Information
and Privacy
Commissioner/
Ontario

Privacy Protection Principles for Voice Mail Systems

Tom Wright
Commissioner
October 1995

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

The Information and Privacy Commissioner/Ontario gratefully acknowledges the work of Peony Gandolfi in preparing this report.

This publication is also available on the IPC website.

Cette publication est également disponible en français.

Table of Contents

Principles

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

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

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

4. Each organization 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.

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.

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

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

Introduction

Voice mail is an electronic telephone messaging service that allows for non-simultaneous voice communication between two or more individuals. Like answering machines, the service takes messages for an individual who is unable to answer a call. However, because it is computerized, the powers and capabilities of voice mail are considerably greater.

Although voice mail appeared in the mid-1970s, its use did not become widespread until about a decade ago. Most private and many public organizations now use voice mail.[1] There are over 40 voice mail systems and an estimated 25,000 voice mail subscribers* within the Ontario government, with thousands of new accounts being opened each year. In the Toronto area alone, up to 100,000 voice messages are sent daily to Ontario government employees.[2]

The popularity of voice mail continues to expand worldwide. In North America, voice mail sales have averaged over $1 billion annually, and while the European market is smaller, voice processing equipment revenues are growing at a rate of 40 per cent a year.[3]

Voice mail has many potential advantages. It can facilitate communication and improve customer service, both within organizations and between organizations and external callers. It has been estimated that as many as 75 per cent of all business calls are not completed on the first try. By handling those calls, voice mail can allow organizations to reduce the number of incomplete calls by as much as 40 per cent.[4]

Voice mail is an efficient method of obtaining or providing information that can reduce "telephone tag" and time spent on hold, returning calls, or talking on the phone.[5] Voice mail may be used at any time and from any place using a touch-tone phone. It frees receptionists for other tasks and enables callers to leave detailed messages that may be difficult for human message takers to relay accurately. Voice mail can even enhance privacy since personal messages are communicated directly to the subscriber rather than through someone taking a message.

On the negative side however, insecure systems or improper set up and implementation (including a lax attitude towards security) can result in privacy breaches as well as poor customer service. Voice mail security will become even more critical as computer systems become increasingly integrated with telephone systems. These integrated systems can provide voice mail, electronic mail (e-mail), fax on demand, interactive voice response, and other technologies at the desktop.[6]

* In this paper, the term "subscriber" shall be used to describe an employee who owns a mailbox on an organization's voice mail system. Subscribers may send voice mail messages to other subscribers and may receive voice mail messages from anyone.

The greater the number of connections, the greater the vulnerability of all those technologies to unauthorized access. For example, the ability to access voice, fax, e-mail messages and other services in a single telephone call will make the need to guard passwords that much more critical. Integrated systems can only be as secure as the least secure gateway into the system.[7]

Another related technology with privacy implications is video mail. This emerging technology is similar to voice mail or e-mail except that the message can include a video image of the sender. Thus, the very purpose of the technology is often the automatic collection, use and disclosure of personal information. This has implications for how that information may be subsequently used, forwarded, retained, or disposed of.

Purpose

The Information and Privacy Commissioner/Ontario (IPC) has a mandate under the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* (the *Acts*) to research and comment on matters related to the purposes of the *Acts*. One of the primary purposes of the *Acts* is to protect privacy. The use of new and existing electronic information technology, such as voice mail, within government organizations has implications for privacy protection. While voice mail records can be requested under the access provisions of the *Acts*, this paper concentrates on the privacy issues associated with voice mail.

To heighten awareness of the privacy issues, the IPC has developed a set of privacy protection principles for organizations to consider when using voice mail systems.[8] Although the principles are directed to government organizations subject to the *Acts*, they have been written in such a way that other public and private sector organizations may also find them useful in their development and implementation of corporate voice mail policies.

Voice mail raises potential privacy concerns for senders, recipients, and individuals who are the subjects of messages. While the privacy of voice mail users[9] with respect to their communications is the primary focus of this document, the ease with which personal information can be exchanged via voice mail is another key concern. This poses a potential threat to the privacy of individuals who are the subjects of voice messages. Users need to bear these issues in mind each time they use voice mail.

