Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. PC-020046-1

Ministry of Public Safety and Security

80 Bloor Street West,
Suite 1700,
Toronto, Ontario
M5S 2V1

80, rue Bloor ouest
Bureau 1700
Toronto (Ontario)
M5S 2V1

416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9195
TTY: 416-325-7539
http://www.ipc.on.ca

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. **PC-020046-1**

MEDIATOR: **Shaun Sanderson**

INSTITUTION: **Ministry of Public Safety and Security**

SUMMARY OF COMMISSIONER INITIATED COMPLAINT:

On September 26, 2002, the Office of the Information and Privacy Commissioner/Ontario (IPC) received a telephone call from the Ministry of Public Safety and Security (the Ministry) – Freedom of Information and Protection of Privacy Services' Deputy Coordinator regarding the theft of a laptop computer from the Office of the Fire Marshall (OFM). The IPC received a follow-up letter dated October 1, 2002. The letter indicated that the computer was stolen at approximately 12:30 p.m. on September 23, 2002 from an OFM office that was normally secured by card access only. However, it was discovered that the office door had become manually unlocked and staff had therefore been using their access cards to open a door that was not locked. Personal information was believed to have been retained on the local hard drive of the computer, and the Ministry indicated that since the computer was on at the time it was stolen, it was not in a password-protected mode. The letter also indicated that both the police and the Ministry's Manager of Information and Information Technology Security had been notified about the theft.

On the basis of this letter, the IPC initiated a privacy complaint under the *Freedom of Information and Protection of Privacy Act* (the *Act*).

Particulars concerning the incident

The Ministry agreed to conduct an internal investigation into the circumstances surrounding the computer theft, and to provide the IPC with a written report. The Ministry's investigation report of August 1, 2003 set out the following background in relation to this incident:

The Ministry is responsible for delivering correctional, policing and public safety and security services in Ontario. The OFM is a branch of the Public Safety Division of the Ministry, with its main corporate offices located in a privately owned building. Visitors to the OFM are required to register at a central reception desk and to obtain a visitor badge to wear at all times during their visit. On September 23, 2002 at approximately 12:30 p.m., a laptop computer was stolen from an OFM office. The computer was stolen from a normally secure, card access only office. However, the office door had become manually unlocked and staff had therefore been using their

access cards to open an unlocked door. The computer belonged to an administrative assistant to the Deputy Fire Marshall, and was removed from its docking station by an unidentified individual who entered the office while the administrative assistant was away from her desk. The computer was on at the time of the theft, and as such, was not in the usual Windows 2000 password-protected mode. No other property was stolen, and the theft was reported to the Toronto Police Service and the Ministry's Manager of Information and Information Technology Security. To date, the laptop has not been recovered.

DISCUSSION:

The following issues were identified as arising from the investigation:

Issue A: Is the information "personal information" as defined in section 2(1) of the *Act*?

Section 2(1) of the *Act* states, in part:

> "personal information" means recorded information about an identifiable individual, including,
>
> (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
>
> (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,
>
> (c) any identifying number, symbol or other particular assigned to the individual,
>
> (d) the address, telephone number, fingerprints or blood type of the individual,
>
> (e) the personal opinions or views of the individual except where they relate to another individual,
>
> (f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
>
> (g) the views or opinions of another individual about the individual, and
>
> (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;"

As previously noted, the stolen computer belonged to an administrative assistant in the OFM. The Ministry advised that the main responsibilities for this position are to provide administrative support to the Deputy Fire Marshall, particularly with respect to the OFM executive and policy committees. The Ministry's report indicates that the hard drive of the computer is believed to have retained primarily non-personal information from 2001 and 2002, such as OFM executive committee meeting minutes, OFM policy committee minutes, meeting information, internal memoranda, information relating to the OFM newsletter and approximately nine external business correspondence items. However, the Ministry notes that the computer also contained an electronic copy of a letter dated May 4, 2001, addressed to a member of the public who had contacted the OFM with concerns about the fire alarm system in her building, and accordingly submits that this letter contained the types of personal information listed in section 2(1) of the *Act*.

The Ministry also notes that the computer is believed to have contained employment-related information relating to senior OFM managers, such as pay-for-performance memoranda and performance appraisals. Although the Ministry submits that this type of information is excluded from the *Act* pursuant to section 65(6), the Ministry notes that the Deputy Fire Marshall has informed all senior OFM managers about the theft of the computer and the type of information contained therein.

