ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2012-07

April 20, 2012

CALGARY POLICE SERVICE

Case File Number F5542

Office URL: www.oipc.ab.ca

Summary: The Complainant was a civilian employee with the Calgary Police Service ("Public Body"). In March 2010, the Public Body's HR consultant was informed by the Complainant's manager that several of the Complainant's coworkers had made allegations about the Complainant's behavior at work, including allegations of inappropriate sexual conduct.

The Public Body began to monitor the Complainant's computer activities, as well as reviewing her past work email activity. While reviewing her work email, the IT Security Manager ("IT Manager") found a personal email that the Complainant had sent to a family member, which included the login ID and password information for the Complainant's personal web-based email account. The IT Manager used this information to access the Complainant's personal email account and found photographs of a sexual nature, which appeared to have been taken on the Public Body's premises. The IT Manager copied these photographs, and provided them to the Complainant's manager and the HR consultant. These photographs were used in the Public Body's decision to terminate the Complainant's employment, and were also used by the Public Body during the subsequent grievance process.

The Complainant made a complaint to this office, stating that the Public Body collected, used, and disclosed her personal information in contravention of Part 2 of the *Freedom of Information and Protection of Privacy Act* ("FOIP Act"). Specifically, the Complainant objected to the Public Body accessing her personal email account, and the subsequent

collection, use, and disclosure of photographs found by the Public Body in that email account.

The Public Body argued that the collection of the Complainant's personal information occurred during the course of investigating the allegations of workplace misconduct against the Complainant, and that the subsequent use and disclosure of the photographs found in the Complainant's personal email account were for the same purpose as they were collected.

The Adjudicator found that the Public Body collected the Complainant's login ID and password to her personal email account in the course of reviewing the Complainant's work email, to which the Complainant did not object. However, Adjudicator found that the *use* of the Complainant's personal email login ID to access the Complainant's personal email was not for the purpose of employee management, since the IT Manager had not been requested to monitor the Complainant's personal email, rather only her work email. There was also no evidence of wrongdoing that would justify accessing a personal email account. The Adjudicator also noted that even were the use of the Complainant's personal information for the purpose of the workplace investigation, a Public Body may only use personal information to the extent necessary to carry out its purposes *in a reasonable manner*; logging in to the Complainant's personal web-based email account was exceptionally invasive, and patently unreasonable in the circumstances.

The Adjudicator found that the collection of the photographs from the Complainant's personal email account could not be considered separately from the fact that they were collected from the Complainant's personal email account. Because the photographs, even if relevant to the workplace investigation, were found as a result of an unauthorized *use* of personal information, their collection and subsequent use could not be justified as "necessary" for the purpose of the Public Body's investigation.

The Adjudicator determined that the Complainant's personal information was not disclosed to, but rather used by, various employees of the Public Body. The Adjudicator had already determined that the use was not authorized under the Act, but found that even if the personal information had been disclosed to the employees, the disclosure would not have been authorized, for similar reasons.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, ss. 1, 33, 34, 39, 40, 72.

Authorities Cited: AB: Orders 98-002, 2001-038, F2005-003, F2006-018, F2010-036.

I. BACKGROUND

[para 1] The Complainant was a civilian employee with the Calgary Police Service ("Public Body"). In March 2010, the Public Body's HR consultant was informed by the Section Commander (the Complainant's manager) that several of the Complainant's coworkers had made allegations about the Complainant's behavior at work, including that

the Complainant had (several months prior to the allegations) bragged about a sexual encounter with an officer at work; the officer was also employed by the Public Body.

[para 2] The Public Body's HR consultant opened a workplace investigation. She also advised the Professional Standards Section ("PSS") of the allegation of sexual misconduct between a civilian employee and an officer. The PSS investigator informed the HR consultant that PSS was already conducting an unrelated investigation of the officer involved, and that email correspondence of a sexual nature between the officer and the Complainant had been found.

