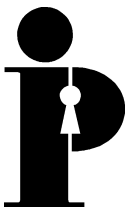
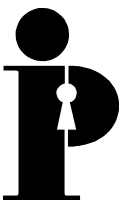
Information
and Privacy
Commissioner/
Ontario

Electronic Records:
Maximizing Best Practices



Tom Wright
Commissioner
March 1997



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 *John Eichmanis* in preparing this report.

This publication is also available on the IPC website.

Table of Contents

Foreword **1**

The Issues **3**

Practices **5**

The Meaning of an Electronic Record 5

Anticipating Future Access Requirements 7

Retaining Electronic Records 11

Security Issues 13

Providing Access to Electronic Records 14

Routine Disclosure/Active Dissemination 15

Conclusion **16**

Appendix A **17**

Foreword

When Ontario's freedom of information and protection of privacy scheme was conceived, use of information technology was still limited to specialized functions. Since then, information technology has advanced with astonishing speed. Many offices are now equipped with computers connected to local area networks and the Internet. While the use of paper has not disappeared, many government organizations are beginning to rely increasingly on various information technologies as the primary means to conduct their day-to-day operations.

In practical terms, more and more records are being created electronically, that can be stored and retrieved electronically, though, needless to say, paper copies are also being retained. It should be remembered that despite the form that a record or piece of information takes, the *Freedom of Information and the Protection of Privacy Act*, and the *Municipal Freedom of Information and the Protection of Privacy Act* (the *Acts*) apply to such documents.

How the *Acts* will operate in this new electronic environment is of concern to records managers, archivists, and other information and privacy professionals. There are a number of issues which need to be examined.

The Office of the Information and Privacy Commissioner (the IPC) shares with all government organizations an interest in ensuring that the *Act*s work effectively. In this context, the IPC has developed this discussion paper entitled *Electronic Records: Maximizing Best Practices*. The purposes of this document are to (1) support better implementation of the *Acts* by raising issues regarding the proper ongoing retention and accessibility of electronic records, (2) help those working with information technologies to better understand their obligations under the *Acts*; and (3) provide suggestions for resolving the issues raised.

In order for individuals to access records, they must be protected against premature disposal and effectively managed. In its annual reports and orders, the IPC has emphasized the importance of proper records management within government organizations. In this new and changing electronic environment, effective management will be even more crucial in ensuring that the *Acts* continue to work for the benefit of the Ontario public.

The suggested practices outlined in this paper are just that — suggested practices. Undoubtedly many organizations have begun to think about the impact of various information technologies on the effective operation of the *Acts*, for retaining records, for archival purposes and for simply dealing with day-to-day operations.

Certain broad standards for dealing with records have been produced. At the provincial level, reference can be made to the *Archives Act*, and the Ontario Archivist's Recorded Information Management bulletins and fact sheets, and the directives and guidelines of Management Board of Cabinet. At the municipal level, many municipal organizations have developed effective ways of dealing with their records.

One of the key purposes of the *Acts* has been to strengthen openness and accountability in government. Such information can be viewed as a common asset that individuals may utilize to increase their own well-being and that of the larger community. The new electronic environment has also transformed government information into a commodity with potential commercial value.

The promise of information technology is that it should enhance the ability of the public to access information. It is a vision of the future that is motivating much of the construction of the information highway. For both the purposes of the *Acts* and the benefits of these technologies to be achieved, however, it will be necessary for government organizations to apply coherent practices to create, disseminate and maintain electronic records.

In preparing this document, discussions were conducted with the Archives of Ontario, Management Board Secretariat, and the Municipality of Metropolitan Toronto Archives.

The IPC wishes to thank these organizations for their assistance. The practices suggested in this document should be read in conjunction with the appropriate guidelines and directives that are issued by Management Board of Cabinet at the provincial level, and the guidelines and directives that may be issued by each municipal organization.

The Issues

Management of electronic records presents interesting challenges for many public sector organizations. The illustrations cited below indicate some of the difficulties that public organizations can encounter if electronic records are not managed in a systematic way.

- The United Nations discovered that methods for identifying, storing, and retrieving vital electronic data, such as field reports on social and economic issues in developing countries, had been completely ignored since the widespread introduction of office-automation technology.

