Information
and Privacy
Commissioner/
Ontario

Privacy Protection Principles for Electronic Mail Systems

Tom Wright
Commissioner
February 1994

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

This publication is also available on the IPC website.

Cette publication est également disponible en français.

Executive Summary

Electronic mail, often referred to as e-mail, is a paperless form of communication which allows messages to be sent from one computer user to another. Within and between organizations, e-mail can be an effective tool that helps break down barriers to communication and promotes the free exchange of information and ideas.

On the negative side, however, one data security expert has noted that e-mail has "the same security level as a postcard."[1] Thus, users of e-mail may be exposed to breaches of confidentiality of their communications. 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.

While the privacy of e-mail users, with respect to their communications, is the primary focus of this document, a secondary concern is the ease with which personal information can be exchanged via e-mail. This poses a threat to the privacy of individuals who are the subjects of e-mail messages.

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 engage in research into matters which affect the carrying out of the purposes of the *Acts*. One of the primary purposes of the *Acts* is the protection of privacy. The use of new and existing electronic information technology, such as e-mail, within government organizations has implications for privacy protection. In order to heighten awareness of the privacy issues, the IPC 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 organizations under the jurisdiction of the *Acts*. However, the principles may also be useful to other public and private sector organizations in developing and implementing their corporate policies on e-mail.

The privacy protection principles outlined on the next page are intended to provide a framework for developing and implementing more specific policies on e-mail. In developing these policies, there are many difficult decisions to be made. The choices that are made will, to some extent, be determined by the technical limitations of e-mail systems, the purposes for which e-mail systems are used, the nature of the information exchanged via e-mail, and the business of the organization. However, it is our belief that these policies should be guided by a commitment to offering the greatest degree of privacy protection possible for e-mail users and subjects within an organizational context.

Principles

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

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

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

4. Users should receive proper training in regard to e-mail and the security/privacy issues surrounding its use.

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

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

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

Table of Contents

Introduction

Electronic mail, often referred to as e-mail, is a paperless form of communication. Whether the system is based on local area networks (LANs), main frame computers, or commercial e-mail services, e-mail allows messages to be sent from one computer user to another. Within an organization, e-mail can replace other forms of communication such as memos, telephone calls and personal visits.

Communications by e-mail are no longer limited to short, word-processed messages. With the development of increasingly sophisticated programs, some e-mail systems can now incorporate information in a variety of forms such as typed memos, spreadsheets, photographs, video clips, bar codes, and voice messages. It can also be linked to electronic data interchange, which is used to transmit structured electronic forms, such as order forms. Furthermore, the development of uniform standards for e-mail is permitting the linking of e-mail systems, allowing organizations to communicate beyond their corporate walls.

The Computer and Telecommunications Services Division of Management Board Secretariat estimates that about 28,000 employees of the Ontario Government are currently using some form of electronic mail system. Most of the e-mail systems in use are LAN-based and can be linked to each other and to public e-mail networks through a system called the Electronic Post Office.

E-mail has many potential advantages. It can help to eliminate “telephone tag” and may reduce paper use. When used by employees in different locations, it can minimize the impact of postal delays and time zone lags that can hamper other forms of communication. E-mail also helps to promote group discussions and generally enhances communication within organizations.

On the negative side, however, one data security expert has noted that e-mail has “the same security level as a postcard.”[2] Thus, users of e-mail may be exposed to breaches of confidentiality of their communications. 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.

While the privacy of e-mail users, with respect to their communications, is the primary focus of this document, a secondary concern is the ease with which personal information can be exchanged via e-mail. This poses a threat to the privacy of individuals who are the subjects of e-mail messages.

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 engage in research into matters which affect the carrying out of the purposes of the *Acts*. One of the primary purposes of the *Acts* is the protection of privacy. The use of new and existing electronic information technology, such as e-mail, within government organizations has implications for privacy protection. In order to heighten awareness of the privacy issues, the IPC has developed a set of privacy protection principles for the use of e-mail systems.

E-mail systems vary from a technical standpoint, and in terms of how they are employed and the types of information that they are used to transmit. Therefore, it was not possible to develop one set of guidelines that would be useful for all organizations. Instead, we outline a number of general privacy protection principles to consider in developing an organization's corporate policy on e-mail. These principles are intended to provide a framework for developing and implementing organization-wide privacy protection policies for the use of e-mail.