Because of the different varieties and uses of voice mail systems, a standard set of guidelines would not be applicable to all organizations. Therefore, the IPC has outlined a number of general principles to provide organizations with a framework for the development and implementation of their own privacy protection policies for the use of voice mail. Organizations may wish to include organization-specific examples in their policies to increase employees' understanding of the principles. Note as well that the principles are interrelated and should not be considered in isolation of one another.

In developing a policy, there are many decisions to be made (e.g., security level required, systems administrator's duties, etc.). These decisions will, to some extent, be determined by the technological limitations of the voice mail system, the purposes for which it is used, the nature of the information exchanged on the system, and the business of the organization. The IPC believes that the policy should be guided by a commitment to offering the greatest degree of privacy protection possible for voice mail users and subjects within an organizational setting.

Principles

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

Generally, voice mail should be considered a private communication between the sender and recipient. Most people have an expectation of privacy on the telephone and often view voice mail as an extension of the telephone. Thus, users often mistakenly assume that using voice mail is as private as having a regular telephone conversation.

The term "privacy" takes on a variety of meanings within different contexts. It is a broad concept that covers a wide range of concerns about various intrusions into an individual's life, such as surveillance, wiretapping, and improper disclosure of personal information. The *Acts* focus on informational privacy, which is based on the idea that personal information belongs to the individual to whom it pertains. Individuals should therefore be entitled to some degree of control over the collection, use and disclosure of their personal information.

Another type of privacy is territorial privacy, which relates to the physical domain within which an individual claims a right not to be intruded upon. Both types of privacy apply, to some extent, in the context of voice mail systems. For example, when a hacker breaks into a voice mailbox and wreaks havoc, the subscriber may feel that his or her territory has been invaded. Informational privacy issues would come into play if the hacker also listens to messages containing personal information.

Due to the inherent characteristics of most voice mail systems, it is not possible to guarantee complete privacy. However, the privacy/security of any system greatly depends on how the organization sets up and operates the system. The potential to improve organizational effectiveness and efficiency by significantly enhancing communication is a major advantage of voice mail. But unless organizations strive to offer the highest degree of privacy possible, employees may be reluctant to use voice mail to its maximum potential.

One survey of American businesses indicated that almost 22 per cent of respondents (and 30 per cent of large companies who responded) had searched employees' computer files, voice mail, e-mail, or other networking communications.[10] Another American study found that over 27 per cent of managers admitted to "regularly scanning employees' voice mails."[11]

While employers may argue that electronic monitoring helps to increase productivity, research indicates that the reverse may be true. For example, another American survey found that electronically monitored workers were more tense, anxious, depressed, angry, bored, fatigued, and physically stressed compared to non-monitored employees.[12] The sense of powerlessness that is often associated with employee surveillance can be a major source of workplace stress.

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

Many privacy issues arise because users do not understand how voice mail works. For example, due to a lack of awareness, users often assume that their communications will always be private. The more users know about voice mail systems, the better able they will be to protect both their own privacy and that of others.

While it is not possible for an organization to educate and train every individual who may use its voice mail system, it can and should train its own employees. Proper training regarding voice mail and the privacy/security issues associated with it is also necessary before employees can effectively participate in the development of a voice mail policy.

In order to safeguard privacy and confidentiality, users need to understand the following about voice mail systems.

The voice mail process is not inherently private.

Because voice mail systems are accessible to anyone, they are vulnerable to breaches of security/privacy. As well, some systems can be networked so that subscribers on two different systems can send and receive messages across the two systems.[13] This can jeopardize privacy and confidentiality if the two systems differ in their levels of privacy protection and security.

There are many ways in which voice mail may be intentionally or unintentionally accessed by third parties. Messages can be overheard by others when played out loud on a speakerphone. Recipients can forward messages to any number of people. A policy might provide for third party access in certain situations. Unauthorized access by hackers, employers or others is another possibility. Voice messages can also be accidentally heard by third parties in the course of operating and maintaining the system.

Finally, regardless of how careful voice mail users, administrators and manufacturers may be, computer systems can always "act up" and inadvertently disclose messages to the wrong ears. In one case, a subscriber, who was trying to access her own messages, heard a message that was not addressed to her. In another case, a Manitoba lawyer attempted to call a government employee, only to find herself suddenly hearing a decidedly passionate voice mail message from the employee's lover.[14]

For all these reasons, it is best to avoid leaving personal, proprietary or other confidential information on voice mail.