- The National Archives and Records Administration in Washington D.C., which is the repository for all federal government records, found that after just 15 years, old magnetic tapes of electronic records were unreadable because new faster machines burned out the tapes.

- The U.S. National Aeronautics and Space Administration (NASA) found that magnetic tapes that chronicled three decades of space flight, which could be intended as a source to help determine long term trends in climate change, could not be read either because the material was not catalogued, had been damaged by heat or floods, or was not labelled according to archival standards. To make some sense of this material NASA will be required to spend millions of dollars.

With the advent of information technologies, the variety of ways that information can be created, stored and manipulated has increased many-fold in comparison to the days when information was produced almost solely through the medium of paper. In devising a strategy to deal with electronic records, organizations may well need to consider this issue in the wider context of managing their global information requirements and the diverse forms of information technology that now exist.

Electronic records exist in an environment that encompasses various forms of hardware, software, and information or data. Moreover, an electronic record can exist simultaneously in a variety of mediums — on paper, in a CD-ROM, on tape, or on hard disk. In fact, no single medium may hold all the records that reflects an organization's activities or functions. Electronic records, however, can be subject to alteration, correction and deletion once a transaction or decision is complete, thereby weakening their authenticity and subsequent usefulness as evidence of the original transaction or decision. Important information about who created the records, when and for what purposes may be lost.

The computer, which just a few years ago was used almost exclusively by technical specialists, is now being employed by nearly everyone in an organization. As a consequence, individual users are often in control of what happens to the records that they create. Given such a decentralized framework for assembling information, corporate standards are essential in order to effectively maintain an organization's records holdings.

For many users of desktop systems , electronic records are created and used in real time, and once they are either sent by e-mail or read, there may seem little reason to keep them. That is, to file them according to some systematic criteria, as was done for paper records. This scenario is less likely to be played out where records are stored in highly structured, closely managed information systems. Problems are more likely to arise with records that deal with administrative, policy formulation, and decision making processes in the organization.

In his annual report for 1994, the Commissioner pointed to a compelling irony - the information age could be the least documented period in human history. In the past, decisions on whether or not to retain a document were typically made months or years after the record was created and temporarily filed. Today, these determinations are often made by individuals soon after the electronic record has been created or within a few days or months, but certainly not years. What is being destroyed are not just historical records but contemporary ones as well.

Based on the principles of the *Acts*, records cannot be accessed by the public if they do not exist. If contemporary electronic records are being destroyed, revised or otherwise affected so that they cannot be retrieved in their original form for purposes of the *Acts*, the rights granted under the *Acts* cannot be properly exercised. Even if records are retained, inadequate provisions may be made to ensure that records remain readable and retain their full value as evidence of decisions or transactions. Changing technologies may render records unreadable or alter their original structure or appearance as documents or data. The management of recorded electronic information can, therefore, be viewed as being integral to the operation of the *Acts*.

Practices

The practices discussed below are arranged so that a suggested practice is cited first, followed by a brief discussion of the reasoning behind the practice. Organizations should take into account their own particular circumstances. The practices suggested here assume that an organization is only beginning the process of dealing with electronic records. To assist the reader, references are made to various authorities, listed in the Appendix A, that form the basis for a particular practice. Appendix B contains a list of sources that are available for further consultation.

The Meaning of an Electronic Record

Practice 1 **Since 'electronic records' may not necessarily take material form (hard copy), a 'record' should be viewed as being an all-inclusive term that encompasses every conceivable way that information, including data, text, image or sound, can be created, stored and retrieved electronically.**

We have been used to thinking that what is printed on paper is a record, because it possesses physical properties. More and more government organizations, however, now utilize various forms of information technology, principally the personal computer, to assemble and present information. The records or other electronic image* created by using this technology may not in many instances be stored as such on the computer. The data or text may only exist as stored memory that can be assembled and retrieved later to form a coherent document or image, or a sound playback. It can also be immediately erased without ever being printed on paper or any other form, or it can be stored electronically, for example, on a hard disk or diskette.

The *Acts* anticipate the creation of records by electronic means, though they do not explicitly describe all the forms that such electronic records could take. The *Acts* define the term record as including any record that is capable of being produced from a machine readable record by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution.** (See Appendix A, Note 1) Similarly, Management Board's Directive 7-5, " Management of Recorded Information" defines recorded information to include various forms of electronic records. (See Appendix A, Note 2).

