IPC
PERSPECTIVES
INFORMATION AND PRIVACY COMMISSIONER / ONTARIO

VOLUME 5
ISSUE 2
SPRING 1996

TOM WRIGHT, COMMISSIONER

Towards a Culture of Openness

How does a government organization respond to the increasing demands of the public? How does it make access to information better, quicker and cheaper in a time of shrinking financial resources? Eleven government organizations show how they meet the challenge in a recent paper jointly released by the Information and Privacy Commissioner/Ontario (IPC) and Management Board Secretariat (MBS).

Enhancing Access to Information: RD/AD Success Stories describes how these government organizations apply fresh approaches through routine disclosure and active dissemination (RD/AD).

Routine Disclosure and Active Dissemination are defined as follows:

Routine disclosure (RD): occurs when a request for a general record can be granted routinely either inside or outside of the formal access process prescribed by the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*.

Active dissemination (AD): occurs when information or records are periodically released (without any request) pursuant to a specific strategy for release of information.

RD/AD advances open government and makes access to government information easier and cheaper. How? *Enhancing Access to Information: RD/AD Success Stories* shows how eleven municipal and provincial government organizations in Ontario are currently working towards openness – with great success.

Each access "success story" is unique yet several common elements were identified in interviews which took place between July and November 1995. One of the most striking was the importance of a "positive access mind-set" or a "corporate-wide attitude of openness" within the organization. Another common characteristic was one of strong leadership – leadership that endorses positive and active ways to get information out to the public – leadership that dedicates the necessary staffing resources to develop RD/AD strategies and put them in place.

The paper also gives a list of practical ideas on how government organizations can make RD/AD a part of the day-to-day operations and help foster a culture of openness.

Here are some practical tips:

- Involve staff from all areas of the organization in developing an access strategy.

Helpful hint for protecting your personal medical files.

Obtain a copy of your medical file used by insurance underwriters by writing to the Medical Information Bureau (MIB). The Canadian address is 330 University Avenue, Suite 102, Toronto, Ontario M5G 1R7. Telephone: (416) 597-0590. The MIB is a data bank with medical information that is used by insurance underwriters to check medical histories.

Continued on Page 3

Assessing the Risk

…Directive 8-2 requires that a computer matching "assessment" be submitted to the IPC at least 45 days before the project begins.

COMPUTER MATCHING – CONSIDERING A COMPUTER matching project in your ministry or agency? If so, have you done your assessment?

What is computer matching, you ask? At its most basic, it involves the computerized comparison of two or more data bases of personal information that were originally collected for different purposes. The computer matching program creates or merges files on identifiable individuals regarding various matters of interest. For example, computer matching could identify people enrolled in a number of government programs who receive certain benefits.

Since computer matching can detect persons who may be intentionally defrauding the government, it may be used extensively for law enforcement purposes to identify suspects for a law enforcement investigation. It is evident that computer matching can be an important and beneficial tool for government organizations, however, the privacy concerns associated with such practices are also significant. Without adequate safeguards, computer matching could become an easy means of invading privacy.

Government organizations that are considering computer matching should be familiar with the Management Board Directive 8-2 and Guideline, *Enhancing Privacy: Computer Matching of Personal Information*. It applies to all ministries and agencies covered by the *Freedom of Information and Protection of Privacy Act* (the *Act*). Contact the Freedom of Information and Privacy Co-ordinator at your provincial organization for valuable assistance in this area.

Once a ministry or agency has the authority under the *Act* to collect, use or disclose personal information for the purpose of computer matching, Directive 8-2 requires that a computer matching "assessment" be submitted to the IPC at least 45 days before the project begins.

The IPC reviews and comments upon each computer matching assessment. The following requirements are mandatory:

- the names of the ministries, agencies or other organizations that will be involved;
- a description of the personal information records, including the number of records that will be matched and the date the match is expected to start and finish;
- the purpose of the computer match and the legal authority for the collection, use and disclosure of personal information required for the match, as well as a description of what will be done with its results;
- the steps to be taken to comply with the following requirements of the *Act*:
  - providing a notice of collection of personal information;
  - recording any non-routine use or disclosure of personal information as required by the *Act*;
  - ensuring that personal information used in the match will be kept secure, confidential and accurate;
- the procedures for notifying individuals who will be directly affected by any action resulting from the computer matching;
- the procedures for verifying any information the match produces; and
- the business case for the computer match.

Each computer matching assessment is reviewed by the IPC to ensure the directive has been followed, thereby balancing effective use of computerized personal information with the privacy interests of individuals.

The Freedom of Information and Privacy Co-ordinator at your provincial organization can be of valuable assistance to anyone considering a computer matching activity. For further information or policy advice, contact the Freedom of Information Branch at Management Board Secretariat; telephone (416) 327-2187.

FOIP at Queen's

CAN I MAKE AN FOI REQUEST FOR MY UNIVERSITY files? It's a frequently asked question. Although universities aren't covered by access and privacy legislation in Ontario, there's good news from Queen's University.