Scope

The principles are specifically addressed to provincial and municipal government organizations under the jurisdiction of the *Acts*. However, the principles may also be useful to other public and private sector organizations in developing and implementing their corporate policies on e-mail.

Principles

Principle 1 — The Privacy of E-mail Users Should be Respected and Protected

In March 1989, Epson Corporation fired its e-mail administrator. Although Epson claimed that the employee was fired for just cause, the employee believes that the firing was the consequence of questioning why a supervisor was reading employees' e-mail messages. The right-to-privacy lawsuit that the former employee brought against Epson left many legal and ethical issues about e-mail unanswered. However, one issue that was made clear in the lawsuit is that employees have an expectation of privacy in the use of e-mail.

The term "privacy" takes on a variety of different meanings within different contexts. It is a broad concept which covers a wide range of concerns about various intrusions into an individual's life, such as surveillance, wiretapping, and e-mail interception. The *Acts* focus on one specific type of privacy — informational privacy. Informational privacy is based on the assumption that personal information belongs to the individual to whom it pertains and that, as such, some degree of control or self-determination over its collection, use and disclosure is an individual's right.

Other types of privacy have also been identified. For example, territorial privacy relates to the physical domain within which the individual claims a right not to be intruded upon. Another type, privacy of the person, is reflected in laws which guarantee freedom of movement and expression, prohibit physical assault, and restrict unwarranted search and seizure of the person. Like territorial privacy, privacy of the person encompasses the notion of physical intrusion, but also transcends the physical dimension to the protection of a person's dignity. Each of these aspects of privacy apply, to some extent, in the context of e-mail systems.

Due to the inherent characteristics of most e-mail systems, it is not possible to guarantee complete privacy in relation to e-mail. However, it can be argued that it is in the best interests of an organization to offer the highest degree of privacy possible. We believe that this will enhance the quality of worklife and encourage employees to use e-mail to its fullest potential.

One of the strengths of e-mail is that it flattens the traditional hierarchical structure of an organization by breaking down barriers to communication between employees and their employers and managers. In a sense, e-mail has "democratized the workplace."[3] Enhanced communication can make the organization 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.

A survey of managers of businesses in the United States indicated that the searching of e-mail files is one of the most frequently used forms of employee monitoring.[4] However, while employers may argue that electronic monitoring helps to increase productivity, research indicates that it can actually have an adverse effect on productivity. For example, according to one study of employees of communications companies in the United States, electronic monitoring can increase "tension, anxiety, depression, anger, and fatigue."[5] The sense of powerlessness that is often associated with the use of employee monitoring can be a major source of stress in the workplace.

Principle 2 — Each Organization Should Create an Explicit Policy which Addresses the Privacy of E-mail Users

The very nature of e-mail heightens the need to address privacy considerations in the provision, use and regulation of e-mail systems. Every organization should develop a formal policy on e-mail privacy. Every individual within the organization should be made aware of his or her rights and obligations under the policy and agree to adhere to it.[6] The policy should enable users not only to protect their own privacy, but that of their co-workers who send them information and other individuals who are the subjects of e-mail messages.

For any policy to be effective, every e-mail user must recognize its merits and commit to its principles. Participation in the development and implementation of the policy is a key element in fostering commitment. But, before users can effectively participate in the development of a policy, they must receive proper training in regard to e-mail and the privacy and security issues surrounding its use. Education and training will also be necessary to ensure that the policy is properly implemented.

In order to formulate a policy that is best-suited to an organization, representatives of employees, managers, human resources, legal counsel, and information systems should be involved in its development.

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

- purposes for which the e-mail system may be used
- access to e-mail on the part of third parties
- consequences of breaches of the e-mail policy

Purposes for which the e-mail system may be used

The corporate policy should specify who may use the e-mail system and for what purposes. It is feasible that the e-mail system may be used by the following:

- employees of the organization
- clients, customers, and suppliers
- external consultants
- the general public

The more accessible the system is to those external to the organization, the greater the risk to security. Users of e-mail may be required to take special steps to ensure the security of e-mail messages, if external gateways are established. In addition, if others outside of the organization are permitted to access the e-mail system, they should be informed of the corporate policy on e-mail and agree to abide by it.