* Throughout this paper, the term 'electronic records' includes data, text, images and sound. If one of these descriptors is not present, no change in meaning is intended.

** The interpretation of the provisions of the *Acts* relating to electronic records is subject to change and may vary depending on the circumstances of the appeal or investigation in which the issue is raised.

Practice 2 **E-mail that records communications relating to the mandate or functions of the organization, and are in the custody and control of the organization, should be considered as a record for the purposes of the *Acts*.**

Within the context of describing electronic records, special mention should be made of electronic messages, or e-mail.

The use of e-mail is becoming widespread in government. However, government employees may not always consider this form of communication to constitute a record, since the form of this communication may appear transitory, personal or unimportant. There is no doubt that in some cases e-mail bears no relation to the mandate or functions of the organization (for example, personal messages) or is so inconsequential that may not need to be retained for operational purposes.

Electronic messages, however, that document communications relating to the organization's mandate or functions should be considered to be records for the purposes of freedom of information legislation. (See Appendix A, Note 3) Such messages chronicle electronic exchange of views on the activities and functions of the organization or document business activities.

The practice of some organizations is to automatically print a copy of such messages for a paper file. Although this is not a long term solution, it may be necessary until the retention capabilities of information technologies have been further developed. Otherwise, important e-mails should be systematically saved onto subject or program-based directories.

Practice 3 **Software created by a government organization should be treated as potentially constituting a record for purposes of the *Acts*.**

A software program is an essential tool for the creation, organization and storage of records. Information or data cannot ordinarily be retrieved without the application of a software program. Viewed from this perspective, a software program may form an integral part of a record. In some cases, the organization itself may have produced the software and, as a result, the information may only be accessible through the use of this particular software. In many cases as well, where using commercial software, the record cannot be accessed in its original form without use of the software through which it was created.

The question of whether software may be considered a record for the purposes of the *Acts* has not been extensively adjudicated, though the issue has been raised indirectly in one order.

(See, Appendix A, Note 4) The *Acts* and regulations also envisage the creation of a record from a software program available to the organization. (For exceptions under the *Acts*' regulations, see Appendix A, Note 13)

It should also be noted that, based on proposals being advanced in the United States, a software program developed by a government organization (as distinct from a commercially acquired, off the shelf program) would be considered a record for purposes of the freedom of information legislation. (See Appendix A, Note 5)

Practice 4. Data and records viewed on-line and not subsequently stored on an individual workstation or database, are generally not considered a record for purposes of the *Acts*.

A government organization may subscribe to an external commercial on-line e-mail service or bulletin board, or may be connected to a wide-area network, such as the Internet. In these cases, individuals will often view electronic documents, publications and other materials on-line with no permanent record of the information being kept by the institution. While this issue has not been specifically adjudicated under the *Acts*, the approach adopted in the United States is that information, text or data viewed on-line (but not down loaded and stored) is not a record for purposes of its legislation. If, on the other hand, the information or data was copied and stored either in an electronic version or as a hardcopy printout, then it should be considered a record. (See Appendix A, Note 10)

Anticipating Future Access Requirements

Practice 5. A good strategy for management of electronic records starts with a review of an organization's functions and business processes to determine what records need to be created and retained, and a review of existing records management practices to determine their continuing effectiveness.

After an organization determines that the management of its electronic records should be reviewed, a good strategy would start with an analysis of the organization's functions and business processes. Such an analysis would seek to determine whether the records that are being created do in fact document these activities accurately and completely. In preparing the analysis, it may be useful to consider the following points:

- The creation of an inter-disciplinary team consisting of systems specialists, archivists, record managers and program managers probably represents the most effective way to undertake this type of investigation and to later develop a workable records management strategy, and then to develop workable program documentation and records management strategies.
- Any review should consider the proper management of all forms of records irrespective of the way in which they are stored, such as electronically, on paper, on microfilm, etc.

- In determining what records need to be created and retained, public organizations should take into account various laws and practices that require documentation for accountability purposes, or as evidence of decisions taken. The *Acts* should be included as part of this review.

Practice 6. Once a need to change existing records management practices has been identified, available options for managing the system should be considered.

