

**ALBERTA  
INFORMATION AND PRIVACY COMMISSIONER**

**Report on Investigation Regarding Disclosure of Personal Information**

**March 19, 2007**

**Calgary Police Service  
(Investigation #F3844 and 3849)**

**I. INTRODUCTION**

[1] On October 12, 2006, the Commissioner's office received a privacy complaint against the Calgary Police Service ("the Public Body"). The Complainant says certain employees accessed the Complainant's personal information in the Public Body's database without the Complainant's authorization. In response to the complaint, the Commissioner opened investigation file #F3844.

[2] Subsequently, on October 16, 2006, the Commissioner's office received a second complaint from the Complainant against the Public Body. The Complainant said the Public Body's FOIP office breached privacy by disclosing the Complainant's personal information. Investigation file #F3849 was opened.

[3] Section 53(2)(e) of the *Freedom of Information and Protection of Privacy Act* ("the FOIP Act") allows the Commissioner to investigate complaints that personal information has been collected, used or disclosed in contravention of Part 2 of the FOIP Act. The Commissioner authorized me to investigate these complaints. This report outlines the findings and analysis of my investigation.

**II. BACKGROUND**

[4] The Complainant is employed with the Public Body. The employees who allegedly accessed the Complainant's personal information are co-workers of the Complainant in the same operational unit. The Complainant and the other employees are authorized to access the Public Body's databases.

[5] The Complainant had applied to the Public Body under the FOIP Act for access to information, "*including the names of internal employees who had made enquiries on our internal Police Information Management System of me*".

[6] The Public Body processed the Complainant's access request and released records responsive to the Complainant's access request. As a result of the access request, the Complainant found that seven employees in total had searched the Public Body's database running the Complainant's name. The Complainant then filed a complaint with this office.

[7] The Complainant questioned why these employees had queried the Complainant's information on the Police Information Management System ("the PIMS"). The Complainant says the employees breached the Complainant's privacy when they accessed information about the Complainant in the PIMS without authorization. The Complainant also says the Public Body failed to protect the personal information in the PIMS against unauthorized access, use and disclosure.

[8] Subsequent to processing the Complainant's access request, the Public Body's FOIP Office conducted an audit as to queries made by the employees on its PIMS. The Complainant filed a second complaint with our office alleging that the Public Body's FOIP Office breached privacy by releasing the Complainant's personal information to these employees.

### **III. ISSUES**

[9] The issues for Investigation #F3844 are:

- Was there an unauthorized access of the Complainant's personal information?
- Did the Public Body fail to protect the Complainant's personal information in contravention of Part 2 of the FOIP Act?

[10] The issue for Investigation #F3849 is:

- Did the Public Body disclose the Complainant's personal information in contravention of Part 2 of the FOIP Act?

### **IV. INVESTIGATION #F3844**

#### **1. General**

[11] The FOIP Act places a duty on public bodies to protect personal information against such risks as unauthorized access, collection, use and disclosure (section 38 of the FOIP Act).

[12] The Complainant and the employees subject to the complaint are employees authorized to access the Public Body's databases. PIMS is accessible through the Public Body Intranet and includes access to a number of databases:

- **UNIQ** A universal query of Public Body files.
- **IDEN** Information from an Identification Unit database.
- **VREG** The motor vehicle database providing personal information of registered owners for vehicles including home telephone numbers.
- **CASE** A database containing occurrence and investigation reports.
- **INET** An intelligence database.
- **SUMN** Provides information on summonses.
- **CPIC** is also available through the PIMS system or through another access point on the Communications Officers' systems. Access to CPIC is provided through an agreement with the Royal Canadian Mounted Police which requires reporting all unauthorized access.

[13] The Public Body says all employees are informed that access to information in PIMS, CPIC and other Public Body databases is only permitted for law enforcement purposes (which is in accordance with section 39(1)(a) of the FOIP Act). Access or use for personal or private reasons is prohibited.

## **2. Investigation Findings**

[14] The Public Body was asked by our Office to provide a list of the employees who accessed the Complainant's information and the reason why the Complainant's information was accessed.

[15] The results of our investigation conducted on the Public Body employees who accessed the complainants' information were as follows:

- Employee 1 - can not recall why the Complainant's personal information was accessed 3 times in 2000 and 2005. The employee explains that perhaps it was due to approving a report regarding an illegally parked vehicle or approving, a PNOT (an automatically-generated action - request). (Complainant states that this employee was not involved in this report and that it was an unauthorized access.)
- Employee 2 - accessed Complainant's information 5 times in 2001 as it was necessary to perform legitimate law enforcement duties; regarding a Human Rights Complaint and Grievance.

- Employee 3 - accessed Complainant's information once in 2006 as it was necessary to perform legitimate law enforcement duties; for security investigation file.
- Employee 4 - accessed Complainant's information once 2001 as it was necessary to perform legitimate law enforcement duties; for a grievance/complaint.
- Employee 5 - accessed Complainant's information twice in 2001 as it was necessary to perform legitimate law enforcement duties; needed to obtain home phone number for appointment scheduling purposes or in relation to grievance/human rights complaint.
- Employee 6 - accessed Complainant's information once in 2001 as it was necessary to perform legitimate law enforcement duties; for CIPC/property file.
- Employee 7 - accessed Complainant's information once in 2001 but does not recall the reason.

[16] Based on the above, it is my opinion that certain employees of the Public Body accessed the complainant's personal information inappropriately. The response that they cannot remember why they made the query is in my opinion an insufficient reason.

[17] The investigation then reviewed whether the Public Body failed to protect the Complainant's personal information from unauthorized access, use and disclosure as required under section 38 of the FOIP Act.

