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-030042-1

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-030042-1**

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 the theft of computers from one of the regional offices of the Office of the Worker Advisor (OWA). On October 6, 2003, a meeting was held at the IPC with the Manager of the Freedom of Information and Privacy Office (FOI), the Chief Administrative Officer of the Internal Administrative Services Division, and the Director of the Office of OWA. At this meeting, the Ministry confirmed that a series of break-ins occurred at the Scarborough OWA earlier in the year that resulted in the theft of several desktop computers.

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

During the course of this investigation, the Ministry provided the IPC with the information outlined below.

During the weekend of April 21, 2003, two break-ins occurred at the Scarborough OWA Office. The first break-in occurred on April 21 and the second occurred on April 22. One desktop computer was stolen during each of these break-ins. A subsequent break-in occurred on May 2 wherein one more computer was stolen. The Police were notified and reports were filed immediately upon discovery of the break-ins. To-date, none of the stolen computers have been recovered by the Police. The OWA also notified MOL Facilities and Economics and Business Cluster Security. FOI and Issues Management Staff were consulted following the break-ins.

The Ministry advised that two of the three computers did not contain any personal information on the hard drives. One of the computers was used primarily for word processing and the user

did not make it a practice to store any documents on the hard drive. The other computer was new and had not yet been used. However, one of the computers did have personal information stored on the hard drive relating to research and preparation of presentations on behalf of injured workers, including client names. The Ministry confirmed that all three computers were password protected with a unique password against access to the hard drives and that they were all turned off at the time of the thefts.

The Ministry advised that the OWA took physical security measures immediately following the break-ins and enhancements were implemented over the following month, including changing the security firm and providing for greater perimeter security measures. Included in the greater perimeter security measures was the installation of a security window film on all windows at the Scarborough OWA Offices, enhanced exterior lighting, the installation of additional security cameras, and exterior landscaping measures.

Following the break-ins, OWA Regional Managers have continued to review security protocols with staff to reinforce prior training that all staff received from the Ministry's FOI training on information management. Specifically, in June 2003, the Director of the OWA circulated a protocol on professional and public servant responsibilities to all OWA staff via e-mail. This document incorporates some general guidelines with respect to the handling of confidential information. In September 2003, a subsequent e-mail was distributed to all staff containing a checklist of best practices for securing confidential information. A subsequent reminder was distributed to all OWA staff in November 2003 regarding the protection of confidential information.

Furthermore, the OWA purchased a CD burner for the Scarborough Office and created a back up for personal, sensitive or confidential information. Staff was instructed that confidential files containing personal information are not to be stored on hard drives. All CD's that are used for back-up are secured under lock and key and all desktop computers are secured to the workstations by locked security devices. The Ministry also confirmed that all computers are equipped with a Windows 2000 Professional operating system and that logon authentication is by means of a user identification and password.

The Ministry further advised that in the fall, a consulting company conducted a Threat Risk Assessment of the OWA information management practices under the supervision of Management Board Corporate Security. A workshop was held on Oct. 28 with participants from the OWA program, the Ministry FOI and Privacy Office, the Economics and Business Cluster, and Corporate Security MBS. The final report will detail findings and recommendations based on the Threat Risk Assessment workshop and business and technical documentation provided by the Program area and on-going discussions with OWA staff. The Ministry also advised that the recommendations of the report will help substantiate and improve upon the best practices and guidelines existing for staff on handling and securing confidential information and will also prompt the implementation of an ongoing information classification process. Training will be provided for all OWA staff for classifying and securing OWA documents.

Finally, the Ministry advised that the OWA is working on a larger scale initiative with the Economics and Business Cluster and Management Board to develop a comprehensive network

attachment storage solution (NAS), with the Scarborough Office as the pilot site. The project will incorporate a data classification initiative to ensure effective management and classification of confidential information files. The NAS solution would ensure that confidential information would no longer be stored on hard drives, thus dramatically reducing vulnerability should there be a theft or loss of computers. The Ministry advised that the NAS server will be made available to all OWA staff by May 31, 2004. As part of the implementation of NAS, the Ministry's FOI and Privacy office will be working with OWA on preparing guidelines for staff on the proper and efficient use of the NAS server for saving confidential and sensitive information.

Additional Matters

In addition to the OWA offices, the Ministry was asked to provide information concerning its Operations Division, specifically, how desktop computer users save data containing personal information. The Ministry advised that desktop computer users work and save all of their data directly onto a local server and are instructed not to save on their hard drives. The Ministry further advised that the Operations Division is in the process of developing guidelines in this regard.

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;

As noted above, three desktop computers were stolen from the Scarborough OWA Office. The Ministry advised that two of the computers did not contain any personal information and they were password protected. In view of the fact that these computers did not contain any personal information, they will not be discussed any further in this report. However, the Ministry did confirm that one of the computers did contain personal information, including client names, as defined in section 2(1) the *Act* as set out above.

Was the "personal information" disclosed contrary to section 42 of the *Act*?

The desktop computer that contained personal information was equipped with a Windows 2000 Professional operating system and protected by a user identification and unique password. The Ministry also confirmed that the computer was turned off at the time of the theft. Although this does not guarantee that an unauthorized user can never access the information, in the absence of any evidence to the contrary, I am not persuaded that there has been a disclosure of personal information contrary to section 42 of the A*ct*.

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 incidents of the thefts of the computers occurred in April and May 2003 and the IPC was not notified until October. This time lapse represents a significant delay and based on the IPC's guidelines, the Ministry should have notified this office of the incidents and possible breaches immediately. Despite the Ministry's own significant efforts to investigate and address this matter, a delay of six months 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. The information on the stolen computer was adequately 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:

In view of the Ministry's ongoing initiatives as described above, I recommend the following:

1. The Ministry should complete preparing guidelines for OWA staff on the proper use of the NAS server for storing personal information. The guidelines should specifically state that personal information must not be stored on the hard drives of desktop computers. All OWA staff should be educated about these guidelines.

2. The Ministry should make the NAS server available to all OWA staff.

3. The Ministry should complete preparing guidelines for the Operation Division on the proper use of its local server for storing personal information. The guidelines should specifically state that personal information must not be stored on the hard drives of desktop computers. All Operations Division staff should be educated about these guidelines.

4. 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