[para 3] The Public Body began to monitor the Complainant's computer activities, as well as her past work email activity. While reviewing her work email, the IT Security Manager ("IT Manager") found a personal email that the Complainant had sent to her brother-in-law, which included the login ID and password information for the Complainant's personal web-based email account. The IT Manager used this information to access the Complainant's personal email account and found photographs of a sexual nature, which appeared to have been taken on the Public Body's premises. The IT Manager copied these photographs and provided them to the Section Commander and the HR consultant. These photographs were used in the Public Body's decision to terminate the Complainant's employment, and were also used by the Public Body during the subsequent grievance process.

[para 4] The Complainant made a complaint to this office, stating that the Public Body collected, used and disclosed her personal information in contravention of Part 2 of the *Freedom of Information and Protection of Privacy Act* (FOIP Act).

II. INFORMATION AT ISSUE

[para 5] The information at issue consists of the login ID and password of the Complainant's personal email account and the photographs of the Complainant collected from her personal email account.

III. ISSUES

[para 6] Per the Notice of Inquiry, dated July 12, 2011, the issue in this inquiry is:

1. **Did the Public Body collect, use and/or disclose the Complainant's personal information in contravention of Part 2 of the Act?**

I will address this issue in three parts:

A. Did the Public Body collect the Complainant's personal information in contravention of Part 2 of the Act?

B. Did the Public Body use the Complainant's personal information in contravention of Part 2 of the Act?

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

IV. DISCUSSION OF ISSUES

A. Did the Public Body collect the Complainant's personal information in contravention of Part 2 of the Act?

[para 7] Section 1(n) defines personal information under the Act:

> *(n) "personal information" means recorded information about an identifiable individual, including*
>
> *(i) the individual's name, home or business address or home or business telephone number,*
>
> *(ii) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,*
>
> *(iii) the individual's age, sex, marital status or family status,*
>
> *(iv) an identifying number, symbol or other particular assigned to the individual,*
>
> *(v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,*
>
> *(vi) information about the individual's health and health care history, including information about a physical or mental disability,*
>
> *(vii) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,*
>
> *(viii) anyone else's opinions about the individual, and*
>
> *(ix) the individual's personal views or opinions, except if they are about someone else;*

[para 8] Both parties agree that the Complainant's photographs collected from her personal email account are her personal information. Previous orders have stated that an individual's email address is also personal information (see Orders 2001-038, at para. 37 and F2010-036 at para. 66). A login ID for a personal email account (which is usually the email address itself), and the password to that account, are similarly personal information.

[para 9] The Public Body cites section 33(c) as authority for the collection of the Complainant's photographs from her personal email account, and section 34(1)(n) as authority to collect the personal information indirectly. These sections state:

> *33 No personal information may be collected by or for a public body unless*
>
> *...*
>
> *(c) that information relates directly to and is necessary for an operating program or activity of the public body.*

34(1) A public body must collect personal information directly from the individual the information is about unless

...

(n) the information is collected or the purpose of managing or administering personnel of the Government of Alberta or the public body

...

[para 10] The Public Body argues that "any collection of the Complainant's personal information occurred during the course of investigating the allegations of workplace misconduct against the Complainant, which is an operating program of the Public Body." The Public Body cites Order F2005-003, which states that managing human resources is an operating activity of a public body under section 33(c). I agree that section 33(c) encompasses the management of a public body's employees.

[para 11] The Public Body states that during the HR consultant's discussion with PSS concerning the investigation into the Complainant's alleged misconduct, PSS told the HR consultant that the officer allegedly involved in the misconduct was already under criminal investigation. The Complainant argues that by including the information regarding the criminal investigation of the officer in its submission, the Public Body is implying that this was a factor justifying the Public Body's search of her personal email.

[para 12] The Public Body has not indicated that its investigation of the Complainant was in any way related to the criminal investigation. Further, the Public Body has not claimed law enforcement as the authority to collect, use, or disclose the Complainant's personal information at issue.

[para 13] The Public Body performed surveillance on the Complainant's work computer for approximately a week during its investigation into her conduct, and also reviewed emails sent to and from her work email address. Specifically, the HR consultant made a request to the IT Manager to provide the following information:

- PIMS [Police Information Management System] activity report that identifies anybody who has searched the Complainant
- the Complainant's email correspondence
- PIMS activity report that identifies the officer with the Complainant. Please includes [sic] date and times of reports taken
- PIMS activity report that identifies the officer and any other Records Processing Unit call takers

[para 14] According to the IT Manager's affidavit, HR made a follow-up request for live monitoring of the Complainant's computer activity, and a Superintendent with the Public Body requested that the IT Manager check the results to see if there was any communication between the Complainant and the officer.

[para 15] The Public Body submits that these requests were "aimed at gathering evidence of the misconduct that had been alleged by the Complainant's co-workers." In

an affidavit, the HR consultant states that "[t]he purpose in gathering the emails was to determine if they evidenced the sexual misconduct that had been alleged, or any other misconduct of which the Public Body might not yet be aware." The work email search found sexually explicit email correspondence between the Complainant and the officer.

[para 16] The Complainant does not object to the investigation conducted by the Public Body or to the collection of her work email for that purpose, which included the email containing the login ID and password to the Complainant's personal email account. In her submission she states:

> [w]hile I do agree that's [sic] the Calgary Police Service or any other organization, has full rights to "view" any email contained within an employee's work email account, I do not believe that any employer has the right to "view" and then hack into or access an employee's personal email account simply because the data is contained within the employer's internet email space.

[para 17] The main issues are the subsequent *use* of the Complainant's personal email account information to access the email account (since the email account information was *collected* from the Complainant's work email in the course of the Public Body's workplace investigation, to which the Complainant does not object); and the collection, use, and disclosure of the Complainant's photographs found in the personal email account.

[para 18] With respect to the collection of the photographs, the Public Body cites previous orders that stated that a public body's decision with respect to the necessity of information collected for a particular purpose should not be interfered with unless it is patently unreasonable (see Order 98-002 at para. 152 and Order F2006-018 at para. 18).

[para 19] However, the collection of the photographs cannot be considered separately from the fact that they were collected from the Complainant's personal email account. As I discuss below, the use of the Complainant's personal email login ID and password, as well as the use of the photographs found in the personal email account, was highly invasive of her privacy, and I find below that this use was therefore not reasonable for the purposes of the investigation into the Complainant's alleged workplace wrongdoing. Because the photographs, even if relevant to the workplace investigation, were found as a result of an unauthorized use of personal information, their collection cannot be justified as "necessary" for the Public Body's purposes of the investigation that was being conducted in this case. There may be investigations in which such invasive techniques might be justifiable; however, in my view, this is not such a situation. Therefore the collection was not authorized under section 33(c) of the Act.

B. Did the Public Body use the Complainant's personal information in contravention of Part 2 of the Act?

[para 20] The Public Body cited section 39(1)(a) as its authority to use the Complainant's personal information. This section states:

> *39(1) A public body may use personal information only*

> *(a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,*

[para 21] Section 39(4) places further limitations on the use of personal information:

> *(4) A public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner.*

[para 22] The Public Body argued that it used the Complainant's email login ID and password, as well as the photographs found in the personal email account, for the purpose for which they were collected: to manage her employment with the Public Body. More specifically, the IT Manager stated that he was looking for data leakage, and was also requested to look for a link between the Complainant and the officer.

[para 23] In a sworn affidavit, the IT Manager stated:

> When we examined [the Complainant's] email records, we conducted a search for the word "password." [The Public Body's] IT Security does this as a best practice on all email searches because 'password' is one of the keywords in determining if any inappropriate activity, such as intentional or unintentional data leakage outside [the Public Body] or password sharing, has gone on. Passwords found in this manner can be crucial in opening locked files that an employee may be unwilling to provide the password to.