E-mail systems may be used for a variety of purposes within an organization. Some of the most common purposes are as follows:

- sending messages/files related to the business of the organization
- sending messages/files of a personal nature
- monitoring of e-mail for non-specific purposes (i.e., curiosity)
- monitoring of e-mail for purposes of staff evaluation
- monitoring of e-mail for policy or security violations

Business Messages

In comparison to other types of messages, privacy concerns are diminished with respect to e-mail messages which contain only non-confidential business information. Employers, managers and other individuals within the organization have a right of access to information which pertains to the business of the organization. Employees should not have an expectation of absolute privacy with respect to business information and should recognize the need to share this information freely with others within the organization.

However, concerns about privacy are more evident with respect to sensitive or confidential business information. Given the lack of security associated with many e-mail systems, an organization may wish to place restrictions on the use of e-mail for the transmission of sensitive or confidential business information. For example, organizations may choose to either implement special security procedures, or place restrictions on the use of e-mail for the exchange of documents that are excluded from disclosure under the *Acts*.

Similarly, organizations should place restrictions on the sending, receiving, and storing of business messages that contain personal information. Once personal information has been sent to others via e-mail, the sender will have little control over how that information is retained, used or disclosed by the recipient. The recipient may forward the information to others or may alter the information and then send it to others. In order to protect the privacy of an individual who is the subject of an e-mail message, the policy should restrict the sending of personal information via e-mail in the absence of adequate safeguards to protect privacy. Alternate forms of communication should always be considered in this context.

In some cases, an organization may find it necessary to exchange information about individuals via e-mail. For example, when employees are in different locations, the information is already available in electronic form, and if there is an immediate need for the information, it may not be practical to consider alternate forms of communication. In such cases, every attempt should be made to remove all personal identifiers before information is transmitted over the e-mail system. If it is not possible to remove all personal identifiers, steps should be taken to ensure that the collection, use and disclosure of personal information is done in accordance with the privacy protection provisions of the *Acts*. Security features and procedures that may be used in transmitting sensitive information are discussed below.

Personal Messages

A report from the State of California indicated that more than 60 per cent of all e-mail messages are of a non-business nature.[7] Each organization's policy should state the corporate position on the use of e-mail for sending messages of a social or personal nature since this will have implications for privacy protection.

There are a number of arguments against implementing policies which restrict non-business e-mail communications. The primary concern is that such policies could have a negative impact on communication, and interfere with normal social contact and the free sharing of ideas. For example, in order to protect itself from any potential lawsuits initiated by employees, Hewlett Packard sent out a memo saying that e-mail messages were monitored by department supervisors. In response to this memo, e-mail of all types, business and non-business, dropped by two thirds.[8]

Another argument for permitting personal use of e-mail among employees is that messages tend to be brief and to the point, and may actually take up less of an employee's work time than other forms of non-business related communications such as telephone calls or personal visits.

If personal communications are permissible on an organization's e-mail system, the policy should state how those communications can be protected. For example, personal communications can be password-protected and stored in protected areas that will not be readily accessible to others.

Monitoring of E-mail for Non-specific Purposes

Accessing another individual's e-mail for unspecified purposes such as satisfying one's curiosity should be strictly forbidden in all policies. E-mail should be considered to be a private communication between the sender and the recipient.

Monitoring of E-mail for Staff Evaluation Purposes

Some organizations may choose to monitor the e-mail communications of their employees for purposes of evaluating their performance or activities. For example, organizations may want to ensure that employees are being courteous to their clients or that they are making efficient use of the organization's resources. However, without a clear explanation of the purpose, procedures, and consequences, this type of covert monitoring may well have a negative impact on employee morale.

Even with advanced warning the monitoring of e-mail for evaluation purposes may be perceived as intrusive on the part of employees. This could not only affect morale, but may inhibit normal communications and the free exchange of ideas. Constantly looking over an employee's shoulder by electronic means is unlikely to foster a productive work environment. Furthermore, in many cases, there are more direct and less intrusive ways of monitoring performance that may also be more effective. The pros and cons of e-mail monitoring should be evaluated prior to considering its implementation. If a decision is made to proceed with e-mail monitoring, staff consultation should be undertaken. A more detailed discussion of the implications of electronic monitoring in the workplace is contained in other documents prepared by this office.[9]

Monitoring of E-mail for Violations of Policy or Security

An organization may want to monitor e-mail to prevent or gather evidence about violations of policies or security. Potential violations might include matters such as safety violations, illegal activity, misuse of corporate resources, racial discrimination, and sexual harassment. The invasion of privacy associated with e-mail monitoring under such circumstances may be perceived as being justified, particularly if there is other evidence supporting the existence of possible violations.