Recently, Queen's University took a giant FOI-step forward by developing its own access to information and protection of privacy guidelines. These guidelines were created to establish access to information and protection of privacy policies which reflect the underlying principles of Ontario's *Freedom of Information and Protection of Privacy Act*, and apply them in a manner appropriate to the University setting.

The guidelines are based on the following principles:

- as a general rule, information contained in University records should be available to members of the public;
- the necessary exemptions from the general principle favouring access should be as limited and specific as possible;
- the collection, retention, use and disclosure of "personal information" contained in University records should be regulated in a manner that will protect the privacy of individuals affected; and
- means should be established for the resolution of disputes concerning access to information and privacy protection matters.

Congratulations to Queen's University for showing leadership in this area! We hope their foresight serves as an example to others. For further information on Queen's access to information and protection of privacy policy and guidelines, contact Don Richan at (613) 545-2378.

Towards a Culture of Openness

CONTINUED FROM PAGE 1

- Study, examine and review FOI requests. Identify trends. Watch for patterns and identify records that can be routinely disclosed outside the formal FOI process.
- Be access conscious when designing forms. For example, where possible, design two-sided forms with disclosable information on one side and personal information on the other – makes for easy photocopying, without having to sever the personal information.
- Use training situations as an opportunity for staff to identify information that can be routinely disclosed or actively disseminated.
- Ongoing staff awareness, orientation, training and education are critical in demonstrating the benefits of RD/AD.
- Think about "partnering" with someone in another government organization to regularly share ideas and gain from each other's experience and expertise.

Ultimately, the most important benefit of RD/AD is that it generates a more open relationship between government organizations and the public they serve. For a copy of *Enhancing Access to Information: RD/AD Success Stories*, contact the IPC at (416) 326-3333 or 1-800-387-0073.

Privacy Profile

by Rob Candy, Freedom of Information and Privacy Co-ordinator, Region of Peel

The following article has been provided by the Region of Peel to assist other institutions in protecting personal information when delivering social services.

Under Ontario law, to establish eligibility for social assistance, sole support parents are required to pursue support for their dependent children from the absent parent. Often the whereabouts of the absent parent are unknown to the applicant. Municipalities use many methods to locate these absent parents, including driver's licence searches from the records of the Ontario Ministry of Transportation (MTO). Similar processes are in place to locate those past recipients of social assistance who are required to repay all or part of their assistance to the municipality, whether by reason of inaccurate or fraudulent declaration of information, or due to their having signed an assignment to repay the amount issued. In both cases (absent parents and required repayments), when municipal staff secure an address for an individual in question, attempts are made to establish contact, generally by mail.

When conducting these searches, it is crucial that staff confirm the identity of the individual prior to attempting contact. Insufficient screening processes could result in a letter, identifying Individual A, being sent to the address of Individual B. As names may be similar or even identical, there is a likelihood of the mail being opened by Individual B. This could mean inadvertent disclosure of personal information by the municipality (section 32 of the *Municipal Freedom of Information and Protection of Privacy Act*), as well as failure to ensure the accuracy of personal information before it is used (section 30).

To avoid such errors, systems should be established within each municipality to screen out inaccurate matches. In reviewing information received from MTO or other sources, staff should be trained to look beyond simple comparisons of first and last names and to review for corroborating matches on personal identifiers, including date of birth, sex, height and address history. Staff must know to look beyond the immediate and to obtain advice from supervisors or other experienced co-workers when in doubt.

Peel Region staff have developed procedures to ensure that personal identifiers are properly matched during address searches. They are as follows:

- The control clerk forwards the drivers' license search form to MTO
- MTO information is received back by the support clerk
- The support clerk matches the MTO information with the request for the search
- The support clerk highlights on both forms the areas of match, i.e. last name, first name, address history, date of birth. A minimum of two matches are required.
- If a match is determined, the support clerk writes a request on the file for the control clerk to change the address in the Comprehensive Income Maintenance System (CIMS)
- The control clerk receives the request and is responsible for ensuring that the information matches on at least two items (a second control measure)

Continued on Page 5

Updated brochures!

The IPC has updated its brochures and pocket guides to reflect the new fees for making an information request or appeal under the *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*. The publications include:

- *Access to Information Under Ontario's Information and Privacy Acts*
- *Your Privacy and Ontario's Information and Privacy Acts*
- *The Appeal Process and Ontario's Information and Privacy Commissioner*
- *Pocket Guides to the provincial and municipal Acts*

For copies, please contact the IPC at (416) 326-3333 or 1-800-387-0073.

Summaries

"Summaries" is a regular column highlighting significant orders and privacy investigations.

Order P-1023

The Ministry of Health received a request for all draft and final reports of a quality assessment review of its Audit Branch (the Branch). The Ministry granted partial access to the nine records that were located. Access was denied to two versions of a draft appendix, pursuant to section 21(1) (invasion of privacy) of the *Freedom of Information and Protection of Privacy Act*.

