A Privacy Breach Has Occurred — What Happens Next?

A presentation by staff of the Information and Privacy Commissioner of Ontario

Information and Privacy Commissioner of Ontario

Friday, September 14, 2001

10:30 a.m.

Presented by staff of the Information and Privacy Commissioner of Ontario:

Colin Bhattacharjee
Project Analyst

Enza Ragone
Intake Analyst

Mona Wong
Mediator

Judith Hoffman
Project Analyst

Information and Privacy Commissioner of Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
CANADA
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

This presentation is also available on the IPC website.

Overview and Objectives

Part III of the *Freedom of Information and Protection of Privacy Act* (the provincial *Act*) and Part II of the *Municipal Freedom of Information and Protection of Privacy Act* (the municipal *Act*) govern the protection of personal information held by provincial and municipal institutions.

This session will:

- Provide guidelines which address what an institution should do once it learns of a possible privacy breach;
- Take you through the IPC Intake and Privacy Investigation process; and
- Provide some tips to help institutions avoid privacy complaints, with emphasis on the role of the IPC's Policy and Compliance Department.

This handout is available on the IPC Website at www.ipc.on.ca.

Part I: Learning of a Privacy Breach

Violations of personal privacy frequently involve the inappropriate disclosure of personal information, contrary to section 42 of the provincial *Act* or section 32 of the municipal *Act*. Such circumstances may result from the loss, theft or inadvertent disclosure of personal information.

An institution may learn that it has breached an individual's personal privacy either directly from the affected individual or from other parties, such as the media.

Once an institution learns that a possible privacy breach has occurred, immediate action should be taken. The following suggestions may assist in controlling the situation. (Many steps will have to be carried out simultaneously or in quick succession.)

Suggestions

- Identify the scope of the breach and take steps to contain the damage. (For example, this may involve retrieving hard copies of personal information that have been disclosed; determining whether the privacy breach would allow unauthorized access to an electronic information system; changing file identification numbers.).
- Ensure that appropriate institution staff is immediately notified of the breach, including the FOI Co-ordinator, the head and/or delegate.
- Immediately inform the IPC of the privacy breach.
- Notify individuals whose personal information has been disclosed.
- Conduct an internal investigation into the matter, report on the findings and quickly implement any recommendations. The objectives of this investigation should include: a review of the circumstances surrounding the event as well as 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, such as in the case of a misguided fax transmission. Are policies/procedures/staff training adequate across the board?
- Try to resolve a complainant's concerns informally, at the onset of the complaint.

Benefits

By adopting a measured strategy to address possible privacy breaches, institutions will be able to:

- Mitigate the damage by immediately preventing further inappropriate disclosures of personal information;
- Assure complainants and affected persons as well as the public, the media, and the IPC that the matter is being taken seriously; and
- Ensure that policies and procedures comply with the privacy protection provisions of the *Acts*, and that staff are properly trained in this respect.

Part 2: The Intake and Privacy Investigation Process at the IPC

For privacy complaints that reach the IPC, the following is an outline of the Intake and Privacy Investigation process:

The Intake Stage

When a privacy complaint is received, the Registrar assigns it to an Intake Analyst for:

- Screening out; or
- Conducting General Intake Functions.

Screening Out – 30 days

A complaint may be screened out of the process in accordance with certain criteria: (a) the matter is not, on its face, within the IPC's jurisdiction or (b) the IPC has jurisdiction, but the matter, on its face, is one that should not be moved forward. (For example, where the matter has been abandoned or decided before.)

If the privacy complaint file is not considered for screening out, it will be assigned to an Intake Analyst to conduct General Intake Functions.

General Intake Functions – 14 days

General Intake Functions include:

- Identifying the privacy issues
- Conducting research on IPC precedents that might be relevant to the complaint
- Contacting the complainant to: clarify the privacy issues; request any evidence to support the complaint; obtain consent to use his or her name when contacting the institution; explain IPC procedures and role; explain that once the IPC is satisfied with the result, even though he or she may not be, the file will be closed.
- Contacting the institution to: obtain its position and discuss the possibility of settlement
- Making recommendations to the Registrar where it is evident that the complaint should be processed in a particular stream

Streams

Where a file has not been screened out, and after completion of the General Intake stage, the Registrar will stream the file to the Intake Resolution Stream or the Investigation Stream.

