Information
and Privacy
Commissioner/
Ontario

What to do if a privacy breach occurs:

Guidelines for government organizations

Ann Cavoukian, Ph.D.
Commissioner
May 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

This publication is also available on the IPC website.

Table of Contents

What is a privacy breach?

The *Freedom of Information and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act* (the *Acts*) establish rules for government organizations to follow to ensure the protection of individual privacy. The *Acts* govern the collection, retention, use, disclosure and security of personal information (sections 37–46 of the provincial *Act* and 27–35 of the municipal *Act*).

A privacy breach occurs when personal information is collected, retained, used or disclosed in ways that are not in accordance with the provisions of the *Acts*. Among the most common breaches of personal privacy is the unauthorized disclosure of personal information, contrary to section 42 of the provincial *Act* or section 32 of the municipal *Act*. For example, personal information may be lost (a file is misplaced within an institution), stolen (laptop computers are a prime example) or inadvertently disclosed through human error (a letter addressed to person A is actually mailed to person B).

If an individual believes that a provincial or municipal government organization has failed to comply with one or more of the privacy protection provisions of the *Acts*, and that his or her privacy has been compromised as a result, the individual can file a complaint with the Information and Privacy Commissioner/Ontario (IPC). As well, upon learning of a possible privacy breach, the IPC may itself initiate a complaint in the absence of an individual complainant.

The purpose of the IPC complaint investigation is future-oriented – that is, should it be established that there was a privacy breach, the IPC will make recommendations that assist the institution in taking whatever remedial steps are necessary to prevent future similar occurrences.

Guidelines on what government organizations should do

Upon learning of a privacy breach, immediate action should be taken. Many of the following guidelines need to be carried out simultaneously or in quick succession.

When faced with a potential breach of privacy, the first two priorities are:

Containment: Identify the scope of the potential breach and take steps to contain it:

- retrieve the hard copies of any personal information that has been disclosed;
- ensure that no copies of the personal information have been made or retained by the individual who was not authorized to receive the information and obtain the individual's contact information in the event that follow-up is required; and
- determine whether the privacy breach would allow unauthorized access to any other personal information (e.g., an electronic information system) and take whatever necessary steps are appropriate (e.g., change passwords, identification numbers and/or temporarily shut down a system).

Notification: Identify those individuals whose privacy was breached and, barring exceptional circumstances, notify those individuals accordingly:

- notify the individuals whose privacy was breached, by telephone or in writing;
- provide details of the extent of the breach and the specifics of the personal information at issue; and
- advise of the steps that have been taken to address the breach, both immediate and long-term.

Additional steps:

- ensure appropriate staff within your organization are immediately notified of the breach, including the Freedom of Information and Privacy Co-ordinator, the head and/or delegate;
- inform the IPC registrar of the privacy breach and work together constructively with IPC staff;

- conduct an internal investigation into the matter, linked to the IPC's investigation. The objectives of the investigation are to: 1) ensure the immediate requirements of containment and notification have been addressed; 2) review the circumstances surrounding the breach; and 3) review the adequacy of existing policies and procedures in protecting personal information;

- address the situation on a systemic basis. In some cases, program-wide or institution-wide procedures may warrant review (e.g., a misdirected fax transmission);

- advise the IPC of your findings and work together to make any necessary changes; and

- ensure staff are appropriately educated and trained with respect to compliance with the privacy protection provisions of the *Act*.

What happens when the IPC investigates a privacy complaint?

When investigating a privacy complaint, the IPC will, depending on the circumstances:

- ensure any issues surrounding containment and notification have been addressed by the organization;
- discuss the complaint with the parties and obtain any relevant evidence;
- interview individuals involved with the privacy breach or individuals who can provide information about a process;
- obtain and review the organization's position on the privacy complaint;
- ask for a status report of any actions taken by the organization;
- review a copy of the personal information at issue;
- research IPC precedents;
- discuss settlement options;
- provide input and advice on current applicable policies and procedures and any other relevant documents and recommend changes; and
- issue a report at the conclusion of the investigation.

What steps can you take to avoid a privacy breach?

Government organizations governed by the *Acts* would be well served by adopting proactive measures to prevent a privacy breach from occurring. These measures should include:

- educating staff about the privacy rules governing the collection, retention, use and disclosure of personal information set out in Part III of the provincial *Act* and Part II of the municipal *Act*;
- educating staff about the regulations under the *Acts* governing the safe and secure disposal of personal information and the security of records;
- ensuring policies and procedures are in place that comply with the privacy protection provisions of the *Acts* and that staff are properly trained in this respect;
- conducting a privacy impact assessment (PIA), where appropriate. The PIA is a process that helps determine whether new technologies, information systems and proposed programs or policies meet basic privacy requirements;
- when in doubt, obtaining advice from your organization's legal department and Freedom of Information Co-ordinator. Management Board Secretariat's Corporate Information and Privacy Office is also a useful resource for Co-ordinators; and
- consulting with the IPC's Policy and Compliance Department in appropriate situations.

IPC website

The IPC has published a number of documents that can assist organizations in avoiding a privacy breach. These documents can be found in the **Publications and Presentations** section of the IPC's website (www.ipc.on.ca).

The following publications offer guidelines and best practices for protecting privacy:

- *Guidelines on Facsimile Transmission Security*;
- *Guidelines for Protecting the Privacy and Confidentiality of Personal Information When Working Outside the Office*;
- *Moving Information: Privacy & Security Guidelines*;
- *E-mail Encryption Made Simple*;
- *Best Practices for Protecting Individual Privacy in Conducting Survey Research*;
- Indirect Collection Guidelines (provincial and municipal versions);
- *Model Data Sharing Agreement*; and
- *A Model Access and Privacy Agreement*.

The following *IPC Practices* also contain guidance and practical suggestions on how government organizations can protect privacy:

- *Copying Information to Individuals Inside and Outside an Institution* (Number 2);
- *Providing Notice of Collection* (Number 8);
- *Video Surveillance: The Privacy Implications* (Number 10);
- *Audits and the Collection of Personal Information* (Number 11);
- *The Indirect Collection of Personal Information* (Number 14);
- *Maintaining the Confidentiality of Requesters and Privacy Complainants* (Number 16);
- *How to Protect Personal Information in the Custody of a Third Party* (Number 18);
- *Tips on Protecting Privacy* (Number 19); and
- *Safe and Secure Disposal Procedures for Municipal Institutions* (Number 26).

Privacy Complaint Reports that are publicly available are accessible through the IPC's website. They may be located via the Subject/Section Indices or by using the search function. Information about the IPC's privacy complaint process can be found in the **About Us – How Things Work** section of the website.