INVESTIGATION REPORT

INVESTIGATIONS PC-000026-1 and PC-010009-1

MINISTRY OF THE ATTORNEY GENERAL

INTRODUCTION

This report deals with two privacy investigations involving the Ministry of the Attorney General (the Ministry). Both stem from incidents involving the disclosure of personal information as a consequence of computer theft. In both instances the police were notified of the theft, but neither computer has been recovered. Both investigations remain ongoing.

BACKGROUND

Privacy Investigation #1 - PC-000026-1

On August 4, 2000, the Office of the Information and Privacy Commissioner (the IPC) received a letter from a Director from one Division of the Ministry regarding the theft of a portable computer containing litigation documents. The letter stated:

> On Thursday August 3, 2000 a portable computer containing information related to litigation conducted by counsel from [the Ministry] was stolen. The computer was locked in the trunk of the lawyer's automobile and was removed while the vehicle was in an underground parking area. The police have been notified and I am advised that efforts are underway to recover this stolen property.
>
> As the data on the computer includes some personal information, [the Deputy Attorney General] requested that I notify you of this matter. Also, please be advised that office policies with respect to the security of portable computers are under review and all staff will be reminded of their obligation to secure personal information.
>
> ...

On the basis of this letter, the IPC initiated Privacy Investigation PC-000026-1, pursuant to the *Freedom of Information and Protection of Privacy Act* (the *Act*).

Privacy Investigation #2 - PC-010009-1

On February 21, 2001, the IPC received a letter from the Ministry's Assistant Deputy Attorney General, Criminal Law Division, which stated:

> On February 14, 2001, a laptop belonging to an Assistant Crown Attorney was stolen from the locked trunk of his car in Durham Region. It appears to have been stolen when he stopped at a Shopper's Drug Mart on his way home from work.
>
> I have been advised that there was personal information, and also information of a sensitive nature stored in the C drive of the computer. The computer was not password protected. There are inquiries being made regarding the extent to which

> the information was backed up so we can determine who ought to be notified of the incident.
> The Criminal Law Division is reviewing current practices regarding the transportation of files in an effort to enhance security measures. Crowns have recently been reminded not to leave laptops and files unattended.
>
> We will take immediate steps to ensure that all laptops in the Criminal Law Division are password protected in an effort to ensure that should such an unfortunate event occur in the future, the information stored on the computer would be inaccessible.
>
> ...

As a result, the IPC initiated Privacy Investigation, PC-010009-1 under the *Act*.

RESULTS OF THE INVESTIGATION

The first two priorities when faced with a potential disclosure of personal information are: (1) to identify the scope of the potential disclosure and take steps to contain it; and (2) to identify those individuals whose personal information may have been disclosed and, barring exceptional circumstances, to notify those individuals accordingly. Although the circumstances which lead to Privacy Investigations #1 and #2 were very similar in nature, the approach taken by the Ministry in addressing these two priorities differed significantly.

Privacy Investigation #1 - PC-000026-1

The Ministry initially advised the IPC that the stolen computer contained a very large number of documents relating to a specific litigation matter. No details were provided. The Ministry informed the IPC that the lawyer whose laptop was stolen was of the view that the only personal information contained in the electronic records stored on the computer consisted of the names and home telephone numbers of certain public servants.

On August 9, 2000, the Director who authored the August 4, 2000 letter to the IPC sent an e-mail to her staff advising them of the stolen laptop and reminding them to "take laptops directly home from the office" and to "ensure that access to documents stored on the laptop is password protected."

On August 28, 2000, the Ministry's Freedom of Information and Privacy Co-ordinator (the Co-ordinator) provided the Director with a copy of the IPC Practices entitled "Privacy and Confidentiality When Working Outside the Office" and asked her to distribute it to the staff of the branch.

The IPC advised the Ministry that it required more information in order to determine whether the actions taken by the Ministry adequately addressed basic privacy concerns. Specifically, the IPC asked the Ministry to provide more information concerning:

- the type of records at issue;
- the scope and type of personal information at issue; and
- the identity of the individuals whose personal information was contained in the records.

IPC staff offered to meet with the lawyer, but the Ministry declined. The Ministry provided a general description of the types of records at issue, but no further details concerning the particulars of the case or the individuals involved.

The Ministry subsequently explained that the records contained privileged information that could not be divulged to the IPC, but that some remedial steps had been taken by the Ministry to prevent similar incidents in future.

As an initial investigative step, the IPC decided to focus our efforts in the following two areas:

1. ensuring that all public servants whose personal information was included in the records had been notified by the Ministry; and

2. ensuring that a privacy expert from the Ministry personally reviewed the hard-copy version of each record contained on the stolen computer to confirm that no other personal information was contained in any of them.