Based on the information provided by the Ministry, I conclude that information in the laptop qualifies as personal information as defined in one or more of the subsections of section 2(1) of the *Act* as set out above.

Issue B: Was the disclosure of "personal information" in accordance with section 42 of the *Act*?

The Ministry notes that the stolen computer was password-protected and equipped with a Windows 2000 application. In order to access information contained on the hard drive of the computer, a user would normally need to provide his or her Ministry user identification and the correct unique password. However, since the computer was on at the time of the theft, the Ministry submits that it is possible that the individual who stole the computer may have viewed the contents of the computer's hard drive. The Ministry notes that once the computer was turned off, it would have reverted to a password-protected mode and that the computer's connection with the Ministry's local area networks would have been terminated upon removal from the docking station.

Section 42 of the *Act* sets out the rules for disclosure of personal information other than to the individual to whom the information relates. This section provides that an institution shall not disclose personal information in its custody or under its control, except in the circumstances listed in section 42(a) through (n). Having reviewed these provisions, I find that none of these circumstances were present in this case. Accordingly, I find that the disclosure of personal information by the Ministry was not in compliance with the *Act*. The Ministry does not dispute this finding.

Steps taken by the Ministry in response to the theft:

In its report, the Ministry indicates that the following steps were taken as a result of the computer theft incident:

- The theft of the computer was reported to the Toronto Police Service, the Ministry's Freedom of Information and Protection of Privacy Office and the Ministry's Information and Information Technology (I and IT) Security Manager.

- Immediately after the incident, the OFM arranged for the relevant office doors to be modified so that it would not be possible for a similar occurrence to happen in the future.

- The Facilities Management Branch was notified about the incident to ensure that this aspect of physical security is taken into consideration with respect to accommodation arrangements. In addition, the Facilities Management Branch has made several suggestions to the OFM for consideration.

- On October 11, 2002, the Deputy Fire Marshall sent a letter to the individual whose personal information was contained on the computer's hard drive, advising her of the incident. On October 31, 2002, the letter was returned by the post office with the notation that the addressee had "passed away".

- The OFM has purchased software that enables staff to trace the location of individual computers. To date, the software has been installed on most OFM computers. It is expected that it will be installed on the remaining computers as part of the computer refresh process by the end of September 2003.

- Several computer security best practices were highlighted for staff in the OFM newsletter, including: electronic retention of records on computer network drives (rather than hard drives), the importance of "locking down" computers when staff are away from their desks and completely shutting down computers when leaving at night to ensure that any necessary updates can occur.

Revised Security Policy and Awareness Program:

In its report, the Ministry advised that the Justice Technology Services is responsible for Information Management and Information Technology related functions within the Justice Cluster (Ministry of Public Safety and Security and Ministry of the Attorney General). The Ministry's current policy on computer security is contained on the Justice Technology Services intranet site, which all staff has access to.

As part of its security awareness program, the Justice Cluster I and IT Security section has prepared a revised security policy and awareness program that is currently in draft form. The Justice Cluster Security Policy Working Group has been tasked to co-ordinate the review, approval and enforcement of the revised security policy, which will be disseminated to all Justice staff following approval by senior management. The Ministry advises that the information will

be posted on the Justice Technology Services I and IT Security website, and will contain three main components: Education and Training, Policies and Procedures, and Resources. The site has been designed to educate existing and new staff about all aspects of information security. The Ministry believes that, in addition to the steps taken as a result of the theft, the finalization and distribution of the revised security policy and awareness program will result in increased privacy protection.

CONCLUSION:

I have reached the following conclusions based on the results of my investigation:

1. The information in question was personal information as defined in section 2(1) of the *Act*.

2. The disclosure of personal information by the Ministry was not in compliance with section 42 of the *Act*.

3. The disclosure was inadvertent, as it was caused by the theft of a laptop from the Ministry's premises. The Ministry has taken appropriate measures to ensure the protection of personal information in the future and to prevent similar incidents from reoccurring. The Ministry should also be commended for initiating its security policy and awareness program.

RECOMMENDATION:

I recommend that the Ministry finalize its security policy and awareness program, as discussed above. The Ministry should also take appropriate actions to ensure that all staff are notified and educated about the revised security policy and awareness program.

The Ministry should provide me with proof of compliance with the above recommendation by December 30, 2003.

September 30, 2003

Shaun Sanderson
Mediator

-