In particular, serious consideration should be given to integrating the management of paper and electronic records. An integrated electronic and paper system would entail ensuring that records in paper and electronic form were carried over to the electronic filing system. There are increasingly powerful records management and document management systems that can assist in their integration.

Practice 7. Government organizations should take records management considerations into account when designing information systems and when planning for upgrades to existing systems.

When organizations consider designing and/or upgrading information systems or software applications, they should carefully consider their ongoing records management needs. These include ensuring the ongoing accessibility of information and its prompt disposal when no longer required. Unless records management needs are specifically addressed, it is unlikely that they will be incorporated effectively into the new system.

Practice 8. Prior to acquiring new information technology*, government organizations should ensure that technical or other solutions are in place to support easy, ongoing access to records placed on a system and ready conversion to other convenient formats, as required.

As government organizations increasingly acquire more sophisticated information technologies, they will be faced with choices about the kind of hardware and software to obtain. Government organizations should incorporate in their analysis of options the access and retention capabilities of the technology they intend to acquire. The technology, whether hardware or software, should be capable of providing easy storage and retrieval of information and data.

Access could be thwarted, for example, if a particular software program does not permit information to be transferred to a new or different systems application or media format. In many instances, utility programs exist that can make this conversion (for example, from a particular word processing format to another text format governed by Standard Generalized Markup Language).

* The term information technology is used broadly to include computers and telecommunications devices that allow for local area and wide area networks, as well as any other machine readable technology that processes information or data.

Practice 9. Government organizations should include in their information technology planning, a strategy for preserving information, data or text for extended periods of time.

It has been recognized that one of the disadvantages of electronic records is that they are stored in media - usually magnetic tapes or disks - that deteriorate over time, in some cases in just a few years. While no new technology has yet been created to fully rectify this problem, steps can be taken to ensure that the information, data or text that these records hold is preserved for longer periods of time. That is, they need to be retrievable and usable over the information's 'life cycle' from creation to final disposition. The use of CD-ROM technology may provide greater capability. The important point is to periodically migrate electronic records to new tapes or disks before decomposition sets in, or, if appropriate, to new technologies.

The need to ensure that records can be transferred to other media and software applications has already been discussed. Given rapid technological obsolescence, this consideration has particular urgency for records having long term value. Moreover, some electronic records have archival value. Where they will eventually be transferred to the Archives of Ontario, an agreement should be developed with the Archives regarding the medium of format in which they will be transferred.

Practice 10. The quality of electronic records can be enhanced if "contextual" information that allows the original purpose or context of a record to be determined becomes part of the records management system.

For an electronic record to be of use as evidence of decisions taken, or transactions made, it must contain certain elements that make the document understandable to someone who did not originally create the record. In a paper context, a record would ordinarily include details that placed the content of the document in a particular context, e.g., letterhead, addresses and titles, etc.

Such a record would also be filed according to some system of record keeping, which would indicate that the document had been produced by a certain person in a certain department of the organization. It should also be filed with other related documents that allow the larger context in which the record was created to be understood (for example, the issue which prompted a particular memo or e-mail message to be written).

In an electronic environment, a record may consist only of its text or data contents without its author being identified. The information is often key to preserving the record's value as *evidence*, whether for legal or more standard operational reasons. In addition, other important contextual information may be absent, including (a) the date and time when the record was created, (b) its origins within the organization, (c) the person or persons to which it may have been sent, and (d) the date and time when it was sent. In some cases it may not be evident *why* a record was created. Or documentation may be lacking which permits the integrity and completeness of

records stored on a database to be assessed. Finally, the record may exist in a number of different locations and may not be filed according to a system that places the record and related records in distinct files and file series following a recognized classification system that permits ready location of required records later.

The key information would include: information about the agency and the persons who created it, the time, place and reasons for its creation, and its relationship with other records.

In addition, to ensure that a record may be retrieved later (and in a manner which retains its evidentiary character), it may be necessary to preserve the software that was used to create it, as well as important information on the technical characteristics of the storage media and system and any guides or protocols that describe and control how records were filed as data on the system or its storage media. Otherwise, the record may need to be transferred to another storage medium that best preserves its accessibility and evidential value.

