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-020033-1

Ministry of the Attorney General

April 3, 2003

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-020033-1**

MEDIATOR: **Shaun Sanderson**

INSTITUTION: **Ministry of the Attorney General**

SUMMARY OF COMMISSIONER INITIATED COMPLAINT:

On July 11, 2002, the Office of the Information and Privacy Commissioner/Ontario (the IPC) received a telephone call from the Executive Assistant and Counsel to the Deputy Attorney General, regarding the theft of a laptop computer from an office of the Ministry of the Attorney General (the Ministry). The IPC received a follow-up letter dated July 24, 2002, from the Assistant Deputy Attorney General, Legal Services Division, setting out the circumstances surrounding the theft of the computer from the Ministry's Crown Law Office – Civil. The letter indicated that the password-protected computer went missing some time over the weekend of July 1st during ongoing office construction. The letter also indicated that the police had been contacted and an investigation was underway.

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 set out the following background in relation to this incident:

The Ministry's Crown Law Office – Civil (CLOC) had planned office renovations for the weekend of July 1, 2002. Sometime over the weekend, the laptop portion of a computer docking station belonging to a lawyer at CLOC went missing, along with a disk which was left in the computer's "A" drive. The Ministry explained that on Friday, June 28, 2002, in preparation for the construction, the computer in question was moved from the individual's office and placed in a room with some other furniture. In addition to the regular building security, two security guards were employed by the Ministry to be in attendance on that floor during the time of the construction. On July 2, 2002, when the furniture was moved back into the individual's office, it was discovered that the laptop was missing. The Ministry then notified its main computer centre and the police. 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;"

The Laptop

The Ministry's report indicates that the computer contained litigation files related to counsel's practice which had been backed up on the computer's "C" drive. In further discussions, the

Ministry advised that the litigation files were comprised of pleadings, affidavits, motion materials, notes and correspondence and that most of this material would have contained information about identifiable individuals. The Ministry also confirmed that the laptop was password protected and had been shut down prior to counsel leaving the office.

I find that the information in the laptop is clearly personal information as defined in one or more of the subsections of section 2(1) of the *Act* as set out above. The Ministry does not dispute this finding.

The Disk

The Ministry's report indicates that the disk, which had been left in the computer's "A" drive, contained notes and "to do" lists prepared for counsel's personal use, and did not contain any documentation related to Ministry business. Although the disk was not password protected, the Ministry advised that it was the personal property of the lawyer and that there was nothing contained in the information on the disk that would identify the owner, nor did it contain any personal identifiers or labels. In view of the fact that the disk did not contain any information relating to Ministry business, its contents will not be discussed further in this report.

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

In this case, the Ministry states that since the computer was password protected, there was no disclosure of information. In its final report to this office, the Ministry notes the following:

- The laptop was password protected and had been shut down prior to counsel leaving the office;
- The laptop is equipped with a Windows 2000 application. In order to access the computer, the user must provide the correct user ID and the correct password. Counsel used a unique password rather than an obvious one such as "password". In addition, the Ministry's Information Technology procedures require that the user must change the password every few months;
- The laptop had been moved from counsel's office to another location during the renovations. There were no labels or indicators on the laptop to identify to whom it belonged; and
- The level of security on laptops with Windows 2000 is such that the information could not have been accessed by anyone other than the authorized user.

The laptop in question was equipped with a Windows 2000 application and protected by a unique password in compliance with the Ministry's policies. Although this does not guarantee that an unauthorized user can never access the information, in light of the measures taken by the Ministry, and in the absence of any evidence to the contrary, I am not persuaded that there has been a disclosure contrary to section 42 of the *Act*.

Findings of the Ministry's investigation and steps taken in response:

In addition to notifying its main computer centre and the police, CLOC distributed the Ministry's Policy on Confidential Information as a reminder to staff. This policy will be discussed in greater detail below.

