E-mail & Internet Surveillance

written by John Boufford, I.S.P.

(October 21, 2000)

Employers are increasingly using E-mail and Internet surveillance as a tool to protect their interests. Employers have a responsibility to respect the reasonable privacy expectations of employees and customers. The CIPS position paper on E-mail and Internet Surveillance outlines acceptable surveillance practices as a guide for IT professionals and employers.

CIPS's Position on E-Mail & Internet Surveillance

(Approved by CIPS National Board of Directors on October 21, 2000)

Background

Employers are increasingly using e-mail and Internet surveillance as a tool to protect their interests. Legitimate business interests include for example, maintaining a workplace that is free from harassment.

Employers have a responsibility to respect the reasonable privacy expectations of employees and customers. At the same time, employees have a responsibility to use company resources in a manner that is efficient, and will not expose the company to service outages or loss of reputation. CIPS, as Canada's largest I.T. professional association, periodically takes positions on issues that are important to Canadians. This position paper has been prepared as a guide for members and employers who are preparing a surveillance policy. CIPS believes that this position strikes a reasonable balance between the rights of employers, employees and customers, and contributes to the public debate on acceptable surveillance practices.

Privacy is a right of individuals. Employers recognize that right in their business practices in a number of ways. They do not normally monitor telephone calls. Other situations where employers respect privacy occur when the employee is dealing with a personnel issue, or where he or she is providing services to a client or citizen on a sensitive issue such as health care or social assistance.

CIPS believes that personal use of e-mail and Internet should be tolerated to the extent that the organization accepts or tolerates personal telephone calls during business hours. A minor amount of personal activity is acceptable if the employee is meeting performance targets. If an employee is abusing that privilege, management takes action against that employee to correct the offending behaviour. However, the entire workforce is not subjected to scrutiny because of the inappropriate activities of a few.

It also needs to be recognized that privacy is not an absolute right. There are legitimate competing interests that mitigate an individual's right to privacy. Most commonly, the competing interests are those of society (e.g., law enforcement activities) or protecting the rights of others. CIPS recognizes that limited surveillance is sometimes necessary where the employer has a legal obligation to take corrective action. For example, if an employee complains of online workplace harassment, management has a legal obligation to investigate and, if the allegation is substantiated, to correct the offending the behavior.

The commonly held belief that an acceptable use policy providing employee notification of surveillance, does not protect employers from contravening the wire-tap provisions of the Criminal Code in all situations. Third parties (e.g., clients and customers) may send highly sensitive and confidential business-related e-mail to individuals that are under surveillance. It is virtually impossible for an internal company policy on e-mail surveillance to remove an expectation of privacy on the part of these third parties.

Abuse of privileges by a minority of employees is not a new phenomenon. Many of the existing performance management tools can be employed where a problem is identified. In most cases, management knows which employees are involved in inappropriate use of the e-mail and Internet services. It is therefore not only reasonable, but also practical, to monitor only those individuals where there is reasonable justification to believe that resources are being used inappropriately.

CIPS's Position

- **CIPS is against indiscriminate monitoring of employees and contractors.**
- **The need for surveillance must be balanced against the legitimate privacy rights of the employee.**
- **Indiscriminate surveillance may erode productivity and trust.**
- **Internet access providers have no legitimate business interests that justify surveillance of clients.**
- **CIPS does not support surveillance of individuals for purposes such as infrastructure management (e.g., network management or software license management). General capacity monitoring is a valid activity where it is used exclusively for planning purposes and not for disciplinary purposes.**
- **Organizations should develop a clear policy on e-mail and Internet surveillance and communicate it to staff. It is advisable to periodically remind employees of the policy in a logon message.**
- **The following guidelines are recommended.**
    - **Surveillance should be the tool of last resort. Traditional management techniques should be used where the offending behavior does not involve criminal behavior.**
    - **Surveillance should be conducted in accordance with the principles in the CIPS' position paper on Privacy and Information Technology or legislated privacy requirements where applicable.**
    - **Surveillance should only be directed at individuals (i.e., targeted individuals) where there is a reasonable justification that an employee is involved in serious misuse of the company resources (e.g., downloading hate or obscene material, or other criminal activity).**
    - **Pre-notification of surveillance activity should be given to the targeted individual where the surveillance does not involve possible criminal activity. Advising the employee that he or she is under performance management scrutiny may correct the offending behaviour. Withdrawal of e-mail and Internet privileges, where they are not necessary to the performance of employee duties, is an alternative to surveillance.**
    - **Surveillance is a management issue - not a technical one. The Chief Administrative Officer and the individual's manager should approve surveillance on a case-by-case basis before surveillance is begun.**
    - **Management needs to consider the privacy rights of third parties when conducting surveillance on targeted individuals. Sometimes the targeted individual's duties involve receipt of sensitive e-mails (e.g., on topics such as human resources, health matters, social assistance, or criminal matters) from other employees or the public. Access to such messages by an individual who does not have similar responsibilities for program delivery would be an invasion of the third party's privacy. Management must take this into consideration and assign someone with similar or supervisory responsibilities to conduct the surveillance.**
    - **Where the offending behavior is a violation of criminal law and the employer is prepared to press charges, law enforcement agencies should be contacted so that a criminal investigation is not compromised.**
    - **When the surveillance activity is completed, the targeted individual should be informed of the results.**
    - **Surveillance should be used infrequently. If surveillance activities become commonplace, management should consider whether inappropriate use of e-mail and the Internet is a symptom of other problems in the workplace.**

For additional information, please contact:
John Boufford, I.S.P.
Co-Chair, CIPS External Liaison Committee
E-mail: info@cips.ca