Government organizations should also consider mechanisms to ensure that records that reflect a final position, decision, or transaction are made tamper-proof. Restrictions should be placed on the persons who are able to alter, change or delete the record. Often, a number of copies of the same record may exist. To avoid any confusion, organizations should find a way to identify the authoritative version.

Finally, it is important to e-mail messages, attachments and other transferred files to be integrated into and stored in the organization's record keeping system. (See Practice 6)

Practice 11. Information systems managers should determine uniform protocols for storing electronic records in consultation or collaboration with records managers so that such information can be easily retrieved as required. All documentation about the system should be retained for easy access.

Government organizations should develop and adhere to standard methods of identifying and storing information, data and text, that will ensure that they can be easily stored and retrieved. This will mean developing systems documentation and data management protocols. It may also include development of file classification plans for paper and electronic records by records management specialists.

Retaining Electronic Records

Practice 12. Records in all media, including electronic media, should not be destroyed without appropriate official authorization.

Before the advent of information technology, a record was typically thought of as a piece of paper that proceeded through a defined and predictable life cycle. It was created and used, filed and then destroyed, or, if of long-term value, given to the organization's archives. Today, however, the record is often not a piece of paper, but information recorded by the use of a computer. Erasable immediately after it is created, the information exists in electronic form in the memory of a computer and becomes material (hard copy) only when a printout is made.

For the *Acts* to operate, and for the public to be provided with an opportunity to request the information in question, the record must be retained so that it can be retrieved.

Those who work with various information technologies invariably make decisions about whether to retain information at the moment that it is either created or received. Thus, for example, an e-mail message relating to the mandate or function of the organization is sent, and once read, the message is often deleted by users. This may occur because technical or operational procedures for retaining and storing e-mail or other computer-generated information have not been adopted. The record, in any event, is not saved.

While few laws obligate institutions to create records, once created, such records are subject to various laws, including the *Archives Act* and the provincial and municipal *Acts*. The former stipulates that records of the provincial government cannot be destroyed or permanently removed from government custody without the approval of the Archivist of Ontario. In addition, under the regulations to the *Acts*, government institutions are required not to inadvertently destroy records. The *Archives Act* and the *Acts* complement each other in this respect, although the former applies only to the records of the *provincial* government. Other provincial legislation may also designate a legal retention period for certain records. (See Appendix A, Notes 6 and 7)

At the same time, reference should be made to provisions in the *Acts* and regulations that deal with the preservation of personal information. (See Appendix A, Note 8)

In requiring that records not be destroyed without proper approval, the legislation recognizes that those who work and make decisions in the public interest must be accountable for their actions and decisions. The saving of records is an essential component of accountability.

At the provincial level, a policy on retaining official records of the Government of Ontario has been adopted and is found in Management Board Directive 7-5," Management of Recorded Information." This Directive is supplemented by the Archives of Ontario Recorded Information

Management bulletins and fact sheets, which provide advice on how official records, including electronic records, should be maintained, controlled and described in a way that allows them to be efficiently accessed, retrieved and interpreted. The Directive states that program managers are responsible for the records in their care.

This Directive applies to all recorded information created or commissioned by the institutions of the Ontario Government (all ministries and Schedule I agencies). The reports of consultants are included in this policy, as is recorded information acquired from other governments, government organizations, and individuals and organizations in the private sector. In the context of electronic records, official e-mail messages must be retained, as well as messages received from individuals or organizations posted on electronic bulletin boards, if the substance of the messages deals with the functions or mandate of the organization.

The exceptions to this general rule, established in the directive, allow for the destruction of duplicate records that have been produced for convenience or reference; as well as publications such as books, journals etc. which are part of an institution's library holdings, or are intended to be part of a library. Duplicate stocks of publications, printed literature or blank forms can also be destroyed. (See Appendix A, Note 9)

Regarding electronic records, the Directive's principle that temporary working papers, such as rough notes or informal drafts, that have no value in documenting the evolution or implementation of government policy or programs can also be destroyed must be considered very carefully. Since a great deal of what constitutes policy making and program implementation now takes place through the medium of networked computers, care should be exercised to ensure that all electronic records are not viewed as only being rough notes or informal drafts.

Practice 13. When new software or hardware is introduced, organizations should use their best efforts to convert their active stored information, data and text to the new systems or retain ability to access.

