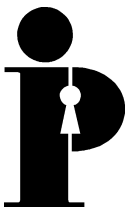
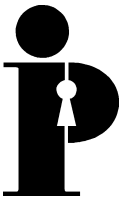
Information
and Privacy
Commissioner/
Ontario

Guidelines on Facsimile Transmission Security



Ann Cavoukian, Ph.D.
Commissioner
Revised January 2003



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 Mark Ratner in preparing this report.

This publication is also available on the IPC website.

Cette publication est également disponible en français.

Table of Contents

Introduction **1**

Obligations Under the Acts **2**

Purpose **3**

Guidelines **4**

Overview 4

Procedures for Sending 5

Procedures for Receiving 8

Staying Aware of the Availability of Privacy Enhancing Technologies **10**

Sending Faxes Directly from Computers **12**

Conclusion **13**

Sources and Further Readings **14**

Introduction

A facsimile (commonly referred to as a fax) is a production of an exact copy of a document by electronic scanning, and the subsequent transmission of the resulting data. Faxes are transmitted over ordinary phone lines using fax machines.

In a typical fax transmission, the document to be faxed is placed in the document feeder of a fax machine and the telephone number of the destination fax machine is dialled. In a very short time, a replica of the document is received at the destination fax machine. By their very nature, faxes can contain any information that appears in written form. As such, faxes will often contain information that is personal, or otherwise confidential.

Unfortunately, much as is the case with other media, faxes represent an imperfect form of communication. Sometimes, faxes do not reach their intended destination, whether it is as a result of human error in the dialling of the number, or because of a technical glitch.

In recognition of the risks involved in the use of fax technology, the Office of the Information and Privacy Commissioner/Ontario (IPC) issued its first *Guidelines on Facsimile Transmission Security* in June 1989. These *Guidelines* were designed for government institutions to consider and use in the development of systems that maintain the integrity and confidentiality of information transmitted by fax.

In February 1990, Ontario's Management Board Secretariat issued *A Directive for The Management of Information Technology Security*. One of the purposes of this directive was to ensure that ministries safeguard the confidentiality, integrity, and availability of their data that has been created, stored, processed, or communicated through information technology, including faxes.

One of the key principles enunciated that document was that "information technology security is to be consistent with the privacy and confidentiality requirements of the *Freedom of Information and Protection of Privacy Act*." This emphasis on privacy is indicative of the government's acknowledgement that the privacy of personal information plays a large roll in the development of technology security in the public sector, and is consistent with the IPC's *Guidelines* with respect to the use of fax technology.

Since the early '90s, the number of fax machines in use has continued to grow, and their variety and complexity has also increased. The use of networked systems, the Internet, and electronic mail (e-mail) have also had an impact on the uses of fax machines. In light of these developments, the IPC has prepared these updated *Guidelines*.

Obligations Under the *Acts*

Both the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* (the *Acts*) regulate government organizations with respect to the use, collection, disclosure, retention, and disposal of personal information.

Privacy is one of the two purposes in the legislation as expressed in section 1(b) of both *Acts*, which expressly states that a purpose of the legislation is:

> … to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right to access that information.

Section 42 of the provincial *Act*, (corresponding to section 32 of the municipal *Act*) sets out a limited number of circumstances in which an institution is permitted to disclose personal information. Because a misdirected fax is not one of the situations dealt with in the legislation, such disclosure would clearly be prohibited under either of the *Acts*.

It is important to note that privacy rules contained in the *Acts* do not apply to all organizations. Rather, they apply only to those organizations that are deemed to be "institutions." Section 2 of both *Acts* deem ministries of the government of Ontario, as well as agencies, boards, commissions, or corporations that are designated under the regulations to be "institutions" under the *Acts*.

While private sector organizations are not obliged to safeguard the personal information of individuals in the same manner as government institutions, private entities may use this document as a resource in formulating their own information security policies.

Purpose

The IPC recommends that institutions use these *Guidelines* in formulating their own written policies governing the use of fax technology.