A message that has been sent or deleted may still exist.

After a message has been sent, it will stay on the system until it is heard and erased. If it is heard and then saved ("archived") it can be retained for as long as there is room on the system. Deleted messages are retained until they are overwritten with new ones.

Voice mail systems can be broken into.

Hackers, competitors, and disgruntled employees have all been known to break into voice mail systems and commit sabotage or espionage.[15] These individuals can invade the privacy of both voice mail senders and recipients by accessing messages and using the information to the detriment of both parties without their knowledge or consent.

Hackers have been known to erase messages or prevent subscribers from retrieving their messages by changing their passwords. They can erase recorded greetings or change them into obscene messages. Such practices can tarnish an organization's image or lead to substantial losses in revenue.

In one American case, a florist discovered that someone had changed her voice mail greeting into one that was harmful to her business. The sabotage was traced to a former employer, who had obtained her password from the voice mail supplier by providing her social security number (SSN). Apparently, the supplier was using SSNs as access keys.[16]

Simple passwords present another temptation for hackers. Many systems are set up so that the password for a new voice mailbox is the same as the owner's telephone extension. Hackers can use a computer to dial each extension in an organization and easily gain access to the private messages of subscribers who did not change their initial passwords.[17]

Voice mail technology may work against privacy.

It is easy to send or forward messages by accident, or send/forward them to the wrong people. Caution should be used when sending/forwarding messages to groups of people. There may be some individuals on the distribution list who should not be receiving the message.[18] Once a voice message has been sent, the sender relinquishes any control over how that information is retained, used or disclosed by the recipient(s). A recipient can forward the information to others or even annotate it with a message of his or her own before forwarding it. Depending on its nature, the annotation can influence a subsequent recipient's interpretation of the message — all without the original sender's knowledge.

Users should also pay attention to the recorded greeting before leaving a message, otherwise a message could be left in the wrong person's mailbox. Mistakes that occur when messages are sent, forwarded or responded to may result in the inadvertent disclosure of sensitive personal information or incomplete or unedited information.

With some telephone models, it is also important to fully disconnect from someone's voice mail before making another call. Otherwise, the second call could be conferenced into the first. This means that a conversation held in the second call could be unknowingly recorded by the voice mailbox that was first dialled.[19] This underscores the need for employees to become familiar with the functions and capabilities of their telephone sets.

Principle 3 — Each organization should create an explicit policy which addresses the privacy of voice mail users

Every organization should develop a formal policy on voice mail privacy. A clear policy sets employees' expectations and helps to establish trust between employees and management. It may even help prevent litigation, wrongful termination suits, and harmful publicity.

Every employee should be made aware of his or her rights and obligations under the policy and agree to adhere to it.[20] The policy should enable subscribers not only to protect their own privacy, but that of other users and individuals who are the subjects of voice mail messages. External callers may be particularly vulnerable because they are often unaware of the privacy implications involved in the use of voice mail, such as possible third party access to the messages they leave.

For a policy to be effective, staff must recognize its merits and commit to its principles. Employee participation in the development and implementation of the policy is a key element in fostering commitment. Representatives of employees, managers, information systems, human resources, and legal counsel should all be involved in developing the policy.

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

- approved uses of the voice mail system;
- third party access to voice mail; and
- consequences of violations of the policy.

Approved uses of the voice mail system

A corporate policy should specify how the voice mail system may be used.

For business or personal messages

Voice mail messages may be personal or work-related. A voice mail policy should specify the degree of privacy which employees can expect with respect to either type of message. While third party access to personal messages should be forbidden, some employers may not feel the same about business messages.[21] The policy should clearly define the circumstances under which managers or others within an organization may or may not access employees' business messages.

Privacy concerns are more evident with respect to messages containing sensitive or confidential business information. Depending on the voice mail system's level of security, an organization may wish to place restrictions on its use for the communication of such information by employees. For example, organizations may implement special security procedures or place restrictions on the use of voice mail for the exchange of information that is excluded from disclosure under the *Acts*.[22] Organizations should also place restrictions on the sending, forwarding, and storing of business messages that contain personal information. (See Principle 5.)