With respect to security during renovations or construction, the Ministry notes that, although additional security personnel were hired, further measures to safeguard equipment during such times should be explored. The Ministry also recognizes that as a general practice, staff should be periodically made aware of the requirements with respect to security issues including safeguarding equipment and confidential information during renovations.

The Ministry proposed the following two recommendations in its final report to the IPC:

1. The Ministry should develop a policy to address the security of the premises when non-employees are visiting. This policy would include measures such as safeguarding equipment during construction/renovations, storing equipment in a secure area, removing disks from computers etc.; and

2. Periodic reminders/training for staff should be conducted on the need for ensuring the security of equipment and the protection of confidential information particularly during renovations/construction.

Additional Comments:

A previous investigation report dated June 27, 2001 dealt with two privacy investigations (PC-000026-1 & PC-010009-1) at the Ministry involving the disclosure of personal information as a consequence of computer theft. As a result of these incidents, the Ministry, in co-operation with the IPC, undertook a broad review of its policies and procedures for the handling of private and confidential material. In August 2001 the Ministry finalized its Policy on Confidential Information, which addresses the following four areas:

Part A – Document Security;
Part B – Transporting Confidential Information;
Part C – Faxing Procedures; and
Part D – Telephone Inquiry Procedures.

In September 2001, the Deputy Attorney General distributed a memorandum to all Ministry staff, notifying them of the Ministry's finalized Policy on Confidential Information. The memorandum stressed the importance for all Ministry staff members to be aware of the requirements outlined in the attached Policy, and also noted provisions regarding laptop computers, including the requirement for all laptops to be password-protected.

Since the previous two computer thefts in 2001, it is evident that the Ministry has implemented a comprehensive set of policies and procedures for ensuring the protection and proper handling of confidential material. In this case, the theft of the laptop from the Ministry's premises was an

unfortunate incident over which the Ministry had little control. It is clear that, in hiring additional security personnel during the renovation period, the Ministry took reasonable steps to prevent this incident from occurring. Furthermore, the stolen laptop was password protected in accordance with the Ministry's new policies, and as such, the Ministry's actions greatly diminished, and likely prevented, a possible disclosure of personal information. The Ministry should therefore be commended for developing and implementing its Policy on Confidential Information.

However, this investigation also raises some important questions regarding the security of the Ministry's premises, particularly during renovations or construction. The Ministry's suggestion to develop a policy for addressing the security of its premises is a good one and will therefore be included as a recommendation in this Report.

Another issue that arose during this investigation relates to the use of computer disks. The Ministry's policy for transporting confidential information does not currently require that disks be password protected. Although, in this case, the disk in question did not relate to Ministry business, this is an opportune time for the Ministry to revise its policy in this regard. A revision with respect to the protection of information on disks will therefore also be included as a recommendation in this Report.

CONCLUSION:

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

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

2. The information on the stolen laptop was adequately protected with a unique password, in accordance with the Ministry's policies regarding confidential information. Based on the fact that the laptop was protected with a unique password, and in the absence of any evidence to the contrary, it is reasonable to conclude that the information was not disclosed contrary to section 42 of the *Act*.

RECOMMENDATIONS:

1. I recommend that the Ministry develop a policy to address the security of its premises when non-employees are visiting. This policy should include measures for safeguarding equipment and ensuring the protection of personal information during construction and/or renovations. The Ministry should also take appropriate actions to ensure that all staff are notified and educated about these procedures.

2. I recommend that the Ministry revise its Policy on Confidential Information with respect to the use of computer disks. In particular, I recommend that disks be password protected for usage off-site. The Ministry should also take appropriate actions to ensure that all staff are notified about this revision.

The Ministry should provide me with proof of compliance with the above recommendations as follows:

1. Recommendation #1 by **October 3, 2003**, with a status report by **July 3, 2003**;
2. Recommendation #2 by **July 3, 2003.**

April 3, 2003

Shaun Sanderson
Mediator