Another aspect of retaining electronically created records is maintaining and modifying the software systems documentation and other data management tools in order that information, data or text can be easily retrieved at some later date. This is particularly important since information technology changes so rapidly. This requires that institutions regularly purchase new hardware and upgrade existing software programs. Unless the stored data or information which has long term value is converted to the new systems, it may become very difficult if not impossible to obtain access to that data stored under older technology. Over time, the development of 'open systems' and standards will help as more information and data will be accessible without complex conversion.

Practice 14. Government organizations should integrate electronic records into their record retention scheduling process.

When paper records were the norm, the question of what records to keep or destroy was usually made some time after the documents were created. In this respect, retention schedules were developed to indicate how long records were to be maintained by the particular department before they were destroyed or transferred to a records centre and archives.

Schedules should similarly be developed for electronic records. Early on in the development of electronic information systems, each department of the organization should determine the retention period for related groups of e-mail messages, reports, database files etc. and see that they are scheduled. This approach will help ensure that electronic records are kept as long as they are needed and that the permanent portions of electronic records can be selected and preserved by archives. Each department of the organization should determine the retention period for e-mail messages, reports, database files, etc. This approach will help to ensure that the permanent portions of electronic records can be selected and preserved more easily. (See Appendix A, Note 11)

Security Issues

Practice 15. The vulnerability of electronic records to a variety of security breaches needs to be addressed through appropriate security procedures.

Without proper precautions, electronic records are vulnerable to unauthorized access and tampering. Among the strategies which organizations can apply to minimize the chance of a security breach are the following:

- Levels of security and authorized access can be formalized for the organization through the use of passwords and sign-on identifiers.
- Confidential information can be encrypted when stored or transmitted.

Records should also be secured from system failures and physical disasters. Therefore:

- An appropriate back-up system will be required.
- A disaster recovery plan needs to be devised.

Providing Access to Electronic Records

Practice 16. Whenever feasible, government organizations should provide individuals with the electronic records that they seek in the format requested.

When a request for access to a record is made under the *Acts*, the government organization will ordinarily provide a paper copy of the record, or give the requester the opportunity to view the original. Where the request is for an electronic record, there may be a variety of ways that the request can be fulfilled, depending on what the requester wants and the capabilities of the technology in use by the institution.

Where the information is stored in a video or audio tape, the organization could provide a copy of the tape, if such is the request, or give the requester the opportunity to listen to or view the tape. Ordinarily, to provide a copy of an audio or video tape is neither time-consuming, nor unduly expensive. (See Appendix A, note 12)

With the increasing use of various forms of information technology, it is often practical to provide access to an electronic record in the format requested. Thus, an institution may hold requested information in a database that is accessible by means of a commercially available software package. The requester could ask that the information be copied to a disk or diskette. A request of this kind neither entails difficult procedures nor a lot of time and should be responded to routinely.

Practice 17. Government organizations should attempt to modify their software in order to provide access to a requested electronic record where it is reasonable to do so. Organizations should be flexible in determining what is reasonable.

Electronic records may not exist in paper form. A record could be data or text assembled in a particular way through the use of a software program. A discrete record or file may not exist, but could be created with the assistance of software or technical knowledge available to the government organization.

The *Acts* and regulations recognize the obligation of government organizations to create electronic records when requested, except where to do so would unreasonably interfere with the operations of the government organization. That obligation would be satisfied through the use of the appropriate hardware and software to create the document. (See Appendix A, Note 13)

Such a scenario would arise where a government database held "raw data" or statistics, and the government organization had a computer software program that allowed the data to be manipulated in a variety of ways for its purposes. A request could be made for the data to be assembled in a way not anticipated by the organization. How should the organization respond?

The spirit and purpose of the *Acts* is to make government information available to the public. To keep to these principles, the organization should modify the software program as may be appropriate, provided that to do so would not unreasonably interfere with the organization's operations. Information technology has developed to the extent that relatively little time and effort is often required to make such modifications. A fee for such a service would be applicable pursuant to the schedule set out in the regulations to the *Acts*.

Less problematic are requests for access to video or audio tapes, microfilm, and microfiche. More challenging is a request for access to a record on-line, that is, where the institution has, for example, created a database comprising discrete pieces of information, and the requester would like to have direct access to that database through his home or work computer.

