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-020036-1

Ministry of Consumer and Business Services

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-020036-1**

MEDIATOR: **Mumtaz Jiwan**

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

SUMMARY OF COMMISSIONER INITIATED COMPLAINT:

On July 10, 2002, the Ministry of Consumer and Business Services (the Ministry) notified the Office of the Information and Privacy Commissioner/Ontario (the IPC) about a possible breach of the *Freedom of Information and Protection of Privacy Act* (the *Act*). The Ministry advised that a number of completed application forms for certificates were missing from their offices. The Ministry could not confirm whether these documents were misfiled, lost, stolen or inadvertently shredded, but did indicate that the police were investigating the matter. The Ministry further stated that it had initiated an internal audit of all of its offices.

On this basis, the IPC opened an investigation file pursuant to our responsibilities under the *Act*. However, we deferred beginning our investigation until the completion of both the police investigation and the Ministry's own internal audit. By January 2003, the police had laid charges against an individual, though their investigation was still ongoing. Nevertheless, the Ministry suggested that we begin our investigation into the matter, which we did.

Our investigation focussed on the scope of the disclosure, notification of the individuals whose personal information may have been disclosed, and the security of the records processing and retention systems.

Background:

The Office of the Registrar General (ORG) is responsible for, among other things, issuing birth, death and marriage certificates. Approximately 400,000 certificates are issued every year. Prior to 1996, certificates were issued by the head office in Thunder Bay and by the Toronto office, where same day service was also provided. Birth certificates are of particular importance as they are considered "foundation documents," relied on by other governments and law enforcement agencies to establish proof of identity.

Starting in 1996, the ORG partnered with the Land Registry Offices (LROs), also part of the ministry, to deliver ORG services in fourteen communities. The LROs acted as ORG agents in issuing certificates, and also provided same day service. According to the Ministry, about 60% of the applications for certificates were processed through the mail while 40% were processed on the premises by same day service.

Terminology:

To assist the reader, below is a description of some of the types of records referred to in this report:

Request for Birth Certificate (also called Birth Certificate Application) is used by individuals to request proof of birth registration (certificates and/or certified copies) in Ontario. This form contains the personal information of both the individual and the parents – for example, the mother's name, maiden name, date and place of birth, and age at time of this birth; the father's name, date and place of birth, number of siblings.

Birth Certificate is an extract of information from the birth registration: the individual's name, date of birth, birthplace, date of registration, certificate number, sex and registration number.

Birth Registration is the original record registered at the time the event occurred (e.g., parents register the birth of a child within 30 days of birth).

Blank Stock is the paper used for all certificates. It has built-in security features including special bonded paper and controlled numbers.

Statement of Death is in the long form and contains information about the deceased such as name, address, date and place of death, date and place of birth, marital status, name of spouse/partner, and occupation.

Death Certificate is a smaller form and contains only an extract of the information on the Statement of Death.

Request for Service Form (RSF) is the form that is attached to a completed application when it is submitted to ORG for processing. The form is numbered and is used to track the processing of revenue and service delivery. An RSF only has value when attached to the completed application.

Flagging the Registration means adding additional security measures to prohibit the unauthorized processing of a certificate or certified copy of a registration.

RESULTS OF THE INVESTIGATION

In June 2002 the Brampton LRO discovered that 4 blank birth certificates were missing. This discovery came to light because at the start of the day, staff at each office is required to account for the number of blank stock in order to establish end-to-end custody. After further investigation at the Brampton Land Registry Office, it was determined that eighteen completed applications for ORG documents were also missing. The Ministry immediately notified the OPP, who referred the Ministry to Peel Regional Police, who commenced an investigation.

As a consequence, the Ministry initiated an internal investigation at all fourteen Land Registry Offices and the ORG Toronto front counter. All offices were asked to check their completed application files for the past 6 months. As a result, a total of eighty completed birth certificate and other applications were discovered missing from the Brampton, Hamilton and Kitchener offices. The Ministry confirmed that these applications had already been processed and the certificates had been issued to the applicants.

In August 2002, an apparently unrelated incident raised further alarms and the OPP and Peel Regional Police conducted a joint investigation. Through investigative steps taken, they recovered a number of ORG documents, including blank birth certificates and a number of RSFs with completed application forms. An individual was subsequently arrested and convicted of numerous charges, including possession of these stolen ORG documents. The Ministry advises this office that despite the arrest and conviction of the individual, the police investigation into this matter remains ongoing.

Between August 2002 and February 2003, the Ministry's internal investigation focused on several waves of audit activity that resulted in comprehensive set findings. These findings were used as the basis for additional threat risk impact assessments, which subsequently informed the design and development of new security measures and/or controls.