[18] The Public Body says it has implemented the following measures to protect personal information contained in its databases:

- **Employees are required to take and sign an Oath of Allegiance:**

"I...solemnly and sincerely swear that I...will not, without due authority in that behalf, disclose or make known any matter that comes to my knowledge by reason of my employment."

"I accept that if I disclose or make known any matter that comes to my knowledge by reason of my employment whether material or otherwise I will be subject to immediate dismissal from the employment of the City of Calgary."

- **Log on Screen**

The Public Body Intranet has a log on screen stating that the user acknowledges that they are aware of the Information Technology Policy and the Investigation Policy.

- **The Public Body's Information Technology Policy**

The Information Technology Policy provides:

Members may be required to justify their use of Public Body IT resources.

Access to information contained in PIMS, CPIC and other Public Body data bases is permitted only for purposes necessary to the efficient discharge of legitimate law enforcement duties. Access or use for personal or private reasons is prohibited.

Public Body IT resources will be used only in a manner that safeguards the confidentiality, integrity, availability, security, reliability and privacy of Public Body information systems and networks, and are consistent with the Service's Core Values."

- **CPIC Policy**

The CPIC Policy provides:

Access to CPIC is permitted only for purposes necessary to the efficient discharge of legitimate law enforcement duties. Access or use for personal or private reasons is prohibited."

- **The Public Body's FOIP Policy**

Access to information contained in PIMS, CPIC and Public Body data bases is permitted only for purposes necessary to the efficient discharge of legitimate law enforcement duties. Access or use for personal or private reasons is prohibited by the Public Body.

[19] If an employee cannot remember why they searched someone, the Public Body says it will look at the name and relationship of the two parties to determine if the search was for law enforcement or personal reasons. The Public Body will question the circumstances of the search and if there is suspicion of personal use.

[20] In my view, the Public Body has made reasonable security arrangements to protect personal information in its databases against such risks as unauthorized access, collection, use and disclosures as required under section 38 of the FOIP Act.

## **V. INVESTIGATION #F3849**

### **1. General**

[21] The Complainant's second complaint relates to an audit conducted by the Public Body's FOIP Office. The Complainant had questioned the Public Body as to why the employees had searched the Complainant's name in the PIMS.

[22] The Public Body's FOIP Office wrote to the employees who had queried the Complainant's name on the PIMS and asked each employee to provide the reason for their query. The Complainant says the Public Body should not have released the Complainant's personal information to these employees.

### **2. Investigation Findings**

[23] The Public Body's FOIP Office is authorized to conduct audits relating to searches made by employees on the Public Body's databases. In conducting its audit, the Public Body's FOIP Office sent each employee a computer printout listing the searches conducted by that employee. The computer printout contained the following data elements: the database that was searched (e.g. CASE), an Identifier number, Date of the search, Time of the search, User number and name of person searched.

[24] I find that the computer printout contained information about identifiable individuals and therefore, the information is "personal information" as defined by section 1(n) of the FOIP Act.

[25] The computer printout is a compilation of the searches conducted by employees for the purpose of ensuring that personal information in the Public Body's databases is accessed for the purpose of law enforcement and in accordance with established policies and procedures.

[26] The Complainant had questioned as to why fellow employees searched the Complainant's name on its databases. The Public Body's FOIP Office was reviewing this matter. The disclosure of the computer printout listing the searches made by that employee is part of the Public Body's review and determination on whether the searches were for law enforcement purposes.

[27] As the disclosure is for the purpose for which that information was compiled, I find that the disclosure is allowed under section 40(1)(c) of the FOIP Act, which states:

40(1) A public body may disclose personal information only

(c) for the purpose for which the information was collected or compiled or for a use consistent with that purpose.

[28] I also find that the disclosure of the computer printout listing the searches conducted would have been allowed under section 40(1)(x) of the FOIP Act [disclosure for the purpose of managing personnel of the Public Body]. The employees are authorized to access the Public Body's databases as part of their employment duties. The Complainant's complaint to the Public Body that these employees may be accessing the databases inappropriately is a performance issue, which is part of the Public Body's management of its employees. Therefore, the disclosure of the computer printout to determine whether the complaint is valid is part of the Public Body's management of its employees.

[29] I also find that the disclosure was limited to the extent necessary as required under section 40(4) of the FOIP Act.

## VI. CONCLUSIONS AND RECOMMENDATIONS

[30] Based on the above, it is my opinion that certain employees of the Public Body accessed the complainant's personal information inappropriately. It will be up to the Public Body as to how they wish to deal with these employees. However, I conclude that the Public Body has now made reasonable security arrangements to protect personal information in its databases against such risks as unauthorized access, collection, use and disclosures as required under section 38 of the FOIP Act (Investigation #F3844).

[31] I also conclude that the Public Body disclosed personal information in accordance with section 40(1)(c), section 40(1)(x), and section 40(4) of the FOIP Act (Investigation #F3849).

[32] However, I believe the following recommendations may be helpful to further ensure personal information in the Public Body's databases are used for law enforcement purpose only:

1. Regular spot audits should be conducted to ensure employees are accessing the Public Body's databases for law enforcement purposes.

2. Employees accessing PIMS should be required to enter the reason for access (as is done with CPIC inquiries). If the present PIMS does not have this capability, then the Public Body may wish to consider adding this capability to the PIMS.
3. Employees leaving their database terminals for any period of time should always log off and allow their relief to log back on under their own user ID.
4. Further training to remind employees of their obligations regarding appropriate access to the Public Body's databases.
5. Public Body may wish to modify the Oath of Allegiance to include, not only disclosure of any matter but also accessing any matter that is not required for the completion of duties with Public Body.

[33] In my opinion this case can now be closed.

Submitted by,

Frank Borsato  
Portfolio Officer