Monitoring Employee Internet and E-Mail Use

STEVE HILLIER

Most of us are aware of the business advantages and drawbacks of computer-stored records. Ease of access, storage and communication now largely outweigh the risks of systems crashes and techno-phobia. Computers have allowed for the storage of mass documents, including employment records, marketing strategies, business correspondence and financial information. However, employers need protection from a variety of new issues and risks that standard corporate policies on confidentiality and integrity simply cannot cover. One of the most controversial is monitoring of employee internet and e-mail use. Certainly employers face a very real risk of civil or criminal liability arising from misuse of technology by employees. At times it appears that new technology is able to obscure commonsense principles in the workplace. People seem to rationalize that actions using internet access or e-mail are activities for which there is less personal accountability either because nothing is physically signed or it was just so simple to send without regard to consequences. So the employer faces all sorts of problems with breach of confidentiality, workplace harassment, defamation and general loss of productivity.

On the topic of E-mail specifically, employees must be reminded that they continue to represent the employer when using the employer's e-mail programs in the same way as when they use the employer's stationery. The careless use of language could easily lead to a defamation action, where damages multiply with each click of the mouse, spreading inaccurate e-mail to more and more recipients. There are numerous instances where e-mail has been inadvertently forwarded to the wrong person disclosing confidential information to inappropriate parties. Once the recipient has received the material, the sender loses control not just of distribution but the text of his or her own e-mail which can easily be altered. Other risks with the internet can be just as damaging to the company. In early October 1999, Xerox revealed that at least 40 of its employees were fired for severe internet misuse. Some of the employees in question had spent up to 8 hours per day visiting non-business-related websites. In this past year Dow Chemicals Co. fired 50 employees and disciplined 200 others for having pornographic and violent images found on their computer hard drives.

There is ongoing debate whether employees have a right to privacy which can override the employer's business interests. Court cases to date would support NO as the short answer. But the Federal Privacy Commissioner has recently stated that – at least in cases covered by federal legislation – monitoring usage is invasive and illegal. In some contexts this may be true. But there are important interests to be balanced in the workplace.

As part of a strategy for reducing corporate risks, one of the first steps is to educate the workforce on the scope of the issue. Computer-stored records are almost universally producible in legal proceedings. Just ask Microsoft, where the corporation's own records were used against it in anti-trust prosecution. Computers and programs are entirely the property of the employer, and employees should have little or no expectations of privacy when using the

2000, 10235 - 101 Street
Edmonton, AB T5J 3G1
PH: 780.423.3003

400 The Lougheed Building
604 1 Street SW
Calgary, AB T2P 1M7
PH: 403.260.8500

201, 5120 - 49th Street
Yellowknife, NT X1A 1P8
PH: 867.920.4542

www.fieldlaw.com

employer's property. Many of the problems caused are due to employees' ignorance of this technology. Employees should be warned of the risks of accidentally sending confidential e-mails to inappropriate recipients. They should also be trained on internet and e-mail according to specific standards of the employer.

The next major step is to develop a comprehensive policy which emphasizes that:

- the internet and e-mail are to be used for business purposes only;
- the employer will not tolerate the use of the e-mail system to transmit offensive and derogatory remarks about a person's race, religion, ethnicity, sex, sexual orientation or disability;
- employees are prohibited from browsing and/or downloading and/or forwarding obscene, discriminatory, defamatory, pornographic, threatening or otherwise offensive material from the Internet;
- the system shall not be used to transmit any inappropriate material;
- e-mail should not contain defamatory statements about individuals or companies;
- the internet and e-mail should not be used to duplicate or transmit copyright material without the copyright owner's written permission;
- personal use of the internet and e-mail which may interfere with regular business operations will not be tolerated;
- employees should not transmit confidential or sensitive information throughout the internet or to unauthorized persons or organizations;
- the internet and e-mail should not be used for any illegal or unethical activity or any activity that could adversely affect the employer;
- employees must comply with the use of security/passwords and the requirement to shut down daily to reduce the risk of unauthorized access;
- the employer reserves the right to monitor the use of the internet and e-mail, at least in response to alleged abuse of these technologies (random enforcement of this may be subject to challenge);
- inappropriate use of e-mail and the internet by employees may lead to discipline, including the risk of dismissal; and
- the employer owns these e-mail and internet accounts and all data communicated through these accounts even where remote(home) access has been authorized.

In short, employees should not carry expectations of unfettered privacy regarding their internet and e-mail use except as meets the terms of corporate policy, including usage that does not interfere with regular business operations. The policy should be clearly written and explained to employees. Employees should be required to sign an acknowledgement stating that they received, and read a copy of the policy, and fully understand that they are bound by the policy. It is important to emphasize that policy breaches will result in discipline, including dismissal.

Step three requires employers to update their workplace harassment policies to include the misuse of electronic communication technologies. Studies have shown that harassment of co-workers is one of the most prevalent forms of computer abuse. Sexist and other discriminatory jokes are common subjects of e-mail correspondence. Browsing, downloading or sending pornographic or other offensive materials from the Internet is a form of harassment for which the employer will normally be vicariously liable. Once revised policies have been implemented, it is important to keep records of the orientation training, records of attendance as well as to update the information package for both new and current employees. And even with policies in place they can only be effective if they are consistently enforced.

As employers continue to invest in the advances of technology, policies need to be developed and revised. A key part of this strategy involves regular alerts to the workforce about their obligations in using these important resources. Keeping employees up to date both minimizes inadvertent breaches and reduces the likelihood of legal challenges of enforcement decisions. But most importantly, it reduces the risk of employer liability. And that drops right to the bottom line.