Intake Resolution Stream – 45 days

The intention of this stream is to reach an informal resolution without making a finding. A complaint can be considered resolved in this stream if the IPC is satisfied with the outcome, even though the complainant may not be satisfied.

Files that lend themselves to this stream include those where it appears a straightforward and quick resolution can be achieved, or where an institution has acknowledged that the events occurred and is prepared to take steps to remedy the situation.

The file in this stream remains with an Intake Analyst for processing, who will:

- Promptly send an acknowledgement letter to the complainant
- Explain to the complainant that once the IPC is satisfied with the outcome, the complaint will not proceed further and the file will be closed
- Work with the institution to resolve the complaint

- Once resolved, send a closing letter to the complainant and institution outlining what was achieved and advising that the file has been closed.

- Proceed to close the file. **Reports issued in Intake Resolution are not made publicly available.**

Investigation Stream – 90 days

Where a file has not been screened out or closed in the Intake Resolution Stream, it will be placed in the Investigation Stream and assigned to a Mediator.

Most privacy complaints are brought to the attention of the IPC by individuals who have concerns regarding the collection, use, retention, disclosure and disposal of their personal information by an institution.

Investigation Stream – Process

- The Mediator will clarify the complaint and initiate settlement discussions with the parties.

- If the matter resolves, the Mediator will issue a Final Privacy Complaint Report (Final Report) outlining the settlement to the parties and the file will be closed. **Final Reports involving settlements are *not* made publicly available.**

- If the matter does not resolve, the Mediator will send a letter to the complainant and institution outlining the IPC's understanding of the complaint and the IPC process that will follow. The complainant will be asked for any additional information; the institution will be asked for its position on the complaint.

- The Mediator will review the institution's response, obtain whatever information is required in order to make any required findings, and prepare a Draft Privacy Complaint Report (Draft Report) outlining the findings. If recommendations are contemplated, the Mediator must obtain information on how they will impact on the institution prior to preparing a Draft Report.

- Once a Draft Report is issued, the parties are allowed 14 days to report factual errors and/or omissions contained in the Draft Report.

- Where no comments are received, a Final Report will be issued. If comments are received, they will be reviewed to determine if the Draft Report should be amended, necessary amendments will be made and the Final Report will be issued.

- **Final Reports of matters that do not settle are publicly available, with limited exceptions.**

- Complainants are not identified in Draft/Final Reports.

- If recommendations are made, the Mediator will follow up with the institution (usually three months after the date of the Final Report) regarding implementation of the recommendations.

- The Draft/Final Privacy Complaint Report contains a summary of the privacy complaint, a discussion of the information obtained, the conclusions and recommendations (if any).

The IPC also processes two other types of privacy complaints. They are Commissioner Initiated Privacy Complaints and High Profile Privacy Complaints.

A **Commissioner Initiated Privacy Complaint** is one where:

- A potential breach of privacy may have occurred, but none of the affected individuals have complained directly to the IPC;

- A potential breach of privacy has been brought to the attention of the IPC by a third party. A third party is not directly affected by the potential breach, and therefore cannot be identified as the complainant;

- The IPC may identify the need for a Commissioner Initiated Privacy Complaint (e.g. through items in the news media).

A **High Profile Privacy Complaint** is one where:

- The allegations of a breach are serious and central to the integrity of the *Acts*, often involving senior government officials and/or prominence in the media;

- The allegations of a breach have been brought to the attention of the IPC by external sources such as a member of the government (e.g. Cabinet Office asked the IPC to investigate when it was alleged that a Special Assistant to a Minister disclosed personal information to a reporter), a member of the public, or the media.

