DIGITAL WORKPLACE PRIVACY

By Stacy King, emergit.com

Since the first desktop PC with Internet access was installed, employees have been using company equipment and network connections for personal communications. For the most part, firms are willing to turn a blind eye to the occasional personal e-mail or off-topic Web browsing. As office e-mail and Internet connections become ubiquitous, many employees forget the basic facts - that those resources belong to the company and, as such, can be monitored by employers at will.

Canadian case law on workplace e-mail privacy has evolved more slowly than in the United States, which has seen a higher number of such cases come before the courts. In many cases, American courts have held that employees do not have a reasonable expectation of privacy when using their employer's equipment, including the computer system. The use of the employer's network to send and receive messages has been interpreted as providing implied consent to any monitoring the employer may feel is applicable.

However, employees are also not expected to completely sacrifice their privacy while at work. In the United States, the issue of privacy invasion is determined by balancing the employee's Product Manager reasonable expectation of privacy against the employer's concerns in protecting their computer systems and minimizing their risk of liability. However, no such legal remedy for invasion privacy currently exists in Canada.

A Canadian employee's right to privacy in their workplace Internet access and e-mail is mainly a contractual issue. Many companies have implemented written guidelines regarding appropriate network resource use that detail the limits and extent of employee's privacy rights. Where such guidelines do not exist, an employee's best bet is to err on the side of caution.

Employees are also not expected to completely sacrifice their privacy while at work.

In addition to monitoring e-mail and Web browsing by checking access logs on the company's servers, an employer can keep tabs on everything happening on their staff's desktop. "BigBrother" software programs allow employers to obtain a snapshot of an employee's desktop at various times throughout the workday. The software, which runs undetected in the background via the PC's network connection, automatically takes a screen-capture of the workstation's desktop at selected intervals and stores those images to the server for later review.

This can be useful for employers who suspect that workers are squandering their time at work with non-Internet activities such as desktop games or other personal computing errands, like balancing their checkbook with the company's financial software. Keystroke monitoring software can also be used to check the number of keys each employee strikes per hour, which is compared against company averages or expected performance levels. While employers may inform their staff of such monitoring devices, they are typically under no legal obligation to do so.

There are some uses of company resources that are obviously inappropriate, providing grounds for discipline or even dismissal. Downloading illegal information or inappropriate graphic files are blatant misuses of corporate equipment. Less obvious are issues concerning the transmission of sensitive company information or excessive personal e-mail, which may equally be of concern to employers.

Many employees bypass their corporate e-mail accounts when sending personal

messages at work, relying instead on Internet e-mail providers such as Yahoo or Hotmail. What they fail to realize is that these systems are no more secure from monitoring than any other data transmitted via their office network connection. A common error is to accept a cookie from such sites, storing your password on your desktop where a network administrator can easily retrieve it.

There are PGP encryption programs that can be downloaded and installed on your workplace desktop to provide e-mail that is secure even from your employer. However, doing so is akin to waving a red flag in the face of your employer, since it suggests that you have something very important to hide from them. As well, many companies have policies restricting what software can be installed on an individual desktop, making such an approach problematic at best.

Another alternative to installing software is to secure your online browsing via the use of an computer and the encryption provider's server, transmitting all requested information in an encrypted format that is decoded only when it reaches your desktop.

This can be useful when searching for personal and sensitive information online, such as health information or banking needs. At the same time, the network administrator has access to logs of your Web surfing. Encryption servers will appear as a single Website that you visited again and again, a curious pattern that may spark further investigation.

Simply deleting information from your hard drive, such as erasing old e-mails, dumping browser history records, or moving files to the trashcan, is often not enough to eliminate inappropriate data. Many companies back up workstation information onto central storage servers, and e-mail programs may automatically save copies of messages sent and received in on the mail server as well as on the desktop.

Overall, your best policy is simply to restrict sensitive Internet communications to the one place that you can be sure your employer can not access them - your own equipment and network connection.

Article printed with permission of emergit.com. For more information see:www.emergit.com

SUBSCRIPTION AND EDITORIAL INFORMATION:

If you are interested in:
- reprints
- back issues
- new subscriptions
- posting upcoming events
- posting employment opportunities on the www

Please contact:
Barbara Marshall
Telephone: 416 864-9667
Facsimile: 416 368-6292
Email: bmarshall@longwoods.com

Subscriptions are $240 per year in Canada. US $240 elsewhere. Simply confirm your subscription by fax or email. We will bill you. Letters are sent out monthly by first class mail.

If you are interested in:
- future issues
- letters to the editor
- submitting articles and opinions

Please contact:
Dianne Foster-Kent
Managing Editor
Telephone: 416 864-9667
Facsimile: 416 368-6292
Email: dkent@longwoods.com

Twelve issues per year

A FOCUS Publication

260 Adelaide Street East, P.O. Box 8
Toronto, Ontario
Canada M5A 1N1
Telephone: (416) 864-9667
Facsimile: (416) 368-6292
Email: notes@longwoods.com
Internet: www.longwoods.com

ISSN 1203-049X Printed in Canada