For example, an organization may wish to monitor e-mail messages to determine how the system is being used. Employers understandably argue that they have a right to determine how their corporate resources are being used. Indeed, some cases of e-mail monitoring have exposed incidents of abuse.[10] However, some experts suggest that it is possible to prevent abuse of e-mail without infringing on the privacy rights of employees.[11] For example, employers can look at the address, the header, the location from which an e-mail message is sent, and the size of the file, in order to determine whether or not corporate resources are being abused, without reading the actual contents of a message.

If the monitoring of e-mail for violations of policy or security is carried out on a routine basis, without just cause, this may be perceived as being invasive by employees. To avoid this perception, organizations should consider only monitoring e-mail to the extent required by law or by legal obligations to third parties, or to protect its interests in the event of reasonable suspicion of crime.

Access to e-mail on the part of third parties

There are some occasions when it may be considered necessary to access an employee's e-mail messages. For example, if a person is working out of the office, on vacation, or is off due to illness, it may be necessary for another individual to access his or her work-related e-mail messages.

It has also been noted that, in the process of operating and maintaining an e-mail system, some messages will inevitably be read and, therefore, privacy can never be guaranteed. For example, according to the State Information Security Manager for the State of California,[12] devices are sometimes attached to communication lines in order to record errors. When such devices are employed, data transmitted over that line, including passwords, identification codes, and messages, will be displayed in a form readable by the technician. For this reason, the State of California has stated in its proposed e-mail policy that the State cannot guarantee that e-mail communications will be kept private.

An organization's policy should specify the circumstances under which a person's e-mail may be accessed by third parties, any limitation on the use and disclosure of information that is accessed by third parties, and special procedures that should be followed for approval of access by third parties.

Conditions for Access

Depending on the nature of the information that is exchanged via e-mail, the policy governing access by third parties should be as unintrusive as possible. At a minimum, the policy should require that, whenever possible, a request for access to e-mail messages be made directly to the employee. For example, employees could be contacted at home or asked for access to their e-mail prior to going on vacation. When it is not possible to obtained access to e-mail directly from the employee, the policy should limit access by third parties for legitimate business purposes, when there are no other readily available means to obtain the information. Specific procedures to follow when accessing an employee's e-mail are discussed below.

From a privacy perspective, there is a distinction between non-confidential work-related messages on the one hand, and confidential or personal communications, on the other. In order to protect the user's privacy, wherever possible the two types of communications should be stored separately. This would allow personal communications to be password-protected and kept in a storage area that cannot be readily accessed by others. In the event that there is a need to search an employee's non-confidential work-related e-mail messages, the threat to the employee's privacy would be minimized.

Where personal communications are stored separately from work-related communications, the policy on access to personal communications can be more restrictive. For example, access to personal communications on the part of third parties could be prohibited. Alternatively, the policy may limit access to those circumstances which are sufficiently urgent to warrant the loss of privacy associated with reading an employee's personal e-mail messages. A more restrictive policy would limit access to circumstances where violations of policy or security are suspected, or for law enforcement purposes.

Use and Disclosure of E-mail

Once an e-mail message has been sent to or accessed by others, the originator of the message has little control over how the information will be subsequently used or disclosed. Therefore, the policy should specify limitations on the use and disclosure of information by recipients of e-mail or other parties who may gain access either intentionally, for some legitimate purpose specified in the corporate policy, or inadvertently, through the operation and maintenance of the e-mail system.

Without consulting the originator, information obtained via e-mail should only be used for legitimate business purposes and disclosed to others who have a need to know. In cases where particularly sensitive information is exchanged via e-mail, an organization may want to further restrict disclosure to third parties, upon the consent of the originator.

Procedures for Access

When access to an employee's e-mail is required and it is not provided directly by the employee, special procedures should be implemented for obtaining appropriate approval. One or more managers should be given the authority to approve and monitor access by third parties, in accordance with the corporate 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 e-mail should be provided to individuals whose e-mail is being accessed. If advanced notification is not possible, then individuals should be informed about access, use and disclosure of their e-mail as soon as possible.

Consequences of breaches in the e-mail policy

For any policy to be considered viable, there must be an effort to ensure that it is being followed. Failure to enforce the policy would convey the message that the policy was not was be taken seriously. Unenforced policies tend to be ineffective.

Procedures for lodging formal complaints about violations of the e-mail policy and consequences of any violations should be clearly specified in the organization's policy on e-mail.

In addition, staff should be made accountable for e-mail privacy in their performance contracts by including a requirement to adhere to the corporate e-mail policy.

Principle 3 — Each Organization Should Make Its E-mail Policy Known to Users and Inform Users of their Rights and Obligations in Regard to the Confidentiality of Messages on the System

In the absence of a known corporate policy, most users of e-mail appear to assume that their communications are confidential. Therefore, it is important that every employee be expressly informed about their 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 policy manual. Each employee of the organization should read the policy and agree to abide by it. Both managers and employees should also be provided with training on how to implement the policy.

Typically, when new employees are hired, they are provided with some form of orientation. This provides an excellent opportunity to introduce the subject of e-mail and the privacy issues surrounding its use. Organizations may also wish to consider displaying the policy on the computer screen each time the employee logs onto the e-mail system. Updates to the policy should be provided in a manner which ensures awareness on the part of all staff (e.g., at meetings, through newsletters, or via e-mail).

Principle 4 — Users Should Receive Proper Training in Regard to E-mail and the Security/Privacy Issues Surrounding Its Use

Privacy issues may arise when users do not understand how e-mail works. For example, due to a lack of awareness, users often assume that their communications are private. The more users know about e-mail systems, the better able they will be to protect their own privacy and the privacy of others.

In order to protect privacy, users need to understand the following about e-mail systems.

The e-mail process is not inherently private.

The very nature of e-mail makes it vulnerable to invasions of personal privacy. E-mail messages are often stored in one convenient location, where they can be accessed and searched electronically for a specific topic. For example, one poll of managers in the United States indicated that almost 22 per cent had searched their employees' computer files, voice mail, electronic mail, or other networking communications. Of those employers who had engaged in this type of monitoring, 66 per cent stated that they did not provide any warning of searches.[13]

Although some organizations may have a policy which limits access by third parties, in many cases these policies specify some circumstances in which access to e-mail by third parties is deemed necessary. For example, access may be permitted for law enforcement purposes. Also, during the normal operation and maintenance of the e-mail system, systems staff may access e-mail.

A message does not necessarily disappear when it is transmitted.

Many users assume that e-mail is a keyboard to keyboard or screen to screen transmission of information. However, once an e-mail message is transmitted, a copy may be printed and/or saved in a personal archive, such as on a hard disk. Furthermore, depending on the security measures employed by the recipient of the message, these copies may be vulnerable to unauthorized access by third parties. After an e-mail message has been sent, the sender will have little control over how the information is subsequently retained, accessed, used or disclosed by the recipient.

Deleting a message from one's personal files does not necessarily delete all copies of the message.

Once an e-mail message has been deleted, copies may still exist in back-up files automatically created by some systems and/or in the personal archives of recipients of the message. Back-up files are, in some cases, retained for prolonged periods of time. Retention periods for personal archives can vary from one individual to the next.

Electronic files can be readily transferred.

Once an e-mail message is received, it can be readily forwarded to any number of individuals, without the consent or knowledge of the originator.

Electronic mail systems may be networked to provide connections to other organizations or individuals, or to public access points.

E-mail systems that are accessible to others outside the organization are more vulnerable to breaches of security. Gateways to other e-mail systems may also provide links to other information stored on the system.

The addressee may not be the only person who reads the e-mail.

E-mail may be read by others who intentionally or inadvertently access the recipient's computer files, or others who may receive copies of the message from the recipient.

Copies of messages are not necessarily duplicates of the original.

Once a message is received, the recipient may alter the message before forwarding it to others. With some e-mail systems, recipients of forwarded messages may have no indication as to whether or not the original message was altered in any way. However, most e-mail systems currently in use have built-in mechanisms to prevent a message from being changed before it is forwarded.

People can break into e-mail systems.

It is possible that hackers, disgruntled employees, those involved in corporate espionage, and others, with or without malicious intent, may actively attempt to gain access to e-mail.

E-mail technology may work against privacy.

The easier an e-mail system is to use, the easier it is to make mistakes. For example, those features that enable users to forward a message with one keystroke, also make it easy for users to accidentally forward e-mail. 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 being transmitted via e-mail.