Following these *Guidelines* will help ensure that institutions implement proper privacy practices (for example, limiting access to sensitive information to authorized persons) and eliminate improper practices (for example, permitting breaches of privacy, security or confidentiality).

While this paper deals briefly with the topic of Privacy Enhancing Technologies (PETs) such as encryption, we do not purport to identify all new fax-related technologies or products, nor do we recommend any particular product, brand name, or vendor. Because technology is constantly in flux, and reference to the latest electronic techniques will almost inevitability become out of date on publishing, users of these *Guidelines* are encouraged to take steps to educate themselves about emerging trends that impact upon fax security.

Guidelines

The process of ensuring that an office becomes a secure environment for the sending and receiving of faxed documents should be continuous. There should be a process of ongoing review of office policies and procedures in order to ensure that the security of faxed documents is preserved. In order to assist in the adoption of appropriate operating procedures, the IPC has put forward several recommended practices. These practices, which are dealt with below, are categorized into three broad categories: overview, procedures for sending, and procedures for receiving.

Overview

Establish Written Policies

In large part, the security of fax transmissions depends on the existence of adequate policies and procedures on the part of both senders and recipients of faxes. Putting these policies and procedures in written form will help to demonstrate institutional commitment to fax security. In addition, a written policy can serve as a useful resource to staff.

All government institutions should develop written policies governing the use of fax technology. The elements contained in those policies should mirror those contained in these *Guidelines*. It is crucial that policies address all of the issues dealt with below.

Designate a Responsible Individual

A crucial element in the effective and secure handling of faxed communications is the development of standardized operating procedures. Integral to these procedures is the designation of one person (the designated individual) as being the person responsible for the handling of all incoming and outgoing fax communications. This individual should play several important roles, both in the handling of documents before they are faxed, and in dealing with incoming faxes once they are received. Offices should also designate a backup for the designated individual to deal with instances in which the designated individual is unable to fulfill his or her role.

Upon receipt of a fax, the designated individual should check the number of pages of the fax to ensure that it matches the number listed on the cover sheet. The individual should then staple all of the pages together, and distribute the entire document to the person to whom the fax was addressed.

Isolate Fax Machine in a Secure Area

An office environment in which the fax machine is easily accessible by all employees is problematic, especially in regard to the security of incoming faxes. In contrast to incoming mail, which is normally sent in sealed envelopes that will only be opened by the intended recipient or someone authorized on his or her behalf, faxes are often transmitted into a centralized location. This allows for the possibility that the entire contents of a faxed message can be easily read by all passers-by, thereby undermining the security of the information.

In light of this risk, high regard should be paid to the location of the fax machine. Ideally, office fax machines should be situated in a location that is not generally accessible. This way, faxes containing personal or otherwise confidential information can only be read by authorized personnel.

Additionally, organizations may receive fax messages after normal office hours. During this time, security may be relaxed and only certain departments may be staffed. Under such conditions, it is prudent for organizations to identify and isolate a specific fax machine that would be programmed to receive all messages after office hours. This co-ordination could be accomplished by having the institution program the fax machine to forward all faxed messages to a central machine during non-working hours. If the fax machine is used to transmit or receive personal or sensitive information, accessibility should be limited to authorized persons.

Procedures for Sending

Use Cover Sheets

All faxes sent by institutions should be accompanied by a standardized cover sheet containing the name, title and organization of both the sender and the intended recipient, along with a notation indicating the total number of pages faxed.

As an extra measure of security, the cover sheet should include a box that allows the sender to "check off" whether he would like the recipient to confirm that she has successfully received the transmission.

The cover sheet should also include a written notice that the material contained in the fax is confidential, and that it may contain personal information that may be subject to the privacy provisions of the *Freedom of Information and Protection of Privacy Act* or the *Municipal Information and Protection of Privacy Act*. The notice should also explicitly state that the fax should not be distributed, copied, or disclosed to any unauthorized persons, and it should also provide instructions for the recipient to follow when the fax is received in error.