[para 24] The IT Manager goes on to say in his affidavit that

> [a] message, attached hereto as Appendix A, was found in [the Complainant's work] email account. Specifically, it was a message sent to someone outside the [Public Body] containing the login name and password to [the Complainant's] personal email account. This seemed odd because it made us wonder why someone would do this.
>
> In addition to that email, we found a number of messages (sent *internally* with case numbers as the subject) containing snippets of records from our PIMS system (CPS Police Information Management System).
>
> We also found a large number of emails between [the Complainant] and [the officer], who is now resigned from the [Public Body], was known to [the Public Body] IT Security from previous investigations and was suspended at the time. This information, and the additional request by [HR] to record [the Complainant's] screen activity, "We'd like to be able to see exactly what's on her computer at any given point," compelled us to follow the trail onto [the Complainant's] personal email. Our primary concern was [Public Body] data, including confidential personal information of third parties, being leaked to the outside as well as the possibility that the emailed login credentials were a way to offload information to an external contact without a direct trail. Our second concern was to look for further communication between [the Complainant] and [the officer], given that part of the request by [a Superintendent of the Public Body] and [HR] was to look for links between [the Complainant] and [the officer]… We clicked on the first email message that had an attachment icon. Attachments were a priority since they can have larger amounts of data then [sic] a regular email message.

[para 25] The IT Manager seems to have been following protocol to find data leakage risks; however, there is no indication that the Public Body had reason to suspect that the Complainant was leaking data. The IT Manager refers to internal emails sent by the Complainant to coworkers, which contained "snippets of records" from the Public Body PIMS system; the Public Body argues that this gave rise to suspicions of other breaches by the Complainant, including sending sensitive date to external email accounts. The Public Body has not argued that the Complainant breached a workplace policy of the Public Body by sending "snippets of records" internally to coworkers. It has not provided evidence to indicate that these "snippets" contained sensitive information or any other evidence to justify the leap from sending "snippets of records" internally to sending sensitive Public Body information to an external email account. The Public Body was reviewing the Complainant's past emails and her current computer usage, yet has not shown any further evidence to support a suspicion of data leakage by the Complainant.

[para 26] The IT Manager also states that it was strange that the Complainant would email the login ID and password to her personal email account. The Complainant states that she sent this email to her brother-in-law to allow him to access a hockey draft. Perhaps the Complainant did not want to actually access her personal email while at work, which, had she done so, would have allowed her to forward on the hockey draft directly. Regardless, while emailing a login ID and password may be strange or risky, it does not, by itself, indicate that the Complainant is leaking Public Body data to her personal email account. As stated above, the Public Body has not provided evidence, other than the "odd" email, that the Complainant was suspected of leaking Public Body data. Further, if the Complainant were leaking Public Body data to her personal email account, it is somewhat difficult to believe that she would then use her *work email* to provide instructions to a third party on how to access that account.

[para 27] The IT Manager goes on to describe how he came upon the photographs:

> Once inside [the Complainant's] personal [non-Public Body] email account we noticed there were a lot of email messages. We clicked on the first email message that had an attachment icon. Attachments were a priority since they can have larger amounts of data then [sic] a regular email message. This first email message contained two file images that appeared to be self-taken topless pictures, of [the Complainant] in a washroom stall. We were about to move onto the next message but then noticed a checkered green and white pattern, with black trim, found in nearly every [Public Body] washroom downtown (HQ and Admin Building). Specifically, it appeared these photos were taken on [Public Body] property… We immediately copied the files to the IT Security drive in case they would be relevant to [HR]. When we advised [HR] what we had found they indicated the photos would be very relevant to what they needed. We closed [the Complainant's] personal email account with the intention of going back in to look for more information. Unfortunately, when we tried to go back into the account a few days later to finish searching for any data leaks, the password had been changed.

[para 28] In searching for data leakage, the IT Manager opened attachments in the Complainant's personal email account on the basis that attachments can have larger

amounts of data (as opposed to considering factors such as to whom or from whom the messages were sent, or the subject line). Upon opening the photographs of the Complainant, it must have been clear that they did not consist of leaked Public Body data. However, the IT Manager viewed them long enough to recognize the tile work in the background of the photograph. At that point, the IT Manager copied the photographs and closed out of the Complainant's personal email account, without continuing his search for data leakage. It was not until a few days later that the IT Manager decided to go back to the email account and continue looking for evidence of data leakage.