The Ministry promptly confirmed that the notifications relating to the first item had been sent by the lawyer during the week of September 7, 2000.

As far as the second item was concerned, the Ministry took until December 22, 2000 to complete the review, almost 5 months after the theft of the computer had been reported. Further, although the review was apparently completed on December 22, 2000, the IPC was not advised of the results of the review until February 2, 2001. In response to persistent enquiries from the IPC, the Ministry finally confirmed that the review had been completed, and advised us for the first time at that point that additional personal information had been identified in the records. The Ministry informed the IPC that internal consultations were underway to address this situation.

On February 22, 2001, the Deputy Attorney General wrote to the Commissioner outlining a number of steps the Ministry had taken to prevent similar situations from arising in future, which are discussed later in this report. As far as the specific records at issue in Privacy Investigation #1 were concerned, the Ministry stated:

> ... during the week of September 2, 2000, the public servants whose personal information was included in the records were notified about the theft of the laptop and possible disclosure of their personal information. The Ministry will notify the remainder of individuals at the conclusion of the litigation when appropriate. Where possible, the Ministry will provide written notice by registered mail or courier service.

In response to receiving a draft copy of this Report, the Ministry modified this position to state that the remaining notifications would be made on a staged basis, depending on the nature of each individual's involvement in the litigation, and that all individuals identified in the documents would be notified by the conclusion of the litigation.

The Deputy Attorney General's February 22, 2001 letter went on to state:

> ... we cannot provide you with any other particulars because of the complexity and sensitivity of the case and concerns regarding solicitor-client privilege. I want to assure you that we will continue to follow our practice of involving your office in breaches of privacy. However, it is our considered opinion that, under the present legislation, which does not provide the Commissioner with clear protection against being compelled to release information, there may be cases such as this one where the Ministry will exercise discretion regarding the release of information to your office. These cases should be few and far between.

In response to the draft Report, the Ministry added:

> ... although in the ordinary course we would respond positively to any request on your part regarding disclosure, we remain concerned ... about the potential for your compellability. Therefore, we feel we are unable to provide you with a list of the names contained in the documents.

Consequently, the IPC has not been provided with sufficient information concerning the litigation, the types of records, the identity of the individuals and the type of personal information contained in the record to be in a position to be satisfied that the Ministry has responded appropriately to the disclosures.

Privacy Investigation #2 - PC-010009-1

The Ministry determined that the computer contained a phone list with the names, home addresses and phone numbers of Ministry staff working in the Durham office. These individuals were notified of the possible disclosure of their personal information on February 23, 2001.

The main computer security centre for the Ministry in North Bay was immediately notified to ensure that anyone trying to access any Ministry system remotely would be denied access, and the incident was flagged for further investigation.

The Ministry identified two other categories of personal information contained on records stored on the hard drive of the stolen computer.

1. Adult pre-trial memoranda

The adult pre-trial memorandum (the PTM) is a document routinely created by a crown attorney and used as a memory aid for the facts and issues of each case during the judicial pre-trials of those matters. Typically, a PTM would contain the following information: name of the accused, pre-trial ate, next court date, charges, name of the crown attorney, name of the defence attorney, name of the Justice dealing with the matter, facts of the case, charter/evidentiary/witness/disclosure issues, admissions, crown position, defence position, comments made by the judge, and any follow-up activity.

The Assistant Crown Attorney with carriage of the records contained on the stolen computer re-constructed its contents by going over the lists of cases he was involved in, retrieving the files, and locating the hard-copy of the PTMs he had prepared for these cases. He reviewed each of these documents and identified all individuals whose personal information was contained in them. The Ministry advised the IPC that it was not possible for the Assistant Crown Attorney to determine with certainty that all adult PTMs had been identified, but assured us that 90% of the PTMs had been located. The 10% difference was attributed to files where no hard-copies of the PTM were found in the file. The Assistant Crown Attorney explained that the absence of a hard-copy PMT did not necessarily mean that none had been created, however none was found despite search efforts by the Assistant Crown Attorney in the files and through other methods.

The Ministry advised the IPC that:

> Letters have been prepared and are currently being sent out to accused (through their counsel), victims and witnesses whose personal information was identified as having been on the hard drive.

The Ministry decided that notification was not appropriate with respect to one individual, for reasons explained to the IPC.

2. Young Offender pre-trial memoranda

The Assistant Crown Attorney provided the IPC with an affidavit stating that the computer contained PTMs concerning certain matters involving young offenders, and that, in his opinion, any such records fall within the scope of section 43 of the *Young Offenders Act*. The Ministry maintains that records of this nature are more appropriately dealt with under that legislation.