Categorize Data

Although high regard should be paid to the security of all documents transmitted by way of fax, not all forms of information attract the same degree of scrutiny. In cases where the document in question contains recorded information about an identifiable individual, the information is considered to be "personal information," and therefore subject to the privacy provisions of the *Acts*.

The scope of the definition of "personal information" is large. Commonly, personal information can appear in documents such as application forms, contracts, correspondence, or client databases. IPC Orders that have interpreted the definition have confirmed that information about an individual will be defined as being "personal" wherever that information is about an identifiable individual acting in a personal capacity.

As a general rule, personal information should not be faxed. Where possible, institutions should take steps to deliver hard copies of records containing personal information. E-mail, where protected by encryption, is also a viable option for the transmission of personal information.

In cases where time or another similar constraint dictates that personal information must be faxed, institutions should consider making using of Privacy Enhancing Technologies such as fax encryptors. Additionally, institutions should also make efforts to sever all personal identifiers from documents that are faxed.

Where it is absolutely necessary to fax personal information that can neither be severed nor encrypted, senders should phone ahead to alert the recipient that a fax is on its way. The responsibility to call ahead is discussed at greater depth below.

Documents that do not contain personal information may still require greater security by virtue of their confidential nature. Examples of documents that may be confidential include (but are not limited to) documents that are classified as exempt record under the *Acts*. Examples of exempt records are Cabinet documents, law enforcements records, and records that are subject to solicitor-client privilege. Depending on their content, such records may give rise to security issues that are similar to those relating to the faxing of personal information.

Confirm number before dialling

Often, master lists of fax numbers maintained by institutions are either out-of date or simply inaccurate. Where such lists are used, they should be regularly checked to ensure currency. Likewise, where numbers that have been pre-programmed into a fax machine are used, these numbers should also be regularly checked for accuracy.

Where there is any doubt concerning the accuracy of the listed fax number, the person designated as being responsible for outgoing faxes should verbally ensure that the number is correct by confirming the number with a person in the office of the recipient. Taking this step will help to ensure that the fax transmission arrives at its intended destination.

Check accuracy of dialled numbers

Once there has been confirmation that the listed fax number is correct, steps must be taken to ensure that this number corresponds with the number that is actually dialled. On most fax machines, the number dialled by sender will appear on the display of the fax machine. As such, the destination fax number can, and should be confirmed by checking the number displayed on the screen before transmitting the document.

Phone ahead to advise that a fax is coming

As stated above, documents containing personal information should generally not be faxed. However, where circumstances dictate that personal information that cannot be severed from a document must be faxed, the sender of the fax should phone ahead to alert the intended recipient that a fax containing personal information is about to be sent.

Adopting this procedure will help to ensure that the recipient is aware of the sensitive nature of the document that will be received. If, after being informed that a fax containing personal information is on its way, the document is not received, the recipient should contact the sender in order to inform him or her that the fax has not been received. The sender will then be aware of, and be able to address, the problem that led to the errant transmission.

Check Confirmation and Activity Reports

Most fax machines have the capability to print a "fax activity confirmation report" after each use. These reports confirm whether a document has been correctly transmitted by indicating the destination fax number and the number of pages transmitted. The sender of each fax should confirm the success of a transmission by checking this report after the fax has been sent.

Likewise, the recipient should check the number of pages received against the transmitted fax cover sheet or the fax activity confirmation report (in cases where no fax cover sheet was transmitted). If pages are missing, the sender should be contacted and asked to re-transmit the information. For further elaboration on the recipient's duties, see the discussion on "Receiving Faxes" below.

Similarly, most fax machines are also able to print "fax activity history reports" based on either a time span or volume of activity. For example, the fax machine can be set to automatically print a history of its activity after every 40 transactions. This report helps monitor the use of the fax and accounts for its activity. On most machines, however, once this report has been printed, it cannot be reprinted.