The Ministry undertook yet another audit of all LROs, going back in time to the date that each office started to deliver ORG services. Staff in each office operated in audit clusters and conducted both a manual search of all paper records and a computer search. The Ministry explained that at the time, the computer only had a 6-month memory capacity and at the end of each six-month period, the information was purged and a purge report issued. The purge report contains the names on the certificates, the numbers of the certificates, the fee paid and the mailing addresses; it does not contain all of the information necessary to absolutely determine the names of all individuals affected. Hard copies are retained in the file drawers and then shredded every fifteen months.

This audit confirmed that RSFs with completed applications for ORG documents, such as birth, marriage and death certificates were missing from the offices but a number of these have been recovered by the police.

In December 2002, the Thunder Bay Police and the RCMP charged an ORG employee with a number of offences related to removing tombstone information, removing certificates (birth, death and marriage) and possessing and dealing in documents that purport to establish or could

be used to establish a person's identity (birth certificates, death statements, marriage certificates, change of name documents, divorce and immigration documents). As a result, the Ministry initiated another internal investigation at the Thunder Bay office.

With respect to both the August 2002 and December 2002 incidents, the Ministry notified all individuals by telephone or by mail where possible. The Ministry indicated that it was not possible to notify some individuals who had not been positively identified (given the computer deficiencies noted above), without the risk of further disclosure. The Ministry has provided me with details on the number of individuals notified and those where it was not possible to do so. The Ministry has also provided me with a description of the content of the notices.

The identifiable individuals to whom the information relates have been notified that flags have also been entered against their registrations.

In May 2003, during the scheduled shredding of deactivated certificates, two managers found that 3 birth certificate numbers entered on the log were not in the shredding pile. The Ministry was able to confirm when these birth certificates were returned by the owners because they were old and/or damaged, that the Ministry had defaced them as is their practice, and that they had been deactivated. The individuals to whom the certificates related were notified and flags were also entered against their registrations. The Ministry conducted several searches but the missing certificates were not found.

The Ministry notified our office immediately. They also notified the Passport Office and other agencies that relied on foundation documents and the OPP. The Ministry revised their procedures to address the fact that the chain of custody had been broken.

FINDINGS:

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 **marital or family status** of the individual,

(b) the **address, telephone number,** fingerprints or blood type of the individual,

(c) 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 the investigation, the Ministry confirmed that records including completed birth certificate and other applications, completed birth certificates, copies of birth registrations and death registrations were missing from its offices. The information in these records would include the names, addresses, dates and places of birth, telephone numbers, gender, marital and or family status of the individual together with information relating to the parents of the individual. In the case of the death registrations, the records would also include the date of death.

The information in these records 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.

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 these circumstances apply. The disclosure, therefore, was not in accordance with the *Act*. The Ministry does not dispute this finding.

Were reasonable measures in place to prevent unauthorized access to the records?

Section 4(1) of Regulation 460, made under the *Act*, states that "[e]very 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."

In the summer and fall of 2000, prior to the events leading to this investigation, the Ministry began strengthening security measures at the ORG based upon expert advice.

In December 2000 the Ministry revised the LRO Procedure Manual and distributed it to the LROs and the Toronto and Thunder Bay offices in January 2001. The manual prescribes the procedures and policies governing the collection, retention and delivery of various services and emphasizes the need for verification and accountability at every stage. The manual contains instructions for staff for every aspect of service delivery including forms, when not to issue certificates, computer logging procedures, obtaining verification of applicant, warnings and cautions on when not to issue certificates. In particular, the manual sets out the specific policies and practices for same day service delivery at the LROs and the Toronto and Thunder Bay offices.

The global events of September 11, 2001 triggered a further review of these policies and procedures. This phase is what the Ministry refers to as Generation One of its security and privacy enhancing measures. One of the changes made as a result of the security review was the introduction, in October 2000, of a new application form for birth certificates, which requires more information and the signature of a guarantor. Other changes included limiting and tracking the number of birth certificates issued to individuals; increasing the security of mail-in and fax applications; deactivating certificates reported lost, stolen or destroyed; and reporting and tracking of deactivated birth certificates.

A process was established to enable staff to verify the identity of individuals filing applications. Birth certificates were limited to one per applicant. Returned certificates were deactivated, defaced and shredded, thereby precluding fraudulent use. The process reflects the chain of custody goal (see below). The Ministry explained that it routinely notifies agencies such as the Passport Office, which rely on foundation documents. The Ministry explained that previously, applications and certificates were couriered to and from Thunder Bay in government blue bags; this procedure has now changed. These measures are in addition to those outlined in the manual.

In December 2001, the Legislature amended the *Vital Statistics Act* to include the requirement for a guarantor on every application for a birth certificate. The guarantor had to be a member of a prescribed group such as a judge, provincial police officer, dentist or lawyer and had to have known the applicant for at least two years. Guarantors are contacted and his/her information verified.