To monitor for policy or security violations

Employers should avoid monitoring voice mail as a means to prevent or gather evidence about policy or security violations (e.g., safety violations, illegal activity, leaking of confidential business information, or discrimination). Alternative methods of detecting improper activity should always be considered first. For example, the systems administrator can determine whether an employee is not retrieving messages, or is receiving an unusually high number of messages per day and from where. These could be indicators of inappropriate behaviour which do not require listening to the employee's messages.

For staff evaluation purposes

Attempting to evaluate staff performance or activities by monitoring voice mail could be intrusive and diminish morale, normal communications and the free exchange of ideas. The usefulness, appropriateness and reliability of such monitoring should be considered carefully. Because voice mail messages present only one side of a story, it cannot be assumed that they can provide an accurate or complete picture of employee performance. There are more direct and less intrusive ways to monitor performance that are more effective.

An employer who is considering monitoring should carefully weigh the pros and cons. If a decision is made to proceed, staff should be consulted. Monitoring should never take place without the knowledge and consent of staff. Covert access or monitoring may not only be unethical but illegal, and could result in a lawsuit.[23]

To satisfy curiosity

Access to another individual's voice mail for unspecified purposes such as satisfying curiosity should be strictly forbidden. One American case involving a former McDonald's Restaurant employee led to a $1 million lawsuit against the employer. Voice mail messages indicating that the married employee was having an affair were accessed by the employer, who played them to the employee's wife and others.[24]

Third party access to voice mail

Organizations should always try to find alternative ways to obtain required information before resorting to searching employees' voice mailboxes. The policy should specify: the circumstances under which an employee's voice mail may be accessed by third parties; limitations on the use and disclosure of that information; and procedures to follow for approval of third party access. Subscribers should be told who has been granted access and if possible, should be notified prior to any access attempt.

Subscribers who cannot retrieve their messages for an extended period of time (e.g., due to vacation), should record a greeting that advises callers not to leave messages, particularly confidential and personal ones, during their absence. The greeting should provide an alternative contact. Some systems can be set up to prevent mailboxes from receiving messages when their owners are on extended absence. In-office or temporarily absent staff who can retrieve messages should clear their voice mailboxes at least once a day or more.

Conditions for access

Any third party access that is permitted should be defined, as unintrusive as possible, and limited to non-confidential business messages and legitimate business purposes. At a minimum, the policy should require that a request for access be made directly to the subscriber whenever possible. For example, staff could be asked for access prior to going on vacation.

Procedures for access

When access to a subscriber's voice mail is required, but not directly provided by the subscriber, procedures should be implemented for obtaining approval. The policy should specify who has the authority to approve and monitor access by third parties, in accordance with the policy. The approval process should include a review of anticipated use and disclosure of the information obtained. Whenever possible, prior notification of third party access to voice mail should be provided to the individuals concerned. Otherwise, individuals should be informed about the access, use and disclosure of their voice mail as soon as possible.

If a policy permits third party access, the organization has an obligation to inform external as well as internal users of this fact. For example, many systems can be set up to play a corporate greeting before an external caller reaches a subscriber's personal voice mailbox. This greeting can tell callers that any messages left on the system may be accessible to third parties.

Consequences of violations of the voice mail policy

Education and training for both managers and staff are necessary to ensure that the policy is understood and properly implemented. Such training could be provided at the same time as voice mail system training. During training, managers and staff should also be informed of the consequences of violations of the policy.

For any policy to be effective, organizations must include measures to ensure that it is being followed. Failure to enforce the policy would convey the message that the policy was not to be taken seriously. A requirement to adhere to the policy could be included in employees' performance contracts. Consequences of violations and procedures for lodging complaints about violations should be clearly specified in the policy.

Principle 4 — Each organization 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 about 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. A policy may also address who owns the information stored on the voice mail system and what rights the owner has.

It may not be sufficient to simply have the policy set out in the corporate policy manual. Each employee should read the policy and agree to abide by it. New employees could be introduced to the organization's voice mail policy and the privacy issues associated with voice mail as part of their orientation. Organizations should ensure that all staff are made aware of any updates to the policy. This might be done through newsletters, meetings, or e-mail. As well, the voice mail system itself can be programmed to provide special information to users when they dial into the system.