Some government organizations are placing certain files on the Internet, thereby allowing individuals to access that information if they have a modem attached to their home computer. This development is still in its infancy, but potentially could lead to direct on-line access to government information.

Routine Disclosure/Active Dissemination

Practice 18. Electronic records, like other records, which contain information of general interest should be routinely disclosed and distributed to the public.

Some government information is now provided through information kiosks at various public locations in Ontario. In addition, the Government of Ontario and a number of municipal institutions now disseminate information through their websites.

As the acquisition of information technology by governments and the public becomes more widespread, access to government information will come to include access by electronic means. When government organizations proactively seize the opportunity to provide public access to electronic records, the public can obtain information it seeks without having to visit a government office.

Principles to follow when adopting this approach are found in *Routine Disclosure/Active Dissemination (RD/AD)*: A Joint Project of the Office of the Information and Privacy Commissioner/Ontario and the Freedom of Information and Privacy Branch, Management Board Secretariat (April 1994) and *Enhancing Access to Information: RD/AD Success Stories* (April 1996).

Conclusion

The *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* were conceived at a time when the full impact of information technology on the operations of government organizations was yet to be felt. Government organizations today are experiencing a transition period, as more and more of their operations become computerized, and as the way they do business increasingly involves the creation of electronic records. While this information technology assists in the delivery of programs and services to the public, it has presented government managers with many new challenges. One of these is, how to make the *Acts* work effectively in a electronic record world.

Information is a resource. The *Acts* are two of the tools which can provide access to that resource. However, the *Acts* can only work effectively and have value if records, including electronic records, are well managed by government organizations.

Electronic records management may be a new issue for many organizations. Helpful advice on this subject can often be obtained from records managers, information technology systems personnel, or staff of the Ontario Archives, where the organization is part of the Government of Ontario.

Appendix A

Note 1. Section 2(1) of the *Freedom of Information and Protection of Privacy Act* and section 2(1) of the *Municipal Freedom of Information and Protection of Privacy Act*) provide:

> 'record' means any record of information however recorded, whether in printed form, on film, *by electronic means* or otherwise, and includes,
>
> (a) correspondence, a memorandum, a book, a plan, a map, a drawing, a diagram, a pictorial or graphic work, a photograph, a film, a microfilm, a sound recording, a videotape, *a machine readable record* any other documentary material, regardless of physical form or characteristics, and any copy thereof; and
>
> (b) subject to the regulations, *any record that is capable of being produced from a machine readable record under the control of an institution by means of computer hardware and software or any other information storage equipment and technical expertise normally used by the institution.* [Emphasis is added]

Note 2. Management Board Directive 7-5, *Management of Recorded Information* defines recorded information as follows:

> Recorded information includes, but is not limited to, the information contained in any record, such as correspondence, memoranda, publications, reports, forms, plans, drawings, maps, pictorial or graphic works, photographs, films, microform records (such as microfiche and microfilm), *sound recordings, videotapes, electronic and all other machine readable records, and any record which has been produced from a machine readable record by means of computer hardware and software and any other information storage equipment and technical expertise*. [Emphasis is added]

Note 3. Archives of Ontario. RIM Fact Sheet #7. Electronic Records: What About E-Mail?

> An e-mail message constitutes an official record when the document is made or received in connection with the transaction of government business.

Note 4. Order P-1281 discusses software as an electronic record under the provincial *Act*.

Note 5. U.S. Department of Justice, Office of Information and Privacy, *Proposed Electronic Record FOIA Principles*, 1994.

> 32. Software that is generated totally at government expense, and in which there exists no private proprietary interest should be subject to the Act and disclosed if not covered by a FOIA [U.S. Freedom of Information Act] exemption.... Such software should be made available at direct cost under the FOIA absent any specific authorization by Congress for charging of a greater fee.

Note 6. Section 6 of the *Archives Act*.

> Subject to the regulations, no official document, paper, pamphlet or report in the possession of any ministry or branch of the public service or of the Assembly shall be destroyed or permanently removed without the knowledge and concurrence of the Archivist.