It was the appellant's position that the requested records primarily describe the operational status of a unit within the Ministry. Any personal information contained in the record was incidental to the focus of the majority of the information contained in it. The Ministry submitted that although the records did not contain the name of any individual, it was reasonable to expect that the individual holding that position could be identified.

It was the IPC's view that while any audit of a government department would likely impact on the individuals working in that department, either favourably or unfavourably, in these situations, an employee could not expect to maintain complete anonymity with respect to the results of this kind of review.

The Ministry was ordered to disclose the information in the records, less some personal information that was not at issue in the appeal.

Investigation I95-030P

The complainant was a former College student. While at the College, he had been overheard threatening to kill anyone who tried to stop him from reaching his career goal. He apologized for this behaviour, but later wrote to a College instructor complaining that he was being harassed and discriminated against.

The complainant was also a patient at a psychiatric institute. After he had left the College, when he was reviewing his psychiatric file, he found a letter from the College to the institute requesting a "risk assessment" of his potential for violence. The complainant believed that the College's actions in obtaining the risk assessment breached the *Freedom of Information and Protection of Privacy Act* (the *Act*).

The IPC found that the College's collection of the complainant's personal information was not in compliance with any of the conditions set out in section 38(2) of the *Act*. The *Occupational Health and Safety Act* did not expressly authorize the collection of the risk assessment. The collection was not used for the purposes of "law enforcement." Although it was accepted that dealing with pending or existing litigation was a lawfully authorized activity, the IPC considered the risk assessment was not "necessary" to the proper administration of this activity.

The IPC recommended that the College take steps to ensure that personal information is not collected except in compliance with the *Act*.

All IPC orders, as well as investigations from June 1, 1993, are available from Publications Ontario at (416 326-5300 or 1-800-668-9938. Both orders and investigations are also available through the QUICKLAW database or on the IPC's World Wide Web site at http://www.ipc.on.ca.

Privacy Profile

CONTINUED FROM PAGE 4

- The control clerk creates a computer input sheet with the address change and inputs it into CIMS
- If any doubt exists about the matching process, a supervisor is consulted.

Following procedures such as these will assist municipalities to ensure privacy in the delivery of social assistance services. To find out more about Peel's procedures, contact Rob Candy, Freedom of Information and Privacy Co-ordinator, (905) 791-7800, ext. 4717.

Q&A

Q & A is a regular column featuring topical questions directed to the IPC.

Q: What is data sharing and what's the difference between data sharing and computer matching?

A: Data sharing is the exchanging, collecting or disclosing of personal information between two or more organizations. It involves personal information that has been collected indirectly, and used for a purpose which may not have been intended at the time of the original collection.

Data sharing happens when organizations share or compare personal information in any format. For example:

- a hand written list with another hand written list;
- a hand written list with a computer database; or
- a computer database with another computer database.

Computer matching is basically a sub-set of data sharing. It involves sharing of information from two or more electronic databases of information. The computer matching program merges files on individuals to identify specific areas and creates another electronic file.

Q: As a government organization, what are the obligations under the Acts *with regards to data sharing and computer matching?*

A: Both provincial and municipal government organizations should complete a data sharing agreement when considering any data sharing activity. The agreement clarifies the rights and obligations of all parties and helps to ensure compliance with the privacy provisions of the *Acts*. The IPC considers that any sharing of personal information should be supported by a written data sharing agreement.*

Also, provincial government organizations are required by Management Board Directive 8-2 to forward a computer assessment to the IPC at least 45 days prior to beginning any computer matching activity. [See *Assessing the Risk*, p. 2]

* For a copy of the *Model Data Sharing Agreement* or the *IPC Survey on Data Sharing in the Ontario Government*, contact the IPC at (416) 326-3333 or 1-800-387-0073. (Also see article in *IPC Perspectives*; Vol.4, Issue 3, Fall 1995)

Aussi disponible en français …

For a French version of this newsletter or other IPC publications, contact Enza at (416) 326-3953 or 1-800-387-0073.

Address changes?

Got an address change? We want to hear it! Please help us keep our mailing list up-to-date by calling with you revisions; Telephone (416) 326-3953 or 1-800-387-0073. Just ask for Enza.

IPC
PERSPECTIVES
is published by the Office of the Information and Privacy Commissioner.

If you have any comments regarding this newsletter, wish to advise of a change of address, or be added to the mailing list, contact:

Communications Department
Information and Privacy Commissioner/Ontario
80 Bloor Street West, Suite 1700
Toronto, Ontario M5S 2V1
Telephone: (416) 326-3333 • 1-800-387-0073
Facsimile: (416) 325-9195
TTY (Teletypewriter): (416) 325-7539
Web site: http://www.ipc.on.ca
Cette publication, intitulée «Perspectives», est également disponible en français.

55% recycled paper, including 10% post-consumer fibre

ISSN 1188-2999