Therefore, it is possible for an unauthorized user to print these activity reports and destroy them, leaving no trace of unauthorized activity. Thus, a person could remove an incoming fax not intended for him/her and eliminate any trace of the transaction by printing and destroying the activity report. As such, the designated person responsible for the fax machine should review the activity reports regularly to ensure that there has no been any unauthorized activity.

Procedures for Receiving

Notify the Sender of Errant Faxes

Despite an institution's successful adoption of written policies and procedures as provided for in these *Guidelines*, situations will inevitably arise where an institution receives a fax that was intended for a different recipient. An institution's written procedures should address what to do when a misdirected fax is received.

The first step should be to notify the sender of the fax received in error. This will alert the sender so that he or she can investigate whether the problem occurred as a result of a technical glitch or human error, and it will allow the sender to take steps to ensure the integrity of future fax transmissions.

At the same time, the recipient should confirm with the sender whether the errant fax should be returned to the sender (by means other than fax), or destroyed; the recipient should not forward the fax to the intended recipient.

Photocopy faxes where a retention period exists

Some older models of fax machines use specially treated thermographic or heat-printed paper to record incoming messages. Institutions having fax machines that use this type of paper are encouraged to photocopy the information received by fax, as the print on this paper will fade after a period of time. By photocopying the information, organizations can ensure that the information will be preserved and can be retained in accordance with minimum retention periods. In the case of personal information, the *Acts* require a one-year retention period.

After the information in question has been copied, the thermographic paper should be destroyed in a secure manner. Messages received on fax machines using thermal ink transfer or equipped with laser printers are not subject to fading.

Staying Aware of the Availability of Privacy Enhancing Technologies

Changing technology has led to a variety of new issues regarding fax security. While many of these changes give rise to operational advantages in terms of operational efficiency, they also create a host of related concerns. As such, institutions should be made aware of the existence of Privacy Enhancing Technologies (PETs). Generally, PETs are defined as being any type of technology that is designed to safeguard the privacy of individuals.

In the context of faxes, one helpful PET is encryption. Simply put, encryption is the name for the process through which digital information is scrambled into a code that may only be read by an individual who posses the required "key" that "unlocks'"the code. While encryption technology is generally used most often in relation to e-mail, devices can be attached to fax machines that provide for the encryption of faxed documents.

The utility of encryption arises out of the fact that faxes are transmitted over ordinary telephone lines or cellular networks. Like telephone conversations, fax transmissions may be tapped and intercepted by unauthorized third parties. The materials required to intercept a fax are surprisingly inexpensive, readily acquired, and easy to assemble.

With the use of a "fax encryptor," faxes sent from any fax machine can be encrypted so that risk of the message being intercepted is reduced. When properly used, a fax encryptor will alter the digitized information that flows from the sending fax machine so that it may only be interpreted by the machine that is the intended recipient. Although it is possible for third parties to intercept faxes before they arrive at their final intended destination, any such information will be in the form of a jumbled encrypted code, rather than a readable document. The use of this technology is therefore an option for institutions to consider when faxing personal or confidential information.

Users of this technology should be cautioned that encryption is not a panacea against any and all security breaches. Because of the limits to fax technology, it is possible for a determined individual to intercept an encrypted fax message and then proceed to manually "break the code."

Additionally, the use of encryption is limited by the fact that fax encryption has not yet gained wide use across government. Because encryption will only "work" where both the sending and the receiving fax machine are equipped with encryptors, there are many instances where the use of encryption is not a viable option.

Because of the security problems associated with fax encryption technology, and the fact that encryptors are not widely used, the IPC recommends caution when using this technology

to transmit documents of a sensitive nature. If there are fears that the fax in question is a target for interception, encryption should not be used. Rather, the sending office should consider arranging for the hand delivery of the documents, or consider the use of encrypted e-mail — a practice that offers enhanced security protection as compared to encrypted faxes.