Subsequent to the events of August 2002, which led to this investigation, the Ministry stated that it instituted further changes to ensure the security and privacy of the information that it collects and maintains for the people of Ontario. The goal was to ensure a chain of custody from the time that an applicant discloses his/her personal information to the end result - tracking its movement and checking its storage throughout the process where it is stored to the end result. The Ministry explained that the focus was on the need to know where a document is at any given time and that managers are accountable for their department.

One direct impact was the immediate suspension of same day service at the LROs. Others included administrative changes to enhance the security processes for RSFs and other document control; an external security and risk assessment that included a review of the internal audit methodology; changes to the purge report system to include sufficient information to enable it to contact the clients if necessary; and additional staff training on the processing, retention and security of all records. The Ministry has provided details of other internal security measures that were implemented.

The guiding principles underlying all security enhancements are:

1) chain of custody process which requires end-to-end auditing of all documents which are processed and entered into the system;
2) dual custody which ensures there are always two employees present for certain actions – for example, when printing certificates or mail delivery;
3) segregation of duty, which requires separate and distinct staff to complete an action.

The purpose is to fill any gaps in the control and auditing process which is currently in place, and to also implement a monitoring system. The Ministry is working towards building a network of security controls and processes, which will function as an automatic security and privacy audit. A necessary part is the ability to add proactive and reactive components to this network.

To this end, the Ministry will be adding a chief officer qualified to monitor compliance of the process, to respond to breaches and to watch for perceived or potential threats. The Ministry will

also be increasing its ORG investigative resources by adding two investigators who will conduct investigations and will perform an educational function by raising staff awareness at all the offices.

A new high security computer system with programs to facilitate end-to-end custody will be in place in August 2003. The new computer will also retain a permanent record of all certificates issued. Special security clearances for staff and improved access cards are among other measures being contemplated by the Ministry.

A special team conducted a Threat/Risk Assessment review with a view to formalizing a governance structure and partnership between the Ontario Registrar General's offices and the LROs, by way of a Memorandum of Understanding that will speak to a common cultural understanding of the extreme importance of security and privacy relating to the protection of personal information.

I have reviewed the Ministry's Policy and Procedures manual together with the procedures that it has implemented since September 2001. I have also reviewed all of the additional measures that the Ministry is contemplating. I note that all of the changes have been clearly defined and documented and that copies of the manual and the addendums have a very limited distribution and are required to be kept securely.

I find that the Ministry has ensured that reasonable measures to prevent unauthorized access have been defined, documented and put into place, taking into account the nature of the records to be protected. It is important to note that well before these events, the Ministry recognized its duty to protect personal information and proactively reviewed its measures to prevent unauthorized access.

I think it is fair to say that criminal activity is not contemplated in the concept of "reasonable measures;" rather, criminal activity is viewed as an exceptional circumstance. The implementation of reasonable measures is not an ironclad guarantee against criminal activity. However, in recognition of the seriousness of these recent events, the Ministry rightly continues to enhance and refine the measures already in place. The disclosure of personal information in violation of the *Act* is a serious matter at all times. In the current environment where identity theft and fraud are becoming increasingly prevalent, the disclosure of information that can be used to obtain foundation documents is a matter of particular concern. It is expected that the significant refinements and changes that the Ministry is making in this area will allow it to position itself in the forefront of "reasonable measures."

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 appreciates the seriousness of the matter and has given considerable thought and priority to taking immediate and appropriate actions.

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

1. Highly sensitive personal information of a 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 notification provided to the individuals about the disclosure in question. 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, the Ministry notified those whose identities they could confirm, and took care to obtain further verification where necessary in order to avoid further inadvertent disclosure.

3. Reasonable security measures were in place prior to the events leading to this investigation report, and those measures continue to be enhanced.

RECOMMENDATION(S):

As indicated above, the Ministry has made a series of privacy protective security enhancements, and continues to do so. Some of the "next generation" enhancements are items that the Ministry already has approval to implement (for example, the creation of the investigator position), while other initiatives rely on government-wide approval (for example, staff security clearances). We recognize that initiatives requiring government-wide approval are not solely within the Ministry's control. In light of this, my recommendations focus on those that are within the Ministry's control, and are as follows:

1. I recommend that the Ministry implement all measures currently underway that are within its control.

2. I recommend that the Ministry ensure that these measures are adequately reflected in their policies and procedures.

3. If the Ministry is considering video surveillance or any other measures that could have a significant privacy impact, I urge the Ministry to consult with this office, at the earliest opportunity, to arrange for a process of input and review.

4. I recommend that before same day service is resumed in the LROs, the Ministry ensure that staff is fully trained in all the policies, practices, procedures, as well as the values of the Ministry to ensure the security of personal information.

5. I recommend that the registrations of all individuals whose documents are not accounted for, be flagged indefinitely, since the prospect of identity theft is not time-limited.

By **October 18, 2003** the Ministry should provide the Office of the Information and Privacy Commissioner with proof of compliance with the above recommendations.

Original signed by: July 18, 2003

Ann Cavoukian, Ph.D.
Commissioner