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-030041-1

Ministry of Labour

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-030041-1**

MEDIATOR: **Maria Tzimas**

INSTITUTION: **Ministry of Labour**

SUMMARY OF COMMISSIONER INITIATED COMPLAINT:

On September 31, 2003, the Office of the Information and Privacy Commissioner/Ontario (the IPC) received a telephone call from the Manager of the Freedom of Information and Privacy Office of the Ministry of Labour (the Ministry) regarding some files that had gone missing from a district office of the Employment Standards Branch. On October 6, 2003, a meeting was held at the IPC with the Manager of the Freedom of Information and Privacy Office, the Chief Administrative Officer of the Internal Administrative Services Division, and the Regional Director of Central Region of the Ministry. At this meeting, the Ministry confirmed that a number of employment standards files had gone missing from the Peel South District Office as well as other District Offices within the Operations Division.

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

Particulars Concerning the Incident

In February 2002, the local Manager in the Peel South District Office identified a problem with an Employment Standards Officer (ESO) not returning closed files in a timely manner. On July 15, 2002, a letter was issued to the ESO by the Regional Director demanding the return of all open and closed files. On July 17, 2002, the ESO confirmed in writing that he had returned all files in his possession. Verification of the ESO's claim that he had returned all files was difficult because the records management tracking and filing system contain numerous weaknesses that prevented the Ministry from verifying whether the files had been returned. The Ministry was unable to locate all of the files that had been recorded as assigned to this ESO. The ESO retired on August 12, 2002.

Employment standards cases are generated when individuals file an employment standards claim. A standard claim form is completed and signed by the individual which contains information such as the name, address, phone numbers, social insurance number, occupation, employment history, remuneration level and the name and address of the employers. Claim files

may also contain other information including T4 slips, medical information, photographs, Workplace Safety and Insurance Information and other personal notes and records depending on the nature of the claim.

In the fall of 2002, the Ministry began to receive complaints from a number of former clients of the retired ESO about the status of their cases. As a result of these complaints, the Ministry decided to conduct an internal audit investigation of the Peel South District Office. This investigation was commenced in November 2002 and was conducted by the Internal Audit Division of Management Board Secretariat (MBS). This audit was concluded in February 2003, out of which a series of recommendations emerged.

In February 2003, the Assistant Deputy Minister (ADM) of the Operations Division circulated a memo to all Directors instructing them to take specific administrative actions to ensure the tracking and security of private and confidential information. As of November 2003, the Ministry confirmed that the following measures had been implemented in all Regions:

- Access to all file rooms is restricted to Managers, Administrative Assistants, and Program Assistants and all file rooms are locked;
- Sensitive documents containing personal information are secured and all offices and workstations have cabinets for locking information;
- All performance plans include responsibility and accountability for file management and security;
- Audits through Corporate Services compliance reviews: Terms of Reference have been updated to include the verification of physical existence of program files.

In addition to the above, the Ministry advised that the following file management improvements have been implemented with respect to file tracking practices:

- All requests for case files are submitted to Program Assistants;
- Program Assistants are responsible for filling in all the fields of the file tracking log when signing out a case file from the central file room;
- The requester must sign the log when receiving the file;
- Program Assistants are responsible for handing files over to requesters;
- On a monthly basis, the Program Assistants are responsible for creating a report for the Manager that contains the files that have been signed out during that month;
- Three weeks into borrowing the file, the Program Assistant will send out a reminder via e-mail to the borrower reminding them that they should either return the file within the 30 days or renew the sign-out;
- Program Assistants are responsible for completing the sign-in process and returning the file to the appropriate location within the Central File Room;
- When returning a file, the requester must sign the log;
- District Managers are required to audit ESO's by spot-checking their open files and any closed files they have signed out;
- Managers review the logging report monthly;

- Corporate Services Management review tracking systems during compliance reviews.

In addition to the interim measures described above, in July 2002, the Ministry initiated a full scale Management review project in Central Region that includes a review of all record keeping practices in all eight district offices and the director's office. Shared Services Bureau (SSB) was contracted in September 2002 to provide a report and recommendations for improving the file management system, including recommendations concerning the security of files. The standards arising from this review will be applied across the Operations Division. SSB's review was completed in March 2003 and a project management team is currently in place to implement the recommendations. As of November 2003, the Director's Executive Committee of the Ministry's Operations Division approved the Divisional File Security and Management Initiative.

The Ministry also retained a consulting company in March 2003 to conduct a province-wide scan of the employment standards program to determine if the missing files were an isolated case relating to the Peel South District Office or a result of a broader systemic problem. A physical review of all closed files for the entire province for the period April 2000 to January 2003 was conducted and revealed that out of approximately 40,000 files, 267 were missing province-wide, of which 119 were directly attributable to the one ESO who retired in August 2002.

As a result of all of the reviews described above, the Ministry concluded that there was no evidence that any of the missing files were lost in the public domain and that these files went missing as a result of poor tracking of transfers between offices and program assistants, district offices, and collection agencies or legal services. The Ministry is of the view that the Operations Division's Information Management Project that is currently underway will establish new standards and operating procedures for file management that will further reduce the risk of such occurrences of missing files in the future. This is a two-year initiative, the completion of which is expected in 2005.

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 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 Ministry confirmed that employment standards files contain information such as names, addresses, phone numbers, social insurance numbers, occupations, employment histories, remuneration levels, and the names and addresses of employers. These files may also contain other information such as T4 Slips, medical information and other personal notes and records depending on the nature of the claim.

I find that the information contained in the missing employment standards files 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.

Were the missing files disclosed contrary to section 42 of the *Act*?

As outlined above, the Ministry has undertaken extensive audits, including internal and external investigations with respect to this matter. As a result, the Ministry concluded that there is no evidence that any of the missing files were in the public domain, but rather that they are missing internally and likely misfiled for the most part. In light of this, and in the absence of any evidence to the contrary, there is no reasonable basis on which to conclude that there has been a disclosure contrary to section 42 of the *Act*.

Was the personal information protected in accordance with section 4 of O. Reg. 460?

Section 4 of O. Reg. 460 states:

> 4. (1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.
>
> (2) Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it.
>
> (3) Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected.

As described above, the Ministry undertook extensive reviews with respect to this incident including an internal audit conducted by the Internal Audit Division of MBS of the Peel South District Office and a province-wide scan of the employment standards program by a consulting company. Both reviews concluded that inadequate measures were in place with regards to file management practices that ultimately jeopardized the security of files containing personal information. On the basis of the results of these reviews, I conclude that the measures that were previously in place by the Ministry to protect personal information were not in accordance with section 4 of O. Reg. 460.

As outlined above, the Ministry described a series of interim measures that it has implemented in an effort to enhance the tracking and security of personal and confidential information as well as file management procedures. The Ministry is also involved in an Information Management Project involving the Operations Division. This is a longer-term initiative that will establish new standards and operating procedures for file management with a view to further reducing the risk of occurrences of missing files in the future. In light of these measures and initiatives, I am satisfied that the Ministry has taken appropriate steps in order to ensure that similar incidents of this nature do not occur in the future.

Delay in notifying the IPC

The IPC has developed a document entitled *What to do if a privacy breach occurs: Guidelines for Government Organizations*. In this document, institutions are provided with a list of guidelines on immediate actions that should be taken upon learning of a privacy breach. One of these actions involves informing the IPC registrar of the privacy breach and working together constructively with IPC staff.

In this case, the Ministry first became aware of a potential problem with respect to the certain files back in February 2002 and by July of the same year it had initiated a full scale Management review in Central Region that included a review of all record keeping practices, followed by other audits/investigations. The IPC, however, was not notified until October 2003. This time lapse represents a significant delay and based on the IPC's guidelines, the Ministry should have

notified this office of the incident in question and possible breaches immediately. Despite the Ministry's own significant efforts to investigate and address this matter, such a delay to contact this office is unacceptable.

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. There is no reasonable basis to conclude that the missing files were disclosed contrary to section 42 of the *Act*.

3. The measures that were previously in place by the Ministry to protect personal information were not in accordance with section 4 of O. Reg. 460.

4. In light of the interim measures implemented by the Ministry, as well as its long-term initiatives, I am satisfied that the Ministry's Operations Division has taken appropriate steps to protect the personal information within its hard copy files in accordance with section 4 of O. Reg. 460.

RECOMMENDATION:

In accordance with the IPC's guidelines entitled *What to do if a privacy breach occurs: Guidelines for Government Organizations*, I recommend that the Ministry develop a policy outlining the procedures that should be followed in the event of a privacy breach, in order to ensure that both the Ministry's Freedom of Information and Privacy Office and the IPC are notified immediately upon learning of a privacy breach. All Ministry staff should be educated about this policy.

By **May 31, 2004**, the Ministry should provide the Office of the Information and Privacy Commissioner with proof of compliance with the above recommendations.

Original Signed by: February 23, 2004

Maria Tzimas, Mediator per:
Irena Pascoe, Team Leader