To use fax encryption technology, both senders and recipients must have the same type of fax encryptor. These encryptors may be useful as a practical safeguard to be used within a "closed" group of users, such as within a department.

On an organizational level, each group of users located in one building may consider dedicating one fax machine to encrypted transmissions. All organizations connected with this group could then use the same type of fax encryptor. In this way, if a fax was wrongly sent to a machine not equipped with a compatible encryptor, the recipient would not be able to read the fax.

Among other examples of PETs for fax machines are features such as "keylocks" and "confidential mailboxes." These devices are useful in overcoming the risk of unauthorized use of the office fax machine. In some instances, institutions may need to fax information requiring greater than normal security protection. In these cases, the fax machine could be equipped with a keylock dedicated to this purpose. A keylock is a fax security device which, when activated, prevents both the transmission and reception of faxes. By installing a keylock, an institution can control who uses the fax machine.

Confidential mailboxes are memory locations of a fax machine that can store incoming documents. Documents that are transmitted into a confidential mailbox can only be printed after the correct password has been entered. The result is that only a specific person can receive a transmitted document. Using this technology requires that the sender's machine is be capable of transmitting a message to a machine having the mailbox feature.

In order to preserve the contents of a confidential mailbox during a power disruption, some users provide fax machines with a more permanent storage device such as a hard disk. The advantage of this system is that the contents of a hard disk cannot be compromised as a result of power failures.

Sending Faxes Directly from Computers

Part way through the 1990s, there was an increase in the popularity of "fax-modems." These devices allow users to send and receive faxes directly from/into computers equipped with modems fax capabilities. This practice is no longer common. Largely, e-mail has replaced the fax-modem as a preferred way of transmitting a document from one computer to another. However, because this technology still exists, it is necessary to deal with privacy and security issues relating to fax-modems in these *Guidelines*.

Operational advantages created by the use of fax-modems include:

- large computerized databases of telephone lists can be maintained and used to send faxes to groups of people;
- the size of a document is no longer a deterrent and people are no longer restricted to printed documents;
- virtually any information that is stored on a computer (e.g., letters, reports, financial spreadsheets, pictures) can be faxed;
- a fax can be compiled from various sources of information that are stored on a computer;
- unlike a printed document that is handled by a fax operator, it is very easy to edit a fax that is stored on a computer (before sending or after receiving it); and
- anyone with a computer and the necessary software/hardware can send/receive a fax.

Several of these operational advantages also give rise to privacy concerns. For instance, the fact that anyone with a computer is able to transmit and receive a fax means that traditional controls used to enhance security and privacy may have to be broadened to deal with the increased accessibility of the fax technology.

In addition to the use of computers to transmit faxes via fax-modems, developments in mobile computing and wireless communication have added an additional layer of concern regarding the secure transmission of faxes. A laptop or notebook computer equipped with fax software and hardware can be used to send or receive faxes using a cellular telephone. As well, portable and hand-held fax machines can be used virtually anywhere.

Because of the unique problems posed by these forms of fax technology, institutions should be aware of whether their employees have the ability to send and receive faxes via their computer terminals, and should take steps to limit their use in accordance with these *Guidelines*.

Conclusion

The *Guidelines* are intended to be a starting point for institutions in the formulating of their own policies and procedures governing the use of fax technology. It is hoped that institutions will approach challenges of enhancing fax security in their workplace with due regard to the specific circumstances of their operating environment.

Sources and Further Readings

Office of the British Columbia Information and Privacy Commissioner, *Guidelines for the Secure Transmission of Personal Information by Fax* (August 1996), online: www.oipcbc.org/advice/faxguide.php.

Office of the Information and Privacy Commissioner (Alberta) *Guidelines on Facsimile Transmission* (revised October 2002), online: www.oipc.ab.ca/ims/client/upload/Guidelines_on_Facsimile_Transmission.pdf.

Organisation for Economic Co-operation and Development, *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (OECD, 2002), online: www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf.