to "users" (employees and others) and a "system" or "network." To effectively manage employee privacy expectations, policies should make clear that devices (laptops, handhelds…) that are company owned and issued for work purposes are part of the system or network even though they may periodically be used as stand alone devices.

4. SHOULD EMPLOYERS HAVE CONTROLS THAT LIMIT ACCESS TO

INFORMATION CREATED BY EMPLOYEES EVEN THOUGH THEY DON'T WANT TO ACKNOWLEDGE THAT EMPLOYEES CAN EXPECT PRIVACY IN THEIR PERSONAL USE?

Access controls are an important part of corporate information security. Rules that control who can access information created by employees (*e.g.* in an e-mail account or stored in a space reserved for an employee on a hard drive) are, first and foremost, for the company's benefit. Access controls should be clearly framed as being created for the company's benefit and not for the purpose of creating any restriction on company access.

5. HOW SHOULD PASSWORDS BE ADDRESSED IN A COMPUTER USE POLICY?

Password sharing should be prohibited by policy. Employees should have a positive duty to keep passwords reasonably secure. A computer use policy should also make clear that the primary purpose of a password is to ensure that people who use the company system can be reliably identified. Conversely, a computer use policy should make clear that the purpose of a password is not to preclude employer access.

6. DOES ACCESS TO FORENSIC INFORMATION RAISE SPECIAL ISSUES?

Yes. Computer use policies often advise employees that their use of a work system may generate information about system use that cannot readily be seen – *e.g.* information stored in log files and "deleted" information. It is a good practice to use a computer use policy to warn employees that this kind of information exists and may be accessed and used by an employer in the course of an investigation (or otherwise).

7. HOW SHOULD AN EMPLOYER ADDRESS THE USE OF PERSONAL DEVICES ON ITS NETWORK?

Ensuring work information stays on company owned devices has always been the safest policy, though cost and user pressures are causing a large number of organizations to open up to a "bring your own device" policy. Employers who accept "BYOD" should use technical and legal means to ensure adequate network security and adequate control of corporate information stored on employee-owned devices. For example, employers may require employees to agree to remotely manage their own devices as a condition of use and with an understanding that they will sacrifice a good degree of personal privacy.

8. SHOULD A COMPUTER USE POLICY GOVERN THE USE OF SOCIAL MEDIA?

Only indirectly. A computer use policy governs the use of a corporate network. A social media policy governs the publication of information on the internet from any computer at any time. In managing social media risks, employers should stress that publications made from home are not necessarily “private” or beyond reproach, so putting internet publication rules in a computer use policy sends a counter-productive message.

9. SHOULD EMPLOYERS UTILIZE ANNUAL ACKNOWLEDGEMENTS?

Annual acknowledgements are not a strict requirement for enforcing the terms of a computer use policy but are helpful. The basic requirement is to give notice of all applicable terms in a manner that allows knowledge to be readily inferred in the event of a dispute. “Login script” with appropriate warning language is also common and helpful. Nowadays, a good login script will say something like, “If you need a confidential means of sending and receiving personal communications and storing personal files you should use a personal device unconnected to our system.”

10. ARE THERE SPECIAL CONCERNS FOR PUBLIC SECTOR EMPLOYERS?

Most public sector employers in Canada are bound by the *Canadian Charter of Rights and Freedoms* and by freedom of information legislation. Many have workforces that are predominantly unionized. The guidance to public sector employers on their computer use policies is no different than to employers in general, but the need to manage privacy expectations that employees may derive from personal use is particularly strong for public sector employers given the legal context in which they operate.

We would be pleased to look at your computer use policy and provide any guidance related to this important development. For more information, please contact Paul E. Broad at 519.931.5604 or any other member of our firm’s Information and Privacy Group.