Principle 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

In addition to protecting the privacy of voice mail users, individuals who are the subjects of voice messages also require protection. Because voice mail may be viewed as a more private medium than e-mail, voice messages may contain more personal information than e-mail messages. Moreover, subscribers who forward their home numbers to their work numbers may be encouraging more personal information to be left on their voice mail than would otherwise occur.

Under the *Acts*, the privacy of individuals with respect to their government-held personal information must be protected. Personal information refers to recorded information about an identifiable individual, including information recorded via electronic means. To protect privacy, organizations should adhere to fair information practices[25] in relation to personal information.

Several features inherent to voice mail systems may contribute to breaches of fair information practices. For example, the ease with which personal information can be intentionally or unintentionally sent/forwarded, and failure to employ adequate security measures may facilitate unauthorized, unnecessary, or indirect collection, without the knowledge of the individual to whom the information pertains. It may also facilitate inappropriate or unauthorized use/disclosure of the information.

The further removed 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, personal information. On some systems, callers can edit or completely re-record a message before sending it, which is useful if callers feel that their original recording contained too much personal or confidential information.

While it is best to avoid communicating personal information via voice mail, it may sometimes be necessary. For example, when employees are in different locations and there is an immediate need for the information, it may not be practical to consider other forms of communication. When sending another individual's personal information, every attempt should be made to ensure that the message contains no identifiers that could link it with the individual concerned. Otherwise, steps should be taken to ensure that the collection, retention, use, disclosure, and disposal of personal information is done in accordance with the privacy protection provisions of the *Acts*. This is mandatory for organizations covered by the *Acts*.

Principle 6 — Organizations should pursue technological methods of protecting voice mail privacy

Voice mail companies should develop and promote the use of technological methods of privacy protection for their systems. Often, they can explain the vulnerabilities of a system and the privacy/security features available to their customers. Many now also offer security training for systems administrators. As well, security consultants are available to inspect an organization's voice mail system.[26] Organizations 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.

Each organization's security needs 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, each organization should conduct a risk assessment to determine its own security needs and select a system with a level of security that is appropriate for them. While there may be no such thing as a completely secure voice mail system, highly secure ones are readily available. However, more secure systems are generally more expensive and may be less convenient to use than less secure ones.

There are several technological ways in which the privacy/security of voice mail users and subjects can be enhanced. Organizations should determine what security features are available on their voice mail systems and implement those that are appropriate.

What subscribers can do

The first line of defence against unauthorized access to voice mail is user identification and authentication. For identification purposes, subscribers normally enter a unique identification number (mailbox number) on a touch-tone telephone keypad. Authentication is accomplished through the use of passwords. Normally, as long as passwords are kept secret, only legitimate users should be able to access their own voice mail.[27] While they are entering their passwords, subscribers should ensure that their telephone keypads are not being observed. Telephones which display the subscriber's identification number and password should be avoided.

Passwords should be at least six digits or longer and not trivial or easily guessed. For example, one's telephone extension, birth date, social insurance number, or child's name, etc. should never be used. Employers may wish to obtain a list of inappropriate passwords and instruct subscribers not to use them. Some systems can be set up to require a minimum number of digits in a password and to automatically reject easily guessed or trivial passwords (like "55555"). The odds against correctly guessing a password increase exponentially with each additional digit.

Depending on the level of security required, 10 to 20 digit passwords can be used to improve security for specific functions, such as system maintenance. Multiple access levels, requiring passwords for each level of access for particular applications might also be established for subscribers and systems administrators/programmers. Passwords should be memorized, kept secret, changed regularly, never written down, and never programmed into the speed-dial keys on the telephone.

In addition to passwords, there may be a number of other ways to enhance privacy. For example, in some systems, a voice message can be marked "private" before it is sent. This ensures that the message cannot be forwarded by recipients. There may even be a feature that allows a subscriber to find out whether someone has attempted to enter his or her mailbox.[28]

What systems administrators can do

To guard against unauthorized entry, many voice mail systems can be set up to automatically prompt subscribers to change their passwords at least every six months or less, depending on the needs of the organization. Some systems can also be set up to automatically disconnect after a specified number of failed attempts to enter a password. Regular system audits can expose multiple failed password attempts, thus alerting the employer to a possible security problem.[29] The security of the file in which identification numbers and passwords are stored and access to that file should be monitored and reviewed.

