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-050003-1

Ministry of Consumer and Business Services

Tribunal Services Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Services de tribunal administratif
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9188
TTY: 416-325-7539
http://www.ipc.on.ca

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. **PC-050003-1**

INVESTIGATOR: **Jennifer James**

INSTITUTION: **Ministry of Consumer and Business Services**

SUMMARY OF COMMISSIONER INITIATED COMPLAINT:

Background

On January 19, 2005, the Office of the Information and Privacy Commissioner (the IPC) was notified by the Ministry of Consumer and Business Services (now Ministry of Government Services) (the Ministry) about a breach of the *Freedom of Information and Protection of Privacy Act* (the *Act*). The IPC subsequently initiated a privacy investigation under the *Act* and the Ministry was asked to submit a written response to the IPC. The Ministry's representatives also attended the IPC's offices to discuss their efforts to contain and remedy the breach.

The Ministry advised that on January 13, 2005, it received an email from a member of the public, who had applied for a birth certificate using the Ministry's Smart Form on-line application. The applicant advised that she was able to access the file directory where the files were stored temporarily and view completed birth certificate applications of others on the Ministry's website, three days after her original session.

The Ministry took immediate steps to address the breach. In particular, once the Office of the Registrar General became aware of the matter they immediately notified the Assistant Deputy Ministry (Registration Division), the Deputy Registrar General (Director of the ORG), the Security Officer for the ORG, senior staff within the Economic and Business Cluster (EBC), Legal Services, program area representatives, the Information and Privacy Coordinator, the Deputy Minister and the Minister's Office and a special team was established to deal with this matter. The Ministry also immediately took the Smart Form off-line, notified the IPC, and commenced its own internal investigation.

The Smart Form is an interactive on-line tool that can be used by individuals applying for a birth certificate. It includes drop-down menus, mandatory fields and edit checks. There is a help

button on every page and the form is designed to eliminate common errors made by applicants. The user is directed to populate the form and the system checks to ensure that it is complete. The system is designed to expunge information after each applicant's individual session is completed.

Once the form is fully populated the user is directed to print the form and submit the paper copy to the Ministry by mail or fax along with the application fee. At the time of the breach, users could only submit their birth certificate request by mail or fax. The Ministry has since introduced an on-line application process where parents of a child under the age of eight can submit their request for a birth certificate electronically.

Throughout the IPC's investigation process, the Ministry expressed its concern over the breach and assured the IPC of their intention to co-operate fully with our investigation, which they have indeed done.

The Ministry's Internal Investigation and Containment Efforts

As outlined above, once the Ministry became aware of the problem, the Smart Form was immediately taken off-line to ensure that no further privacy breaches could occur while the matter was being investigated. An internal investigation was launched immediately by senior Ministry staff.

The Ministry's internal investigation focused on how the Smart Form software failed to expunge the viewed sessions, the extent of the files involved, who else may have accessed the information and whether other web-based applications were affected.

The Ministry's investigation team identified a design flaw that allowed records to be retained and accessed. The system was designed to expunge information after an individual's session was completed. However, the software created temporary files during the session that were not immediately deleted after the form was completed. These temporary files were stored in a specified directory for a short period of time.

The team reviewed the historical system transactions logs from the time the Smart Form was launched until the day it was taken out of service and found that four separate files had been accessed during the period of January 8, 2005 to January 11, 2005; three by the individual who had notified the Ministry and one by another individual who was not known to the Ministry. The Ministry concluded that no other access had occurred and no other web-based applications were affected. The Ministry contacted the applicant who had reported the situation and was assured that she had not printed, stored nor transmitted any files. With respect to the other individual, the Ministry consulted with the IPC and was advised that the Ministry did not need to take any other steps to try to identify and contact this individual.

The Ministry's internal investigation was followed by a review by independent IT security experts retained by the Ministry, who duplicated the test results of Ministry staff. As part of its investigation, the Ministry reviewed the entire Smart Form application and made modifications to ensure that only the individual completing the form could view the information and that the system did not retain a record of completed or partially completed forms. The independent IT

security experts also tested the new web application's security measures, as well as two others using the Smart Form technology before it was placed back in service. The Ministry advised that only after both the internal and external testing was complete did the Ministry make the decision to bring the application back on-line.