Note 7. Section 4(3) of Ontario Regulation 460, made under the *Freedom of Information and Protection of Privacy Act*, and section 3(3) of Ontario Regulation 823, made under the *Municipal Freedom of Information and the Protection of Privacy Act*, provide:

> Every head shall ensure that reasonable measures to protect the records in his or her institution from *inadvertent destruction* or damage are defined, documented and put in place, taking into account the nature of the records to be protected." [Emphasis is added]

Note 8. Section 5(1) of Ontario Regulation 460, made under the *Freedom of Information and Protection of Privacy Act*, and section 5 of Ontario Regulation 823, made under the *Municipal Freedom of Information and the Protection of Privacy Act*, provide:

> Personal information that has been used by an institution shall be retained by the institution for at least one year after use unless the individual to whom the information relates consents to its earlier disposal.

Note 9. Management Board Directive 7-5, *Management of Recorded Information*.

> This Directive applies to all recorded information created or commissioned by the Ontario government, regardless of medium of storage, or acquired from other governments, government organizations and individuals and organizations in the private sector.

The Directive does not apply to information contained in the following:

- duplicate copies preserved within the same medium of storage and retained solely for convenience, reference, or future dissemination;
- publications (such as books, journals, and published reports) which constitute part of a library's regular catalogued holdings;
- duplicate stocks of publications, printed literature or blank forms;
- temporary working papers such as rough notes or informal drafts when of no value in documenting the evolution or implementation of government policy or programs.

The Directive also does not apply to the specialized data management functions associated with planning, developing, and operating computerized information systems *except for specific aspects of such functions affecting the following*:

- the scheduling of computerized or other recorded information;
- the retention or disposal of computerized or other recorded information;
- the acquisition, preservation and retrieval and interpretation of archival information by the Archives of Ontario;
- the ability to locate information within ministries, agencies and individual information systems, records series, or other such discrete bodies of information. [Emphasis is added]

Note 10. U.S. Department of Justice, Office of Information and Privacy, *Proposed Electronic Record FOIA Principles*, 1994.

16. Information or data maintained outside of the government that is accessed electronically by an agency [government organization], but merely viewed by agency employees, should not be deemed to come into the agency's possession and control by virtue of such electronic access.

17. Any such data that is retrieved into an agency database by an agency employee or agent, or is printed out in paper form, becomes subject to the Act [U.S. Freedom of Information Act].

Note 11. The Archives of Ontario, RIM Fact Sheet # 2, Scheduling: The Foundation of RIM Policy.

> A schedule is a binding agreement which tells you how long records are kept and whether they are eventually transferred to the Archives of Ontario.

Note 12. Order P-840

> The appellant requested access to audio tape recordings. The institution denied the request on the grounds that copying the tapes would be unduly expensive. The order upheld the appellant's request to receive the tapes, since reproducing them would not be unduly expensive.

Note 13. Section 2 of Ontario Regulation 460, made under the *Freedom of Information and Protection of Privacy Act*, and section 1 of Ontario Regulation 823, made under the *Municipal Freedom of Information and Protection of Privacy Act*, provide:

> A record capable of being produced from machine readable records is not included in the definition of a 'record' for the purposes of the Act if the process of producing it would unreasonably interfere with the operations of an institution.

Appendix B

Australian Archives, *Keeping Electronic Records: Policy for Electronic Record keeping in the Commonwealth Government*, 1995. www.aa.gov.au/AA_WWWAA_Issues/KER/KeepingER.html.

Australian Archives, *Guidelines for Managing Electronic Records in Australian Government Agencies*, 1995. www.aa.gov.auAA_WWW/AA_Issues/ManagingER.html.

Ontario, Management Board of Cabinet, Directive 7-5, *Management of Recorded Information*.

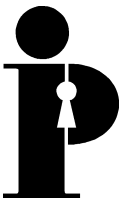
National Archives of Canada, *Managing Electronic Records in an Electronic Work Environment*. May 1996.

National Archives of Canada, *Record Keeping in the Electronic Work Environment*. May 1996.

Ontario, The *Freedom of Information and Protection of Privacy Act*.

Ontario, *Municipal Freedom of Information and Protection of Privacy Act*.

Ontario Archives, *Retention and Disposal of Recorded Information: Electronic Records — Special Issues.* Draft, 1996.



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