ALBERTA

INFORMATION AND PRIVACY COMMISSIONER

INVESTIGATION REPORT # 2001-IR-001

INTO

ALBERTA CHILDREN'S SERVICES

March 22, 2001

Introduction

On Saturday, March 17, 2001 and Sunday, March 18, 2001, newspaper articles reported that an individual received two e-mails from a regional office of Alberta Children's Services (the "Public Body") that contained personal and sensitive information relating to children.

In view of the seriousness of the matter, on Monday, March 19, 2001, the Commissioner ordered an investigation under the *Freedom of Information and Protection of Privacy Act* (the "Act"). This report outlines the findings and recommendations of the investigation conducted by this office.

The Breach

The individual reported in the newspaper articles (hereafter referred to as the "Unintended Recipient") was contacted and confirmed he received two e-mails from the Public Body at his personal e-mail address.

According to his recollection, he received the first e-mail on Monday, March 12 or Tuesday, March 13, 2001. The e-mail contained the name and title of the employee of the Public Body (the "Employee"), the Employee's e-mail address and the name of the regional office (the "Regional Office"), which was not the Lac La Biche office as reported in the newspapers.

The e-mail contained three attachments labeled by the child's first and last name. The Unintended Recipient said each attachment consisted of a "Placement" form containing the child's personal information, including reason for the placement.

The e-mail was addressed to 10 agencies. The only similarity in the e-mail addresses was that the first two characters in the address of one agency were the same as the Unintended Recipient's e-mail address.

Two days later, the Unintended Recipient received a second e-mail from the Public Body. The attachment contained the Placement form for one child.

The Unintended Recipient stated that he did not contact the Public Body. Instead, the Unintended Recipient decided to contact a local newspaper. He copied the two e-mails and attachments to a diskette that he provided to the newspaper.

The Unintended Recipient informed this Office that he made no other copies in any form and had deleted the e-mails from his computer.

Investigation Findings

In January 2001, the Regional Office began using e-mail to facilitate placement of children in an agency foster home, residential or group care. It was explained that the use of e-mail assists in locating appropriate care for children in need. In some situations, there is an urgent need to place a child. In the e-mails giving rise to the incidents, the Regional Office was seeking placements for the children in an agency foster home. This is a foster home that has been screened and approved by an agency that has been accredited by the Public Body.

The process used is as follows:

- A Foster Care Worker employed with the Public Body identifies a child in need of foster care and completes a Placement Intake Screening form (CS 3104) on a computer screen.
- The Placement Intake Screening form is forwarded electronically to a Placement Coordinator, employed by the Public Body, who identifies accredited agencies that are involved in the provision of foster care.
- The Placement Coordinator e-mails a message to the agencies to inquire if there is an opening and attaches the Placement Intake Screening form.
- Each agency determines whether it has a foster home that is appropriate to meet the needs of the child and advises the Public Body by e-mail if it has a placement.

There is no process in place to confirm that an Agency received an e-mail. Some agencies will notify the Regional Office that they have no placements available. Some agencies do not respond if they do not have an available placement.

The Regional Office had no information with respect to whether any agency was forwarding e-mail or attachments from the Public Body to foster care home providers.

The Placement Intake Screening Form contains the following personal information: name, gender, date of birth, ethnic origin, legal status, circumstances that brought the child into care, descriptions of behaviors and mental and physical health information. In addition, information

regarding the history of the child may be included, such as involvement with prostitution, sexual acting out, fire starting, verbal and physical aggression, etc.

The Regional Office agreed it was not necessary to disclose the name of the child or all personal information when making a placement inquiry to the agencies. The Regional Office agreed that for an initial inquiry on availability, anonymous information would be sufficient in most cases.

The Regional Office stated it began use of e-mail after becoming aware another regional office of the Public Body was using e-mail to facilitate placements. The Regional Office acknowledged that a Privacy Impact Assessment had not been done and that the Public Body's FOIP Coordinator had not been consulted.

To date, the Regional Office had used e-mail for placement approximately 12 times.

It was confirmed that the first e-mail and three attachments the Unintended Recipient erroneously received, were sent by the Regional Office on Tuesday, March 13, 200l.

It was confirmed that the second e-mail with one attachment that the Unintended Recipient erroneously received was sent by the Regional Office on Thursday, March 15, 2001.

The Employee, who sent the e-mails, had developed a distribution list of accredited agencies that provide care. The Employee had previously typed the e-mail addresses of the agencies into a distribution list.

Both e-mails were addressed to the same 10 agencies. All the e-mail addresses are the same on both e-mails. The Employee used a distribution list and therefore did not individually type in the e-mail address. The same distribution list was used for both e-mails.

On February 16, 2001, the Employee e-mailed the 10 agencies without any apparent problem.

The Employee reported that between February 16 and March 13, an unexplained change had occurred in the e-mail address of one agency in the distribution list. The change involved the removal of the first four characters of the agency's e-mail address. The remaining two characters are the same as characters in the Unintended Recipient's e-mail address. The Employee reported that no one else had access to the distribution list or was known to have made a change to the e-mail addresses in the directory.

Some of the agencies on the distribution list have their own mail servers. This means that an e-mail from the Public Body is received at the agency's mail server.

A few of the agencies do not have their own server and use an Internet Service Provider. This means the e-mail goes from the Regional Office to the Internet Service Provider and then is routed to the agency.

The investigation included a site visit to the Regional Office with a Systems Analyst from the Commissioner's Office. Tests were conducted to identify if the breach originated or was caused

by the Regional Office. In addition, the computer logs and tests results provided by the Public Body were reviewed to determine the electronic trail of the e-mails.

Tests confirmed that one agency on the distribution list did not receive the March 13 and March 15 e-mails. This is the same agency that the Employee had noted an unexplained e-mail address change. The review showed that this agency does not have its own server. It uses the same Internet Service Provider as the Unintended Recipient.

The results of the review of computer logs provided by the Public Body showed that the Internet Service Provider received an e-mail from the Regional Office on March 13th that was for an incorrect, non-existent e-mail address. Subsequent e-mail tests by the Public Body, and confirmation with the Internet Service Provider, indicates that the incorrect e-mail address was then misdirected to the Unintended Recipient. It appears that the Internet Service Provider sent the incorrectly addressed e-mail from the Public Body to an e-mail address with the closest matching prefix, which happened to be that of the Unintended Recipient.

The Public Body informed this Office that it was advised that it is the usual practice of that private Internet Service Provider to route e-mails to the address with the closest prefix.

Steps Taken By the Public Body

The Public Body took immediate steps to investigate the breach prior to being contacted by this Office. The investigation included a systems analysis.

At the direction of the Commissioner, the Public Body immediately ceased the practice of using e-mail for foster care, residential or group placement of children. The Public Body is conducting a review of use of e-mail and will be developing a policy. In the interim, the Public Body issued a reminder to employees to share only the minimum amount of confidential information when it is absolutely essential.

The Public Body reported that it has contacted the families/guardians of the children whose personal information was disclosed. It has also contacted the Unintended Recipient who allowed the Public Body to access his computer to ensure the files were removed from the hard drive.

Conclusions

The Act places a duty on public bodies to ensure that personal information is secure and not improperly disclosed.

The Public Body acknowledges that an unauthorized disclosure of sensitive and confidential personal information occurred.

Based on the evidence, it is concluded that the breach was originally caused by an incorrect e-mail address in the distribution list.

This error was compounded by the fact that the addressed agency used an Internet Service Provider. Typically, an incorrect address would be returned to the sender. However, in this situation, the evidence shows that the Internet Service Provider forwarded the e-mail to a subscriber with a similar prefix. In other words, the Internet Service Provider's computer, when faced with an incorrect address, routed the Regional Office's e-mail to another subscriber with a similar address.

Recommendations

1. The Public Body must first define what personal information, if any, needs to be disclosed when making inquiries to agencies for placement.

2. When sending out personal information, only the minimal amount of personal information necessary should be disclosed.

3. When sending out personal information, personal identifiers should be removed whenever possible.

4. The Public Body must include a statement on e-mail transmittals that clearly states that individuals receiving e-mails in error must notify the Public Body immediately and that the information must not be used or disclosed in any manner.

5. The Public Body must establish security measures to protect personal information from unauthorized use, collection and disclosure. The Public Body may wish to consider security measures such as:

    - Develop policies and procedures regarding the use of e-mail for placement such as standardizing e-mail to be directed to a specific individual within each agency; checking directories and e-mail addresses on a continual basis to ensure the address is correct and current; requiring that agencies confirm receipt of e-mail, etc.

    - Ensure contractual agreements with agencies include clauses that agencies must protect personal information received from the Public Body, from unauthorized use, collection and disclosure.

    - Require that agencies establish clear policies for their employees regarding access, use and disclosure of personal information received from the Public Body.

    - Require that agencies conduct an assessment of risk associated with the use of Internet Service Providers.

Valerie Kupsch
Portfolio Officer