In order to avoid errors, individuals should be aware of how the system functions and its defaults. For example, in order to send a response to an e-mail, the user should know if the system automatically sends the response to the originator of the message only or if it sends the response to everyone who was copied on the original message. To avoid errors, users should carefully check the names of the recipients of all messages and responses to messages, prior to transmission.

E-mail can be monitored from a remote location without any indication that the monitoring is occurring.

Within an organization, there may be some individuals who wish to monitor another person's e-mail for a variety of reasons: to satisfy their curiosity, for purposes of evaluation, or to prevent or obtain evidence about potential breaches of security or policy. E-mail can be monitored at any time of the day or night, from a remote location. In most cases, users will have no way of knowing if and when e-mail is being monitored by third parties.

Use of e-mail at remote sites may result in the creation of records that the organization has little control over.

Users who have access to e-mail systems from remote sites, such as their homes, may make printed copies of e-mail messages and/or store copies of messages in unprotected personal archives at these locations. In addition, individuals working at one location could send information to be printed at another location. The organization may have little control over how the information in these records is retained, accessed, used, or disclosed by third parties at remote sites.

Not all e-mail systems automatically encrypt files and messages.

While many e-mail systems encrypt messages and files automatically, it is important to note that some do not. For example, encryption is virtually non-existent in public e-mail systems. Furthermore, if an e-mail system is linked to one or more different e-mail systems, unless the type of encryption is compatible, when a message leaves one system it will be decrypted and vulnerable to interception.

In some cases, without automatic encryption, it is possible for users to use special software designed to encrypt communications. However, this generally makes the e-mail system less convenient to use.

Wireless systems are more vulnerable to unauthorized interception of e-mail messages than other systems.

Many users are unaware of the fact that some LANs use radio frequencies and telephone transmissions and that wide area networks may be linked via satellite. E-mail systems which use radio frequencies are more vulnerable to interception than other systems.

Principle 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. In the context of the *Acts*, personal information refers to recorded information about an identifiable individual and includes information recorded via electronic means.

In order to protect privacy, the *Acts* require organizations to adhere to certain fair information practices in relation to personal information. In general, fair information practices help to ensure that personal information is not collected, used or disclosed without the knowledge or consent of the person to whom it relates. This allows individuals to maintain some degree of control over their own personal information.

Specifically, the *Acts* limit the collection of personal information to that which is necessary to achieve a specific purpose. With limited exceptions, they require that personal information be collected directly from, and with the knowledge of, the person to whom it relates. Under the *Acts*, use of personal information is limited to the purpose for which it was collected or a consistent purpose, unless the data subject consents to another purpose or there is legal authority to use the personal information for another purpose. The *Acts* also limit the disclosure of personal information to specific persons and circumstances. Individuals are given the right of access to their own personal information and the right to request correction if the information is inaccurate, out-of-date, or incomplete.

When personal information is exchanged via e-mail, several features inherent to e-mail systems may contribute to breaches of fair information practices. For example, the ease with which personal information can be exchanged via e-mail, both intentionally and inadvertently, may facilitate the unnecessary collection and inappropriate or unauthorized use and disclosure of personal information.

Although the originators of e-mail messages may carefully adhere to fair 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. Recipients could alter the information and forward it to others, or fail to employ adequate security measures to ensure that the personal information is not vulnerable to unauthorized or inappropriate access by others.

The further removed the personal information becomes from the original source, the more difficult it becomes to adhere to fair information practices. Collection of personal information may be carried out without appropriate authority and in a manner other than directly from the individual to whom the information relates. 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.

Principle 6 — Providers of E-mail Systems Should Explore Technical Means to Protect Privacy

Many individuals expect e-mail to have the same level of privacy as other types of communication such as telephone and postal services. Unfortunately, as mentioned earlier, e-mail has “the same security level as a postcard.”[14] Nevertheless, some technical features can be incorporated into e-mail systems to enhance privacy protection for users and other individuals who are the subjects of e-mail messages.

The first line of defence against unauthorized access to e-mail is user identification and authentication. For identification purposes, users can either enter a unique identification number at a keyboard or use a bar code card, magnetic stripe card, or smart card. Authentication is usually accomplished through the use of passwords. As long as passwords are kept secret, no one other than legitimate users should be able to access their e-mail. Passwords should be carefully constructed, never posted, and changed frequently. In addition, automatic log-off after a specified number of attempts to enter a password will help to prevent unauthorized access.

Authentication can also be achieved through biometric means, such as hand prints, voice registrations, or retinal images. However, the collection, retention, use and disclosure of this type of biometric information can also have serious privacy implications. If biometric security techniques are used, they should be implemented in a manner that does not pose a threat to privacy.

In order to prevent unauthorized access, identification numbers, access cards, passwords, and other means of authentication should be invalidated when they are no longer required, or where they will not be used for an extended period of time.

Encryption is another important technical means of protecting privacy. Many e-mail systems automatically encrypt files and messages into a special scrambled code, at the sender’s terminal, that can only be unscrambled with the use of the correct password, at the terminal of the receiver. This ensures the message is read only by the sender and the intended recipient(s). Unfortunately, encryption is usually not available with public e-mail systems, since many computing devices do not have the capacity to decrypt messages. Therefore, even if a local e-mail system is capable of encryption, it should be noted that messages that are transferred to a public system may be decrypted and remain vulnerable to interception.

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. Automatic log-off from the system, whenever the computer is inactive for some specified period of time, is another security feature that will help to prevent unauthorized access to e-mail.

From a technical perspective, patterns of e-mail use can be monitored electronically through the use of specially designed security software. This software permits those responsible for operating and maintaining the system to know who is using the system and when it is being used. Unauthorized or inappropriate access to e-mail can often be detected through changes in the normal patterns of use.

Some experts claim that it is possible to develop e-mail systems that offer complete security. However, such systems come at a cost. In general, secure systems are more expensive, require more computer processing capacity, and may be less convenient to use than less secure systems.

Each organization's needs for security will vary depending on the type of information that is transmitted and received via e-mail. Therefore, each organization should examine its own security needs and select a system with features that can provide an appropriate level of security. As suggested in the Information Technology Security directive distributed by Management Board of Cabinet, "the extent and cost of security measures are to be commensurate with the likelihood and/or potential impact of a breakdown in information technology security."[15]

Principle 7 — Organizations 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.

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 on the computer system where they will be vulnerable to access by third parties. If a password is loaned out, perhaps during a time of crisis, the policy should require that it be changed as soon as possible.

Passwords will also be ineffective if a computer is left unlocked and accessible when the individual is out of the office. This is a problem particularly if the computer is left on and the individual's password to the system has already been entered. In such cases, e-mail files and messages may be available to anyone who has access to the terminal. Even if the computer is not left on, e-mail messages that have been copied into a personal archive, such as on a hard disk, may be available to anyone who has access to the individual's computer.

In order to protect privacy, security procedures should ensure that individuals maintain an adequate level of control over their computers. Computers should not be left on in an unlocked environment, especially if they will not be attended to for a prolonged period of time. Also, depending on the nature of e-mail messages in the particular organization, security procedures may require that messages not be stored on any device that is not protected through the use of a password.

While a secure password and encryption may help to secure access to and use of corporate e-mail, they will not keep e-mail secure from a systems administrator who wants access or a manager who insists on looking over the administrator's shoulder or has similar access privileges. Systems administrators have the capacity to change passwords. Therefore, even if they do not know a password, those with systems administrator privileges can access e-mail messages by changing a password.

Growth in the number of LAN based e-mail systems has lead to increased opportunities for security infractions.[16] This is because, in many of these systems, the messaging database is distributed throughout several LANs. Each LAN may have several systems administrators, each with his or her own "superaccount". These accounts allow them to create and delete users, change passwords, and perform other tasks. By spreading this responsibility around the organization, the risk of unauthorized access to and use of e-mail may be increased. This is a problem particularly where the LAN is linked to other LANs outside of the organization. While staff education about privacy and security issues may help to minimize problems, organizations should also consider how changes to the LAN based architecture, involving fewer systems administrators, might reduce the security risks.

Another security issue is the "backed-up" copies of e-mail that are created by some e-mail systems. Even after e-mail messages are deleted, they are often permanently stored on magnetic tape, along with other data from the computer system. The unknown existence of an archive tape file of the White House PROFS e-mail system precipitated the investigation of Oliver North in the Iran-Contra hearings. Although North thought that he had deleted all sensitive e-mail messages, back-up copies were accessed and used as evidence in the investigation. While, in this case, the invasion of privacy may have been justified for law enforcement purposes, this may not always be the case.

If back-up files of e-mail messages are created, employees should be aware of their existence and policies and procedures should be put into place to ensure that the retention and destruction of back-up e-mail files do not pose a threat to the privacy of users. For example, back-up files should not be retained indefinitely.

Conclusions

Within and between organizations, e-mail can be an effective tool that helps break down barriers to communication and promotes the free exchange of information and ideas. But without policies and procedures to protect privacy, the usefulness of e-mail may be diminished. A commitment to protecting e-mail privacy 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 transmitted via e-mail.

The privacy protection principles outlined on the next page are intended to provide a framework for developing and implementing more specific policies on e-mail. In developing these policies, there are many difficult decisions to be made. The choices that are made will, to some extent, be determined by the technical limitations of e-mail systems, the purposes for which e-mail systems are used, the nature of the information exchanged via e-mail, and the business of the organization. However, it is our belief that these policies should be guided by a commitment to offering the greatest degree of privacy possible within an organizational context.

Principles

1. The privacy of e-mail users should be respected and protected.
2. Each organization should create an explicit policy which addresses the privacy of e-mail users.
3. Each organization should make its e-mail policy known to users and inform users of their rights and obligations in regard to the confidentiality of messages on the system.
4. Users should receive proper training in regard to e-mail and the security/privacy issues surrounding its use.
5. E-mail systems should not be used for the purposes of collecting, using and disclosing personal information, without adequate safeguards to protect privacy.
6. Providers of e-mail systems should explore technical means to protect privacy.
7. Organizations should develop appropriate security procedures to protect e-mail messages.

Notes

1. Ronald L. Rivest, personal communication of professor of computer science at MIT and a pioneer in the field of data security reported in *Technology Review*, Aug/Sept 1992, p. 11.

2. Ronald L. Rivest, personal communication of professor of computer science at MIT and a pioneer in the field of data security reported in *Technology Review*, Aug/Sept 1992, p. 11.

3. Michael Crawford, "The New Office Etiquette," *Canadian Business*, May 1993, p. 26.

4. Charles Pillar, "Bosses with X-ray Eyes," *Macworld*, July 1993, p. 7.

5. The study was conducted by researchers from the University of Wisconsin and the Communications Workers of America. James Pillar, "Bosses with X-ray Eyes," *Macworld*, July 1993, p. 6.

6. Many of the ideas for topics addressed 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.

7. Office of Information Technology, Department of Finance, State of California, "Security and Risk Management Guidelines Update," *Calculated Risk: Risk Management, Public Access and Privacy*, Apr-May-Jun 1992, p. 4.

8. Jeffrey Rothfeder, *Privacy for Sale: How Computerization has Made Everyone's Private Life an Open Secret*, New York: Simon and Schuster, 1992, p. 170.

9. See *Workplace Privacy: A Consultation Paper* released June 1992 and *Workplace Privacy: The Need for a Safety-Net* released September 1993, by the Office of the Information and Privacy Commissioner/Ontario.

10. For example, two employees at Nissan Motor Corporation in the United States were fired for "unprofessional work habits, including misuse and personal use of the e-mail system." The two were caught exchanging messages that push the limits of corporate propriety by their superiors. Jeffrey Rothfeder, *Privacy for Sale: How Computerization has Made Everyone's Private Life an Open Secret*, New York: Simon and Schuster, 1992, p. 168.

11. Alice LaPlant, "Perspectives. Is Big Brother Watching?," *Infoworld*, 12:43, October 22 1990, p. 65.

12. Office of Information Technology, Department of Finance, State of California, “Security and Risk Management Guidelines Update,” *Calculated Risk: Risk Management, Public Access and Privacy*, Apr-May-Jun 1992, p. 4.

13. Charles Pillar, “Bosses with X-ray Eyes,” *Macworld*, July 1993, p. 7.

14. Ronald L. Rivest, personal communication of professor of computer science at MIT and a pioneer in the field of data security reported in *Technology Review*, Aug/Sept 1992, p. 11.

15. Management Board of Cabinet, Information Technology Security, Directive 7-3, February 1991, p. 1.

16. James Carroll, “The Increasing Risk of Using E-mail,” *The Bottom Line: The News and Information Publication for Financial Professionals*, September 1992, p. 21.