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

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT PC-000043-1

Ministry of the Attorney General

June 15, 2001

FINAL PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. PC-000043-1

INSTITUTION: Ministry of the Attorney General

SUMMARY OF COMMISSIONER INITIATED COMPLAINT:

The Office of the Information and Privacy Commissioner (the IPC) received a letter from the Assistant Deputy Attorney General, Criminal Law Division, setting out the circumstances surrounding an inadvertent disclosure of personal information that had occurred a few days earlier.
In particular, a locked vehicle owned by a *per diem* Crown Attorney was broken into while the vehicle was parked. Several briefcases were stolen which contained a number of Crown files pertaining to criminal matters that were currently before the courts.

On the basis of this letter, the IPC initiated an investigation pursuant to our responsibilities under the *Freedom of Information and Protection of Privacy Act* (the *Act*).

Theft of the briefcases

The letter from the Assistant Deputy Attorney General set out the following additional information regarding this incident:

> Police were notified and, following an investigation, the police recovered the files three days after the theft. The police promptly identified which Crown files had been in the stolen briefcase and quickly determined whether the lost information posed any security risk to victims or witnesses. In such cases, the parties were notified immediately of the theft.
>
> The police investigation was still ongoing. Once the investigation was complete the police and Crown would meet to consider the appropriateness of notification to the remaining individuals. The Ministry would seek the IPC's input on the issue of notification.
>
> The Criminal Law Division would undertake a review of current practices regarding the handling and transporting of Crown files with a view to enhancing confidentiality procedures. As an interim measure, all managers in the Criminal Law Division would be asked to remind their staff that Crown briefs should not be left unattended and that appropriate measures should be taken when files are being transported.

DISCUSSION:

The following issues were identified as arising from the investigation:

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

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

> (a) information relating to the race, national or ethnic origin, colour, religion, **age**, **sex**, sexual orientation 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,
>
> (d) the **address, telephone number**, fingerprints or blood type of the individual,
>
> (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;"

During the course of our investigation, the Ministry confirmed that, in fact, three brief cases containing approximately eighty-eight Crown briefs were stolen. Among the information included in these briefs were names, addresses and telephone numbers of victims and their family members, those accused including young offenders, and witnesses; Canadian Police Information Centre records and psychological snapshots; witness statements; copies of police investigation notes and notes of Crown lawyers.

The information that was stolen meets the definition of personal information as defined in one or more of the subsections of section 2(1) of the *Act* set out above. The Ministry does not dispute this finding.

Was the disclosure of the personal information in accordance with section 42 of the *Act*?

Section 42 of the *Act* sets out a number of circumstances under which an institution may disclose personal information. Clearly, in situations where there has been a theft of personal information, none of those circumstances apply. The disclosure, therefore, was not in accordance with the *Act*.

Steps taken by the Ministry immediately after the theft

- Police were immediately notified and searched the area without success.

- The Crown Counsel immediately notified the acting Crown Attorney and early the next morning notified the Ministry's West Regional Directorate office.

- The initial concern of the West Regional Directorate was to ensure that any vulnerable persons be immediately notified of the of the theft. With this in mind, the west Regional Directorate instructed the acting Crown Attorney to contact the relevant police services to ensure their notification. The Ministry has provided evidence that telephone notification did occur on a wide scale.

- Within forty-eight hours of the theft, a lawyer telephoned the London Crown Attorney's office and advised that his client could be in possession of these briefcases. The briefcases were returned to the police the next day, three days after the reported theft.

- As a result of various telephone conversations with the lawyer and upon the Crown Attorney's and police review of the returned briefs, they were able to reasonably conclude that all briefs were accounted for and had not been tampered with, duplicated, disseminated and/or distributed to anyone else in whole or in part.

Additional remedial steps taken by the Ministry

- The Assistant Deputy Attorney General, Criminal Law Division reported the incident to the Deputy Attorney General and circulated, via e-mail, a confidential memorandum to Assistant Crown Attorneys, Crown Counsel and other staff in the Criminal Law Division briefly describing the circumstances surrounding this incident and reminding staff of the need to take great care when transporting Crown briefs and other files containing personal and confidential information.

- All Ministry staff received, via e-mail, an "interim" policy issued by the Deputy Attorney General on the subject of "Transporting Confidential Information". The policy addresses procedures for the removal of confidential information from the office and, in particular, sets out protocols for the use of laptop computers outside the office. I am advised that this policy is one of a series of four privacy related policies being developed by a Privacy Committee that was struck by the Deputy Attorney General and is being lead by an Assistant Deputy Minister. The Ministry of the Attorney General's Freedom of Information Co-ordinator is on the Committee. The other three policies will deal with faxing, document security, and conveying information over the telephone.

- At the request of the IPC, the Ministry sent in excess of 400 letters to accused persons, witnesses and victims notifying them of the theft and subsequent recovery of files that contained their personal information.

CONCLUSION:

I commend the Ministry staff for their prompt response after learning of the improper disclosure of personal information, and for the steps the Ministry has taken to address this. It is clear that the Ministry understands the seriousness of this matter and gave considerable thought and priority to taking appropriate action.

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

1. Highly sensitive personal information of a large number of individuals was disclosed, though inadvertently by theft, in contravention of the *Act*.

2. In the particular circumstances of this case, I am satisfied with the extent of the notification provided to individuals about the disclosure.

   In situations where there has been improper disclosure of personal information, this Office requests that the institution notify all individuals affected by the disclosure. In this case, immediate wide scale notification did take place, with priority being given to those whom the police and Crown Attorney assessed as potentially most vulnerable. Within forty-eight hours of the theft the briefcases were recovered and through inquiries and review of the actual documents, it was confirmed that the disclosure of the personal information had been limited to one individual who, when realizing what the documents were, immediately took steps to return them to the Ministry.

3. Thefts of work materials (briefcases, laptop computers, etc.) containing personal information are an increasingly common occurrence both generally and at the Ministry. While clearly certain staff must take files out of the office in the performance of their duties, the fact that the theft occurred raises concerns about the awareness of staff regarding the *Act* and issues pertaining to privacy protection.

RECOMMENDATIONS

In addition to the steps already taken by the Ministry, I recommend the following:

1. The Ministry establish an ongoing training program for all new and current staff on both the access and privacy provisions of the *Act*, and Ministry privacy policies.

2. The Privacy Review Committee at the Ministry complete and distribute the remaining three privacy related policies (as part of its package of four privacy related policies), taking into account the IPC's comments which have already been provided to the Ministry.

The Ministry should provide the Office of the Information and Privacy Commissioner with proof of compliance with the above recommendations no later than **September 15, 2001**.

Original signed by: June 15, 2001

Diane Frank
Manager of Mediation