[para 29] In my view, the purpose for using the Complainant's personal email login ID and password information (i.e. accessing the Complainant's personal email account) was not employee management. The IT Manager was not asked to monitor or access her personal email use, only her work email use. There is no evidence that he was led to her personal email because she accessed it from a work computer. Similarly, there is no evidence that he had reason to suspect that the Complainant used her personal email account to leak Public Body data, nor is there any evidence that he was requested to look for data leakage. It might be policy to for IT to check for data leakage whenever a Public Body employee is being investigated for inappropriate email or computer use, but this cannot extend, without cause, to an employee's personal email account. Therefore the use of the Complainant personal email login ID and password by the Public Body was not, in my view, authorized under section 39(1)(a) of the Act.

[para 30] Even if I found the use to have been for the purpose of the workplace investigation, section 39(4) requires a Public Body to use personal information only to the extent necessary to carry out its purposes *in a reasonable manner*. Logging in to the Complainant's personal email is exceptionally invasive, and patently unreasonable in the circumstances.

[para 31] With respect to the photographs collected from the Complainant's personal email account, they were arguably relevant to the workplace investigation into her conduct. However, these photographs were discovered only via the unauthorized use of the Complainant's personal email login ID and password. For this reason, I have found above that the collection of these photographs was not authorized under section 33(c); the use of the photographs is similarly not authorized under section 39(1)(a), for the same reasons.

[para 32] The Public Body passed the photographs from the Complainant's personal email account to the HR consultant, the Section Commander and its labour arbitration advisors. Both the Public Body and the Complainant address this as disclosures of the Complainant's personal information; however, in my view it is more likely a *use* of her personal information under the FOIP Act, as each of these Public Body employees was involved in the investigation or resulting disciplinary action.

[para 33] I have found that both the collection and use of the Complainant's photographs by the IT staff was unauthorized. This finding also applies to the use of the

photographs by any other members of the Public Body, for the same reasons as given above.

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

[para 34] The Public Body cited section 40(1)(c) and 40(1)(h) as its authority to disclose the Complainant's personal information. These sections state:

> *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,*
>
> *(h) to an officer or employee of the public body or to a member of the Executive Council, if the information is necessary for the performance of the duties of the officer, employee or member,*
>
> *...*

[para 35] I have determined above, that when the Complainant's photographs were given to the HR consultant, the Section Commander, and its labour arbitration advisors, this was a use of the Complainant's personal information under the FOIP Act. However, even if this were properly characterized as disclosures, I would have found the disclosures to be unauthorized, for the following reasons.

[para 36] The Public Body also argues that the disclosure to the HR consultant was necessary for the performance of her duties, specifically, to investigate the Complainant's workplace conduct. The Public Body argues that the HR consultant was obliged to consider any and all available evidence concerning the allegations.

[para 37] As I have found that the collection of the photographs was not necessary for the purpose of the investigation into the Complainant's conduct at work, it would be an inconsistent and unreasonable result to find that the disclosure of the photographs to the HR consultant, or any other Public Body employee, was necessary for her to perform that investigation. Although the Public Body did not argue the application of section 40(1)(h) to the disclosure of the photographs to the other employees involved in the investigation and subsequent grievance process, I note that the result would have been the same with respect to those disclosures.

[para 38] I have no evidence that the photographs were disclosed to other employees of the Public Body, or anyone else.

V. ORDER

[para 39] I make this Order under section 72 of the Act.

[para 40] I find that the Public Body collected the Complainant's personal information in contravention of Part 2 of the FOIP Act. I order the Public Body to stop collecting personal information in this manner. As a condition of complying with this order, the Public Body must provide training to staff concerning the appropriate collection of personal information in the course of investigating employment and personnel matters.

[para 41] I find that the Public Body used the Complainant's personal information in contravention of Part 2 of the FOIP Act. I order the Public Body to stop using personal information in this manner. As a condition of complying with this order, the Public Body must provide training to staff concerning the appropriate management of personal information in personnel files.

[para 42] I further order the head of the Public Body to notify me and the Complainant, in writing, within 50 days of being given a copy of this Order, that it has complied with the Order. The notification should include a description of the steps the Public Body has taken to comply with my Order in paragraphs 40 and 41.

Amanda Swanek
Adjudicator