There are many access paths into a voice mail system which should be monitored for suspicious activity. Specialized software which enables a systems administrator to know who is using the system and when is available. Unauthorized or inappropriate access to voice mail can often be detected through changes in the normal patterns of use. In some cases, the systems administrator can even lock out a hacker by changing the password to a breached mailbox.

Another way to prevent unauthorized access is to immediately deactivate telephone numbers/extensions, identification numbers, and passwords when they are no longer required, or if they will not be used for an extended period of time (e.g., when an employee is no longer employed at the organization or is on a leave of absence). For additional security, internal telephone records, numbers, or system operator information should be shredded before they are discarded. This will prevent "dumpster divers" from digging up the information in order to obtain illegal access to the system.[30]

In extreme cases, organizations that are particularly concerned about security can shut down parts of the telephone system at night (the time when illegal entries often occur). However, this could also reduce the benefits and convenience of having a voice mail system.

Automatic security features

Some systems have built-in security features that do not have to be activated by the purchaser, such as message disk drives that cannot be downloaded and automatic message encryption. Encryption is an important technological means of protecting privacy that scrambles messages so that they cannot be understood if intercepted. Only the correct password can reassemble or decrypt a message for the listener. In many systems, including many public ones, messages are fragmented and automatically stored in encrypted form across a number of disk drives. Other systems also encrypt passwords or do not allow them to be copied or read from the drive.

Principle 7 — Organizations 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. For example, passwords will be ineffective if the organization does not implement a policy against sharing and disclosing them. The policy should warn individuals about the potential consequences of writing their passwords down or storing them where they may be found by others.

While passwords and encryption may help keep voice mail secure, they will not keep out systems personnel who have been granted access privileges. These privileges can enable the holder to access any subscriber's voice mail messages, without knowing his or her password, simply by changing the password. If this is done, perhaps in an emergency situation, the policy should require the subscriber to create a new password as soon as possible.[31]

Systems administrators are also able to create and delete mailboxes and perform other tasks on the system. These responsibilities should be limited to as few individuals as possible. To minimize the risks, organizations should develop well-controlled procedures for resetting passwords and a code of conduct for systems administrators that clearly defines their role and responsibilities. They should also have a responsibility to protect privacy in their performance contracts.

Sometimes systems administrators are contacted by potential hackers (perhaps posing as security specialists) or others requesting information about the organization's voice mail system. Such information should never be released without first taking all reasonable and appropriate steps to verify the identity of the caller and determine exactly why the information is being requested.

Another security issue concerns the existence of "back-up" copies of deleted messages that may be created by some voice mail systems.[32] If these are created, employees should be told about it. Policies and procedures should also be implemented to ensure that the retention and disposal of these messages do not pose a threat to the privacy of users.

With respect to physical security, the voice mail system should be located in a locked room, with access limited to authorized personnel only.[33]

Conclusions

Voice mail can be an effective tool that facilitates communication and the exchange of information both within organizations, and between organizations and the outside world. But without policies and procedures to protect privacy and confidentiality, the advantages of voice mail may come at a very high price. A commitment to protecting voice mail privacy and confidentiality may not only promote effective communication, but enhance the work environment by letting individuals know that their rights in the workplace are considered to be important enough to warrant protection. In addition, implementation of a policy will help to protect the privacy of individuals whose personal information is collected via voice mail.

The privacy protection principles summarized on the next page are intended to provide a framework for developing and implementing specific privacy-enhancing policies on voice mail. In developing these policies, there are several decisions to be made. Those decisions will, to some extent, be determined by the technological limitations of voice mail systems, the purposes for which they are used, the nature of the information communicated via voice mail, and the business of the organization. However, it is the IPC's belief that these policies should be guided by a commitment to offering the greatest degree of privacy possible in the workplace.

Principles

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

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

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

4. Each organization 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.

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.

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

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

Notes

1. Paul Brent, "Voice mail can do more than just answer phone." Telecommunications Special Report, *Financial Post*, April 1, 1995, p. 28.

2. Information provided by Corporate Information Technology Division of Management Board Secretariat.

3. Mary Ann O'Loughlin, "The European markets for voice processing and computer telephony," *The 1995 International VoicePower Directory & Buyers Guide*, January 1995, pp. 7-8.

4. Paul Brent, "Voice mail can do more than just answer phone." Telecommunications Special Report, *Financial Post*, April 1, 1995, p. 28.

5. A Gallup study on productivity found that 36 per cent of Fortune 500 telecommunications managers claimed voice mail had improved workplace productivity more than any other telecommunications product in the past three years.

   Source: Paul Brent, "Voice mail can do more than just answer phone." Telecommunications Special Report, *Financial Post*, April 1, 1995, p. 28.

6. Margaret Norton, "Messaging: the next step beyond voice mail," *The 1995 International VoicePower Directory & Buyers Guide*, January 1995, pp. 63-65.

7. Lawrence Surtees, "Security stifles voice mail hack attacks," *Globe and Mail*, May 1, 1991, p. B4.

8. See also two companion documents prepared by the IPC: *Privacy Protection Principles for Electronic Mail Systems* (February 1994) and *Update on 1989 Guidelines on Facsimile Transmission Security* (June 1990.)

9. In this paper, the term "user" will be used to describe any internal or external caller who sends a voice mail message. A user may or may not be a subscriber.

10. Charles Pillar, "Bosses with x-ray eyes," *Macworld*, July 1993, p. 4.

11. Dom Foulsham, "Who else is listening in to your voicemail?," *The Times*, June 16, 1995.

    To date, this is not known to have occurred within the Ontario government.

12. Richard L. Worsnop, "Privacy in the workplace," *CQ Researcher*, Vol. 3, No. 43, November 19, 1993, p. 1014.

13. "Octel Voice Information Processing — Intelligent Systems That Meet Changing Communication Needs." Version 6, 12/94. Product brochure.

14. "Racy voice mail message raises concern over privacy," *North Bay Nugget*, December 16, 1994, p. C5.

15. See William G. Flanagan and Toddi Gutner, "The perils of voice mail," *Forbes*, January 17, 1994, pp. 106-7. The article also recommends that when a key employee leaves to join a competitor, all remaining staff should immediately change their passwords.

16. *Second Annual Report of the Privacy Rights Clearinghouse* (October 1993 — September 1994), Center for Public Interest Law, University of San Diego, January 1995, p. 43.

17. To minimize this risk, systems administrators can assign random numbers as the initial, temporary password when creating new mailboxes. On some systems, the administrator can also prevent uninitialized mailboxes from receiving messages. This prevents the receipt of sensitive information that could be accessed by unauthorized individuals. It may also be a good idea for administrators to regularly check for and deal with mailboxes that have remained uninitialized for a long time.

    Excessive traffic on the system (especially during non-business hours), busy voice mail numbers, or several hang-ups in a subscriber's voice mailbox may all be signs that the system is being tampered with. If staff or the systems administrator suspect improper activity, they should notify each other via memo, not voice mail. As well, the passwords of the mailboxes concerned should be immediately changed.

    "The great voice-mail robbery," *The Economist*, August 13, 1994, p. 56.

18. Some systems enable a subscriber to deliver a single recorded message to several people at the same time through the creation of a distribution list. This eliminates the need to call each person individually to relay the same information.

19. Personal communication of Ross Tennant, Director of Marketing for Octel Communications Canada, Inc., June 1995.

20. Many of the ideas presented in this section were adopted from a document prepared for the Electronic Mail Association by David Johnson and John Podesta, "Access to and Use and Disclosure of Electronic Mail on Company Computer Systems: A Tool Kit for Formulating Your Company's Policy," September 1991.

21. To enhance privacy, business messages and personal/confidential messages should be stored separately whenever possible. This way, should there ever be a need to search an employee's business messages, his or her personal/confidential messages can remain private. A password-protected "home" mailbox might be an example of a personal message file. Available on certain systems, home mailboxes are portions of subscribers' mailboxes that have been assigned to subscribers' families. This allows subscribers to send messages to and receive messages from their families.

22. Subscribers should also note that forwarding a business number to a home answering machine can expose confidential business information to third parties.