Finally, the Ministry indicated that in light of this incident, a special team was established to review policies and procedures in an effort to develop a more detailed and more rigorous privacy and security risk analyses when implementing new technological processes. The Ministry indicated that it intends to consult the IPC's Policy and Compliance Department upon its completion of its finalized policy.

Notification of Individuals Whose Forms Were Accessed

During the investigation stage of this complaint, the Ministry contacted the IPC to seek direction as to how it should notify the individuals whose personal information may have been inadvertently disclosed. The challenge in doing so was that the web application was not designed to retain the personal information of the person filling out the form. Accordingly, the Ministry's staff was only able to retrieve the machine name/number and the Internet service provider of the four clients whose files were accessed.

After consulting with the IPC, the Ministry contacted each of the Internet service providers and asked them to forward an e-mail to their client, if their client was an individual residential customer or if it was an institution, if it could be linked to an identifiable individual. The e-mail advised the individual that on a specific date, they or someone using their Internet account accessed an on-line application form for an identity document. The e-mail requested that the individual who used the form contact the Ministry's Deputy Registrar General.

All of the Internet service providers agreed to send an e-mail to their clients. One of the Internet service providers responded that it was unable to successfully forward an email to their customer. Follow-up attempts to re-send the e-mail failed, despite the Internet Service Provider having contacted someone at the phone number on record for the account and having explained the situation. In addition, the Internet Service Provider forwarded by mail a letter to the customer from the Ministry, with the same content as the e-mail, requesting that the person who used the form contact the Deputy Registrar General.

At the time of this report, only one individual contacted the Ministry. The Ministry advised the individual that the user who viewed their application had assured the Ministry that she did not print, store or forward it. The individual was also advised of the steps taken by the Ministry to address the inadvertent disclosure. The Ministry offered to flag the birth registration so that any request for a copy of that certificate would have to undergo additional security precautions and the individual accepted. A follow-up letter was also sent to this individual by the Ministry. The Ministry advised that if or when the remaining affected individuals contact the Ministry, the same procedure will be followed.

DISCUSSION:

The following issues were identified as arising from the investigation:

Issue A: Was the information disclosed on the Ministry's website "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,

...

(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.

I have reviewed the record at issue, which is a form entitled "Request for Certificate". The form contains the:

- name, address, martial status, date of birth and place of birth of the mother;
- name, date of birth and place of birth of the father;
- name, sex, date of birth, place of birth, weight at birth, number of siblings of the person named on the birth certificate;
- name and address of the person attending to the birth and whether the birth took place in a hospital, birthing centre or other location;
- name, address and telephone number of the applicant in addition to their credit card information if the applicant choose to submit the application by fax; and
- name, occupation, telephone numbers and address of the guarantor.

I conclude that the record clearly contains information which qualifies as personal information under sections 2(1)(a), (b), (c), (d) and/or (h) of the *Act* set out above.

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

Section 42 sets out a number of circumstances under which an institution may disclose personal information. None of these circumstances are present in this case, where personal information is inadvertently disclosed. Accordingly, I conclude that the disclosure of the personal information of other individuals who were not the applicant by the Ministry was not in compliance with the *Act*.

CONCLUSIONS:

I commend the Ministry for the prompt action taken to contain the privacy breach and for its attempts to notify the affected individuals. As well, the Ministry should be commended for its thorough investigation into this matter and all the steps that have been taken, in an effort to prevent future similar occurrences. The use of independent IT security experts to test the system prior to putting back in service is particularly laudable and represents a best practice in this area.

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

1. The information disclosed in the record is "personal information" as defined in section 2(1) of the *Act*;

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

3. The disclosure was inadvertent, and an unintended result of a technical anomaly;

4. The Ministry has taken appropriate steps in its attempt to notify the individuals affected by the disclosure; and

5. The Ministry has taken appropriate steps to contain the privacy breach and prevent future similar occurrences.

In view of the circumstances of this case and the initiatives undertaken by the Ministry described above, no further action is necessary with respect to this matter.

Original signed by: August 8, 2005

Jennifer James
Investigator