Investigation Stream – What to Expect

When investigating a privacy complaint, a Mediator will discuss the complaint with the parties, obtain and review the institution's position on the complainant's allegations, research IPC precedents, and discuss possible settlement options.

Depending on the circumstances, a Mediator may also:

- Ask the parties to provide any relevant evidence;
- Ask for a status report of any actions taken by the institution;
- Review a copy of the record(s) at issue;
- Ask the institution to retrieve any copies of records that have been inadvertently disclosed;
- Ask the institution to notify any individuals whose personal information has been disclosed;
- Review current applicable policies and procedures and any other relevant documents;
- Interview individuals involved with the potential privacy breach or individuals who can provide information about a process.

Part 3: Proactive Ways of Avoiding Privacy Breaches

General Tips

- The IPC's Intake and Privacy Investigation process usually takes place *after* a privacy breach has allegedly occurred.
- However, institutions governed by the *Acts* should adopt proactive measures to prevent privacy breaches from occurring in the first place. These should include:
    - Complying with 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*
    - Complying with the regulations under the *Acts* governing the safe and secure disposal of personal information and the security of records
    - Conducting privacy impact assessments (PIAs), where appropriate
    - Obtaining advice from your institution's legal department and FOI Co-ordinator. Management Board Secretariat's Information and Privacy Office is also a useful resource for Co-ordinators.

- Consulting with the IPC's Policy and Compliance Department in appropriate situations

The IPC's Policy and Compliance Department

- The functions of the IPC's Policy and Compliance Department include policy development, issues identification and management, and providing guidance to institutions governed by the *Acts* relating to the protection of privacy.

- Section 59(a) of the provincial *Act* allows the Commissioner to offer comment on the privacy protection implications of proposed legislative schemes or government programs. Similarly, under section 46(a) of the municipal *Act*, the Commissioner may offer comment on the privacy protection implications of the proposed programs of municipal institutions.

- Consequently, the Policy and Compliance Department encourages institutions to consult with us on:

  - Proposed legislation (statutes, regulations, by-laws) that may have privacy protection implications

  - Proposed programs or projects that raise novel privacy issues (e.g. the use of biometric technology)

  - Proposed programs that are potentially controversial from a privacy perspective (e.g. the use of video surveillance in public places, alternate service delivery)

- The Policy and Compliance Department also reviews applications from institutions that wish to engage in the indirect collection of personal information, and comments on computer matching proposals from provincial institutions:

  - **Indirect Collection** – Personal information must be collected directly from an individual except in a number of specific and limited circumstances set out in the *Acts*. The term "indirect collection" covers all occasions where an institution collects personal information from a source other than the individual concerned. The Commissioner has the power to authorize indirect collections of personal information by provincial and municipal institutions (section 59(c) of the provincial *Act* and 46(c) of the municipal *Act*). Consequently, unless the personal information may be collected from an individual under the specific and limited circumstances set out in the *Acts*, an institution must apply to the Commissioner for authorization to collect this information indirectly.

- **Computer Matching** – Management Board Directive 8-2 requires provincial institutions engaging in computer matching to prepare a Computer Matching Assessment and to provide the IPC with a copy of the Assessment 45 days before the institution is to start the computer matching activity. The Commissioner may provide an institution with comments on the proposed computer matching activity within the 45-day time period.

IPC Website

- The IPC has published a number of documents that can assist institutions in avoiding privacy breaches. These documents can be found in the *Publications and Presentations* and *Our Role - Guidelines and Documents* sections of the IPC's Website, which is located at www.ipc.on.ca

- Some of these 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
    - A Model Access and Privacy Agreement

- Several *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)
- 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.

Contacts

Brian Beamish
Director, Policy and Compliance
(416) 326-3906
bbeamish@ipc.on.ca

Colin Bhattacharjee
Project Analyst
(416) 326-3940
cbhattac@ipc.on.ca

Judith Hoffman
Project Analyst
(416) 325-9178
jhoffman@ipc.on.ca

You may also contact the IPC toll-free at 1-800-387-0073.

Information and Privacy
Commissioner of Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
CANADA
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca