ALBERTA
INFORMATION AND PRIVACY COMMISSIONER

Report on Investigation into the Practice of Applicant Identity Verification

September 12, 2006

Edmonton Police Service

Investigation #3532

Investigation Report F2006–IR-02

I. INTRODUCTION

[1] On December 30, 2005, a lawyer complained that the Edmonton Police Service ("the EPS") requested his client provide photographic identification to EPS prior to the release of records responsive to an access request made by the lawyer on behalf of the client.

[2] In response to this complaint, the Commissioner initiated an investigation on January 11, 2006. The investigation is on the Commissioner's own motion under section 53(1)(a) of the Freedom of Information and Protection of Privacy Act ("the FOIP Act"), which authorizes the Commissioner to conduct investigations to ensure compliance with any provision of the FOIP Act.

II. ISSUES

[3] The issues of this investigation are:

i) Is the practice of the EPS to require photographic identification from applicants consistent with the FOIP Act, specifically section 38?
ii) Is the collection of personal information consistent with section 33 of the FOIP Act?

III. FINDINGS AND ANALYSIS

A. General

[4] This investigation involved interviewing Ms. Bonnie Bokenfohr, the EPS Legal Advisor and FOIP Coordinator, and the review of a submission detailing the development and implementation of the practice.

[5] Ms. Bokenfohr advised the following:

- That in order to ensure the confidentiality of applicants' access requests and to ensure that EPS records are provided only to the individual to whom they relate, the EPS FOIPP Unit requires applicants to present identification to verify identity before releasing records.
- On December 15, 2005, the EPS FOIPP Unit adopted the practice that individual applicants whether appearing in person, making their request by mail, or being represented by a third party had to verify their identity by providing two pieces of valid identification, including one piece of valid photo identification. The information contained in the identification, including name and identification number, would be recorded prior to the release of the records.
- Occasionally, the EPS FOIPP Unit will be confident that the records relate to the applicant based on conversations with the applicant either in person or over the phone and the applicant's knowledge of the records requested. In such a circumstance, the EPS FOIPP Unit may consider sending the records via registered mail without presentation of identification or obtaining photocopies.

[6] During the course of this investigation, the EPS agreed to alter its practice. The EPS indicated that the amended practice would be:

- If an applicant attends at a police facility to pick up their records, they will be required to present two pieces of identification, one of which must be photo identification. The member releasing the records shall confirm that they have viewed the identification and note the type of identification viewed but will NOT record the identification numbers from the pieces of ID.

- If an applicant requests that their records be forwarded to them by mail, or if the request is received as made on behalf of the individual to whom the information relates (this includes lawyers making requests for clients), the individual to whom the personal information relates will be given the option of attending at a police facility to pick up their records OR sending photocopies of identification (one of which must be photo identification). Photocopies of identification received shall be retained on the file related to the applicant's FOIPP request. FOIPP files are retained as per the EPS retention schedule. This accommodates the requirement of s. 35(b) of the FOIP Act that public bodies retain personal information for at least one year after using it to make a decision that directly affects the individual.

B. Issue (i) - Is the practice of the EPS to require photographic identification from applicants consistent with the FOIP Act, specifically section 38?

[7] The FOIP Act is silent on specific requirements of identity verification for the processing of a FOIP Access Request.

[8] Section 7(1) of the FOIP Act establishes that "a person must make a request to the public body that the person believes has custody or control of the *record*."

[9] Section 7(2) establishes the basic requirements for the submission of an access request:

> 7(2) A request must be in writing and must provide enough detail to enable the public body to identify the record.

[10] Section 38 states:

> 38 The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

[11] Disclosing personal information about the "applicant" to someone who is not the "applicant" is a potential unauthorized access / disclosure.

[12] In order to meet the responsibilities of section 38, it is reasonable to expect that public bodies must take steps to ensure that applicants requesting their own personal information confirm they are the person who made the request for access. In evaluating the possibility of risk under section 38, a public body needs to consider factors such as:

> a) the sensitivity of the information;
> b) the possibility of the information being misused, for example, does it have a financial or other value; or
> c) the possibility of the information being disclosed to others.

In that regard, personal information in the custody / control of the EPS would be at a high risk and the obligation of the EPS proportionately high.

[13] The practice of requiring identification of the applicant before the release of records containing the applicant's personal information is consistent with section 38, in that it constitutes making reasonable security arrangements against the risk of unauthorized access / disclosure.

C. Issue (ii) - Is the collection of personal information consistent with section 33 of the FOIP Act?

[14] The amended practice only requires collection of personal information for records requested by mail. The EPS practice requires that photocopied identification be mailed in to the EPS FOIPP Unit. The photocopy of the identification is retained on the applicant's FOIP file.

[15] EPS stated that the FOIP files are maintained in the same manner as any other record in the EPS, with respect to security, use, retention and destruction and the files are subject to the FOIP Act.

[16] Section 33(c) authorizes the collection of personal information if it is related directly to and is necessary for an operating program or activity of the public body. The processing of FOIP requests is an activity of the EPS.

[17] In accepting photographic copies by mail the EPS is collecting this information in the form of a record. In order to process the access request by mail and ensure that they have taken reasonable security measures, EPS must collect this photocopied identification. This collection therefore would be related directly to the activity of processing the FOIP access request and would be reasonably necessary to ensure the security of the process in accordance with section 38. As such, the collection would be permissible under section 33(c).

IV. CONCLUSION

[18] I find that the amended EPS practice is consistent with section 38 of the FOIP Act as it is a reasonable security arrangement to protect the personal information of individuals from inappropriate access / disclosure. I also find that the amended EPS practice of collecting the photocopied identification is allowed under section 33(c) of the FOIP Act.

V. RECOMMENDATIONS

[19] Although I have found the EPS practice to be consistent with the FOIP Act, I would make the following recommendations to ensure that it is applied appropriately. I recommend the following actions be taken by the EPS:

i) That the practice be formalized as a policy and be written and available for individuals to review.
ii) That the personal information collected be used only for the stated purpose of that collection or as authorized by the FOIP Act and that the written policy state that.

Submitted by,

Richard Marks
Portfolio Officer