FINDINGS

Section 2(1) of the *Act* defines "personal information" as recorded information about an identifiable individual, including,

> ...
>
> (b) information relating to the education or the medical, psychiatric, psychological, criminal, or employment history of the individual or information relating to financial transactions in which the individual has been involved,
>
> ...
>
> (d) the address, telephone number, fingerprints or blood type of the individual,
>
> ...
>
> (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

Section 42 of the *Act* sets out a number of circumstances under which an institution may disclose personal information.

Privacy Investigation #1 - PC-000026-1

I find that the names and home telephone numbers of public servants constitute their personal information as defined in section 2(1), and that the disclosure of this information through the theft of the computer is clearly not permitted by section 42 of the *Act*.

Based on the limited information provided to the IPC by the Ministry, I am unable to independently determine that personal information of other individuals was also contained on the stolen computer. However, the Ministry has itself made this determination as a result of the review of hard-copy records conducted by the Co-ordinator. The disclosure of any such personal information through the theft of the computer is not permitted by section 42 of the *Act*.

Privacy Investigation #2 - PC-010009-1

I find that the names and information relating to the criminal history of an accused constitutes the personal information of these individuals as defined in section 2(1) of the *Act*. Similarly, I find that the names and statements made by victims and witnesses contained in the records constitutes their personal information. I also find that the names, home addresses and phone numbers of Ministry staff constitute their personal information under section 2(1). Consistent with my

finding relating to Privacy Investigation #1, I find that disclosure of this personal information through the theft of the computer is not permitted by section 42 of the *Act*.

In response to the draft copy of this Report sent to the Ministry, the Ministry takes the position that, because the computers were stolen, "there has not been an unauthorized 'disclosure' by [the Ministry] under s.42 of the *Act*." The Ministry states: "In our view, the *Act* contemplates intentional or wilful disclosures of personal information." Finally, the Ministry points out that even if a theft constitutes a "'disclosure,' there is no evidence that anyone had access to or learned of the information on the computer."

I do not accept the Ministry's position on this issue. Section 42 of the *Act* imposes a mandatory requirement on an institution not to "disclose personal information in its custody or under its control," except in the various permitted circumstances outlined in this section. The section does not limit the obligations on an institution to circumstances of "intentional or wilful disclosure" as suggested by the Ministry nor, in my view, is it reasonable to interpret section 42 in this restrictive manner. Clearly, none of the enumerated exceptions outlined in section 42 are present in the circumstances of Privacy Investigations #1 and #2 and, accordingly, the prohibition on disclosure imposed on the Ministry by section 42 of the *Act* applies, irrespective of whether the disclosure was unintended or done without any wilful motive, or whether the Ministry has knowledge that the personal information on the computers was accessed by anyone as a consequence of the thefts.

REMEDIAL STEPS TAKEN BY THE MINISTRY

The Ministry has undertaken a broadly scoped privacy review, which addresses policies and procedures for the handling of private and confidential material. The Ministry has developed a specific interim policy on transportation of confidential information which includes, among other things, the use and security of laptop computers. A copy of this interim policy was sent to all Ministry staff. A copy was also provided to the IPC for our review and comment.

The interim policy recommends that all information be stored on the Y-drive of laptop computers and that only documents currently being worked on can be stored on the C-drive. The Y-drive is a network drive and is only accessible at the office or remotely via modem. A limited number of Ministry staff are currently able to access the network remotely so it is necessary for them to transport a small number of documents on the C-drive if they are going to work off-site. As well, the policy requires all laptop computers to be password protected.

The IPC completed its review and provided comments on the interim policy to the Ministry. The Ministry has also been asked to provide input into a policy paper under development by the IPC entitled "Protecting the Privacy and Confidentiality of Personal Information When Working Outside the Office." The Ministry has undertaken to review its' interim policy to ensure that it is consistent with the direction and content of the IPC's policy paper.

The Ministry's Information Technology Security office is developing a security policy and an awareness program which would include the security of laptops and education to staff on how to prevent theft of their laptops.

RECOMMENDATIONS:

Privacy Investigation #1 - PC-000026-1

1. Advise the IPC of the types of records contained on the stolen computer, including the scope and type of personal information at issue and the identity of the individuals whose personal information was contained in the records.

2. Notify all individuals whose personal information is contained in the records, unless previously notified. If the Ministry feels that notification is not appropriate regarding any individual or specific item of personal information, the rationale for making this determination should be fully explained to the Commissioner's satisfaction.

Privacy Investigation #2 - PC-010009-1

1. Confirm that individuals whose personal information is contained in the records have been notified of the disclosure of their personal information, with the exception of the one individual identified by the Ministry.

Privacy Investigations #1 - PC-000026-1 and #2 - PC-010009-1

1. Confirm that the Ministry's interim policy on transportation of confidential information has been finalized and is consistent with the direction and content of the IPC policy paper. Provide a copy of the Ministry's final policy to the IPC.

2. Implement the Ministry's security policy and awareness program.

3. Instruct staff to purge laptop computers on a regular basis to ensure that they contain only information relating to ongoing and active work.

4. Consider supplementing the password-controlled access to laptop computers with other reasonable safeguards such as data encryption.

By September 27, 2001 the Ministry should provide the Office of the Information and Privacy Commissioner with proof of compliance with the above recommendations.

FINAL COMMENTS

In April 2000, I made a Special Report to the Legislative Assembly of Ontario on the Disclosure of Personal Information by the Province of Ontario Savings Office. It included an Addendum that identified obstacles the IPC encountered during the investigation of that matter, and pointed to the need for clarity regarding the powers and authorities provided to the Information and Privacy Commissioner in conducting privacy investigations. I ended my Special Report with the following recommendation:

> We call upon the government, in the strongest terms possible, to introduce amendments to the *Act*, providing Ontario's Commissioner with the same type of clear and explicit powers and authority to conduct privacy investigations that are available to other Privacy Commissioners in Canada, and to do so by the end of this legislative term.

The government did not accept this recommendation. As a direct consequence, the IPC was again unable to conduct a proper and thorough investigation of the circumstances stemming from the computer theft in Privacy Investigation #1.

The contrast between the approach taken by the Ministry in these two privacy investigations effectively crystalizes the deficiencies in the current statutory framework for privacy investigations. In Privacy Investigation #2, the Ministry co-operated fully with the IPC and satisfactorily addressed the issues of containment and notification. In Privacy Investigation #1, which, for all intents and purposes dealt with the same issues, the Ministry did not fully co-operate and, absent the necessary powers and authorities to compel co-operation, the IPC was unable to satisfy itself and the public that the Ministry's response to the disclosure of what I can only assume to be highly sensitive personal information, was adequate. This is clearly an untenable position for any Privacy Commissioner to be put in, and does not reflect public expectations.

The Deputy Attorney General states in his letter to me on Privacy Investigation #1 that the *Act* "does not provide the Commissioner with clear protection against being compelled to release information," and requires him to exercise discretion regarding release of information to the IPC. He reiterated this position in responding to the draft version of this Report. I do not fully accept this position. Section 55 of the *Act* provides:

> (1) The Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information that comes to their knowledge in the performance of their powers, duties and functions under this or any other Act.
>
> (2) The Commissioner or any person acting on behalf or under the direction of the Commissioner is not compellable to give evidence in a court or in a proceeding of a judicial nature concerning anything coming to their knowledge in the exercise or performance of a power, duty or function under this or any other Act.
>
> (3) No proceeding lies against the Commissioner or against any person acting on behalf or under the direction of the Commissioner for anything done, reported or said in good faith in the course of the exercise or performance or intended exercise or performance of a power, duty or function under this or any other Act.

In my view, this section adequately addresses the concerns identified by the Deputy Attorney General. However, if I am wrong and this section is deficient in any respect, then it is incumbent on the government to introduce whatever amendments are required to remedy the deficiency, and to do so promptly and comprehensively.

In my April 2000 Special Report, I made the following statements that I believe are equally applicable in the context of this report:

> It is abundantly clear that the present situation should not continue. We are confident in saying that the public expects its Privacy Commissioner to decide what type and what level of investigation is required in a particular situation, and to have the power and authority to ensure that all investigations are thorough and complete. Unless the *Act* is amended to provide explicit powers in this area, the particular government institution involved in potential privacy incident will be the one to decide whether and to what degree the incident warrants investigation. We can attempt to investigate, but without the coercive powers normally associated with an investigative mandate, such as the authority to order the production of records, to enter and inspect premises, and to summons and examine witnesses under oath, we will always be dependent on the co-operation of the particular government institution.
>
> ...
>
> The absence of explicit powers has prevented us from conducting a thorough investigation in this case. As a result, we had no choice but to investigate as best we could and to report our findings. This we have done, but we are not satisfied

> with the experience or the results of this investigation. We do not think the government should be satisfied either. ...

The need for change is long-standing and well documented; what is missing is the will to do so.

I am again calling on the government to address this important statutory deficiency as a top priority.

Original signed by: June 27, 2001

Ann Cavoukian, Ph.D. Date

Commissioner