ONTARIO GIVES LEAD ON ELECTRONIC MAIL PRIVACY PRINCIPLES

Responding to the extensive use of electronic mail (e-mail) and its potential threats to privacy, Tom Wright, Information and Privacy Commissioner of the Canadian province of Ontario, has developed a set of privacy protection principles for the use of e-mail systems. The principles are specifically addressed to provincial and municipal government organisations under the jurisdiction of Ontario's Freedom of Information and Protection of Privacy Act. However, they are useful for both public and private sector organisations in developing and implementing their corporate policies on e-mail worldwide.

E-mail is a paperless form of communication which allows messages to be sent from one computer user to another. Within and between the organisations, e-mail can be an effective tool which helps break down barriers to communication and promotes the free exchange of information and ideas. On the negative side, however, as noted by a data security expert, e-mail has "the same security level as a postcard." In addition, e-mail creates an electronic trail of messages that can be used to monitor individuals. Complex legal and ethical questions have emerged about the right to privacy of e-mail users, particularly in the workplace, as well as the individuals who are subjects of e-mail messages.

The following privacy protection principles are intended to provide a framework for developing and implementing more specific policies on e-mail.

1. The privacy of e-mail users should be respected and protected

A survey of managers in the USA indicated that searching of e-mail files is one of the of employee monitoring. While employers may argue that electronic monitoring helps to increase productivity, research indicates that it can actually have an adverse effect on productivity.

Although it is not possible to guarantee complete privacy in relation to e-mail, it is in the best interests of an organisation to offer the highest degree of privacy possible. One of the advantages of e-mail is that is has democratised the workplace by breaking down barriers to communication between different levels of hierarchy. Enhanced communication can make the organisation run much more effectively and efficiently. However, employees will only make use of e-mail to the extent that they feel comfortable that what they transmit will remain, for the most part, confidential. Management's efforts towards employees' privacy will enhance the quality of worklife and encourage employees to use e-mail to its fullest potential.

2. Each organisation should create an explicit policy which addresses the privacy of e-mail users

Every organisation should develop a formal policy on e-mail privacy. Every individual within the organisation should be made aware of his/her rights and obligations under the policy and agree to adhere to it.

The policy should be developed jointly by representatives of employees, managers, personnel, legal and IT departments. Participation of the e-mail users in the development and implementation of the policy is a key element in fostering commitment. Also, education and training will be necessary to ensure that the policy is properly implemented.

The policy should, as a minimum, set out the following:

- purposes for which the e-mail system may be used
- conditions and procedures for access to e-mail by third parties
- consequences of breaches of the e-mail policy.

3. Each organisation should make its e-mail policy known to users and inform them of their rights and obligations regarding the confidentiality of messages on the system

It is important that every employee is expressly informed about his/her rights and obligations regarding the use of e-mail in the workplace. It may not be sufficient to simply have the policy set out in the corporate manual. Each employee should read the policy and agree to abide by it. Also, training on how to implement the policy should be provided for both managers and employees. Finally, updates to the policy should be made in a manner which ensures awareness on the part of all staff, for example, at meetings, through a newsletter, and via e-mail.

4. Users should receive proper training regarding e-mail and security and privacy issues surrounding its use

Due to a lack of awareness, e-mail users often assume that their communications are private.

"The more users know about e-mail systems, the better they will be able to protect their own privacy and the privacy of others. Users need to understand the following about e-mail systems:

1. the e-mail process is not inherently private
2. a message does not necessarily disappear when it is transmitted
3. deleting a message from one's personal files does not necessarily delete all copies of the message
4. electronic files can be readily transferred
5. electronic mail systems may be networked to provide connections to other organisations or individuals, or to public access points
6. the addressee may not be the only person who reads the e-mail
7. copies of messages are not necessarily duplicates of the original [as a message can be altered before being forwarded]
8. people can break into e-mail systems
9. e-mail technology may work against privacy
10. e-mail can be monitored from a remote location without any indication that the monitoring is occurring
11. use of e-mail at remote sites may result in the creation of records that the organisation has little control over
12. not all e-mail systems automatically encrypt files and messages
13. wireless systems are more vulnerable to unauthorised interception of e-mail messages than other systems."

5. E-mail systems should not be used for the purposes of collecting, using and disclosing personal information, without adequate safeguards to protect privacy

The privacy rights of both e-mail users and individuals who are the subjects of e-mail messages must be addressed. When personal information is exchanged via e-mail, several features inherent to e-mail systems may contribute to breaches of fair information practices required by Ontario's privacy law. The ease with which personal information may be exchanged via e-mail, both intentionally and inadvertently, may facilitate the unnecessary collection and inappropriate or unauthorised use and disclosure of personal information.

Although the originators of e-mail messages may carefully adhere to their information practices in disclosing personal information to others via e-mail, they may have no control over how that information is subsequently used or disclosed by recipients. Also, since recipients of personal information may not be aware of the original purpose for which the information was collected, they may inadvertently use or disclose the information for an inconsistent purpose. The further removed the personal information becomes

from the original source, the more difficult it becomes to adhere to fair information practices.

6. Providers of e-mail systems should explore technical means to protect privacy

There are some technical measures which can be incorporated into e-mail systems to enhance privacy protection for users and other individuals who are subjects of e-mail messages.

The first line of defence against unauthorised access to e-mail is user identification through a unique identification number, bar code cards or smart cards and authentication through the use of passwords, hand prints or voice registration.

Encryption is another important technical means of protecting privacy. However, even if a local e-mail system is capable of encryption, the messages which are transferred to a public e-mail system are vulnerable to interception, as encryption is not usually available with public systems.

Other privacy protection features include the capacity to conceal the subject of a message and a warning that a message requiring special security has been received. Also, automatic log-off from the system, whenever the computer is inactive for a specified period of time, is another security feature which will help to prevent unauthorised access to e-mail.

Each organisation should examine its own security needs and select a system which is most appropriate for itself. An organisation's needs for security may vary depending on the type of information that is transmitted and received via e-mail.

7. Organisations should develop appropriate security procedures to protect e-mail messages

Technical features and privacy protection policies regarding e-mail will only be effective to the extent that they are accompanied by appropriate procedures to ensure the security of files and messages transmitted and received via e-mail.

This shortened version of the Ontario Information and Privacy Commissioner's report was edited by Bojana Bellmay, a *Privacy Laws and Business* consultant.

The full text of the report *Privacy Principles for Electronic Mail Systems* published by Tom Wright, Information and Privacy Commissioner, Ontario is available from his office. See page 25 for contact details.

FRANCE: VIDEO SURVEILLANCE UPDATE

Mme Louise Cadoux, vice president of the CNIL, France's Data Protection Authority, has called PL&B to give further information on our recent report (PL&B October '94 p. 17) on the CNIL's jurisdiction over video suveillance.

She stresses that CNIL claims jurisdiction over both digital and analogue video images captured and stored by any device. If a video image of a person is stored at all, the CNIL claims competence.

As stated in our report, the Senate debated the Public Security bill on November 8th and improved the text. However, the Senate rejected the CNIL's view of the extent of its competence over video surveillance.

A minimum of 60 members of the National Assembly may make an appeal to the Constitutional Court against this decision. But in the past, the court has said that a new law may modify the scope of a previous law. Therefore, the CNIL's view is unlikely to prevail along this route.