23. See also the IPC documents entitled, *Workplace Privacy: A Consultation Paper* (June 1992) and *Workplace Privacy: The Need for a Safety-Net* (September 1993). The following excerpt from *Workplace Privacy: A Consultation Paper* may be applicable to voice mail communications:

> In Ontario, disclosure of a telephone conversation by a person who is not intended to be a party to such a conversation is prohibited under the *Telephone Act*. Section 112 of the *Telephone Act* provides that:
>
> > **112.** Every person who, having acquired knowledge of any conversation or message passing over any telephone line not addressed to or intended for such person, divulges the purport or substance of the conversation message, except when lawfully authorized or directed so to do, is guilty of an offence.
>
> According to the findings of a case in which section 112 was considered, the purpose of the provision is to create a right of privacy with regard to telephone conversations. In addition to the *Telephone Act*, the *Criminal Code* prohibits the interception of private communications, such as telephone conversations (p. 36).

24. "McDonald's snooping too," *Privacy Journal*, Vol. 21, No. 3, January 1995, p. 5.

25. Fair information practices are set out in the Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris 1980.

26. Management Board of Cabinet's *Information Technology Security Directive* (February 1991) states that, "Ministries and agencies must also conduct or avail themselves of periodic security reviews of (their information technology) facilities to ascertain that their security needs are being met" (p. 7-3-2). In addition:

Ministries and agencies must ensure that the contracts for information technology services negotiated with providers external to the ministry and agency include:

- a description of how the security requirements of the ministry's or agency's information systems will be met;
- a provision for periodic independent security reviews of information technology facilities (p. 7-3-3).

27. In some instances, organizations have arranged for the ability to reset passwords to allow subscribers who have forgotten their passwords to access their messages. However, this feature also enables the resetter to access those messages.

28. This feature requires the subscriber to record his or her name and the time each time the subscriber accesses his or her mailbox. Each time the subscriber subsequently accesses the mailbox, the system should play back the subscriber's last recording. If it does not, then unauthorized entry can be suspected.

29. Management Board of Cabinet's *Information Technology Security Directive* states that, "Periodic internal audits or independent verifications must be made of the security provided by any external information technology facilities used by the ministry of agency. Internal auditors must also conduct regular audits of internal facilities" (p. 7-3-3).

30. Stephane St-Onge, "Lack of voice-mail security can let hackers into system," Telecommunications Special Report, *Financial Post*, April 1, 1995, p. 37.

31. After resetting a password, the administrator will create a new, temporary password, which the subscriber should immediately change. If a temporary password has not been assigned, the subscriber will not be able to access his or her mailbox. If this occurs, it may be an indication of unauthorized entry and should be reported immediately.

32. For example, see *Second Annual Report of the Privacy Rights Clearinghouse* (October 1993 – September 1994), Center for Public Interest Law, University of San Diego, January 1995, p. 42.

33. When the voice mail system and the systems administrator terminal are locked in the same room, access is both physically protected and password protected. However, in cases where the two are located separately, and modems are used to connect them, the risk of unauthorized access increases.

In this situation, additional protection may sometimes be achieved by using a modem security device on the systems administrator terminal port. This device intercepts incoming calls and requires a user ID and password. If the entered codes are valid, the call is disconnected and the administrator is then called at a previously specified telephone number. When the administrator answers this call, access to the system is granted. Finally, a terminal access password is required before menus are displayed.

The systems administrator's password should not be automatically provided to individuals claiming to be maintenance personnel. Instead, call back numbers should be obtained and identities verified.

Sources: "Security on Octel Voice Processing Systems," Octel Product Note, April 1995, p. 11. Also, Octel Security Presentation training video, TRT:26:35.

Systems which are set up to enable service persons to dial into a port for maintenance purposes should be protected from illegal phone or modem access. A port is a serial or communications board inside the equipment that a modem connects to. This modem should be disconnected when not in use. A secure modem, such as the one described above, or password protected modem might also be used. A maintenance port that is not being used should be removed.

Source: Jan Smith, "Call of the dialed," *Compuserve Magazine*, June 1995, p. 35.

Physical security is infinitely more of an issue with respect to answering machines. Many office answering machines sit in highly accessible areas where the tape may be easily stolen or played by anyone with the push of a button. Messages are not encrypted and passwords are not required in order to access them. Messages are often played out loud for any passer-by to hear. Any policy on automated telephone answering systems that is going to include answering machines will need to address these kinds of issues.