Ontario defines privacy protection principles for voice mail systems

Information and Privacy Commissioner for Ontario, Tom Wright, issued, last October, a set of privacy protection guidelines aimed at users of voice mail systems. This is a third in a series of extremely useful papers produced by the Commissioner's Office to help organisations in both public and private sectors deal with privacy issues, related to technology in the workplace, arising from the widely used facilities and technologies - facsimile transmission, e-mail and voice mail systems. The *Privacy Laws & Business Newsletter* has already reported on guidelines for fax transmissions and e-mail systems (PL&B, Feb 1995, p.4, Dec 1994, p.8). Both private and public sector organisations should find the voice mail principles useful in their development and implementation of corporate voice mail policies.

The widespread use of voice mail and its popularity continues to expand on a daily basis. Many advantages have been recognised by its users; it facilitates communications, improves customer service, reduces time spent on hold, returning calls or talking on the phone. It can even enhance privacy since personal messages are communicated directly to the user, rather than through someone taking a message.

However, the voice mail system also has a negative side. Insecure systems or improper set-up and implementation can result in privacy breaches, as well as poor customer service. Voice mail security becomes even more critical with developments in technology and computer systems being increasingly integrated with telephone systems. These integrated systems can provide voice mail, e-mail, fax on demand, interactive voice response and other technologies at the desktop. The greater the number of connections, the greater the vulnerability of all those technologies to unauthorised access. That is where a corporate policy on privacy issues involved in these new technologies becomes essential.

Voice mail raises potential privacy concerns for senders, recipients and individuals who are the subject of voice mail messages.

The principles developed by the Information and Privacy Commissioner are not meant to be a standard set of guidelines applicable to all organisations. Due to different varieties and uses of voice mail systems, the guidelines are more of a framework for the development and implementation of an organisation's own privacy protection policies for the use of voice mail. They may need to be supplemented by examples specific to an organisation in order to increase employees' understanding of the principles.

The principles

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

Voice mail should be considered a private communication between the sender and recipient. However, due to the inherent characteristics of most voice mail systems, it is not possible to guarantee complete privacy. It is up to organisations to ensure that the system is set up and operated to guarantee the best possible degree of privacy and security. Unless organisations strive to offer the highest degree of privacy, employees may be reluctant to use voice mail to its maximum potential, hence annulling all the advantages of using the system.

2. Employees should receive proper education and training regarding voice mail and the security/privacy issues surrounding its use.

The more users know about voice mail systems, the better able they will be to protect both their own privacy and that of others. Any training should make the employees understand the following:

- the voice mail process in not inherently private
- a message that has been sent or deleted may still exist
- voice mail systems can be broken into
- voice mail technology may work against privacy.

3. Each organisation should create an explicit policy which addresses the privacy of voice mail users.

A formal and clear policy on voice mail privacy creates employees' expectations, helps to establish trust between employees and management, prevents litigation, wrongful termination law suits

and harmful publicity. Employees should be made aware of their rights and obligations under the policy and agree to adhere to it.

As a minimum, the policy should set out the following:

- approved uses of the voice mail system
- third party access to voice mail, including conditions and procedures for access
- consequences of violations of the voice mail policy.

4. Each organisation should make its voice mail policy known to employees and inform them of their rights and obligations regarding the confidentiality of messages on the system.

All staff should be informed abut their privacy rights and obligations regarding the use of voice mail in the workplace. By setting a clear policy and standard that everyone understands and agrees with, users will know what to expect regarding the confidentiality of messages on the system.

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

Every coherent corporate voice mail policy has to recognise that in addition to protecting the privacy of voice mail users, individuals who are subjects of voice messages also require protection. Some features inherent to voice mail may contribute to breaches of fair information practices, such as the ease with which personal information can be intentionally or unintentionally sent/forwarded. The further personal information becomes from its original source, the more difficult it becomes to adhere to fair information practices.

Since recipients of personal information may be unaware of the original purpose for which the information was collected, they may inadvertently use or disclose it for an inconsistent purpose. For all these reasons, subscribers may wish to record greetings that discourage callers from leaving messages containing sensitive information.

> "...subscribers may wish to record greetings that discourage callers from leaving messages containing sensitive information."

6. Organisations should pursue technological methods of protecting voice mail privacy.

Organisations should conduct privacy impact assessments of proposed or existing systems to determine how and when privacy may be threatened and address vulnerabilities before problems occur. Security needs of each organisation will vary depending on the type of information that is communicated via voice mail and the system's level of integration with the office computer network. Therefore, a risk assessment should be conducted to determine the organisation's security needs and select a system with an appropriate level of security.

There are several technological ways in which the privacy/securty of voice mail users and subjects can be enhanced. The security problems can be tackled and measures be implemented on three levels:

- by voice mail users
- by system administrators
- by automatic security features of the system.

7. Organisations should develop appropriate security procedures to protect voice messages.

Privacy protective policies and technological features will only be effective to the extent that they are accompanied by appropriate procedures to promote and maintain privacy, confidentiality and security.

New Fax Security Guidelines

The Office of the Information and Privacy Commissioner for Ontario has issued, in April this year, an updated set of *Guidelines on Facsimile Transmission Security*. First developed in 1989, and updated in 1990, the Guidelines have been revised once again as a result of the changes in fax and communications technology, increase in computing power, the use of networked systems, and the Internet, and the growing number of providers offering on-line services.

To obtain these documents, contact the Office of the Information and Privacy Commissioner/ Ontario, 80 Bloor Street West, Suite 1700, Toronto, Ontario, Canada, M5S 2V1. Tel: +1 (416) 326 3333 Fax: +1 (416) 325 91955