ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2007-028

February 14, 2008

EDMONTON POLICE SERVICE

Case File Number 3621

Office URL: www.oipc.ab.ca

Summary: The Applicant requested records containing his personal information from the Edmonton Police Service (the "Public Body"). The Public Body disclosed some information to the Applicant, but withheld the identities of the authors and recipients of certain emails. The Public Body advised the Applicant that it would not search its electronic backup files.

The Applicant requested that a FOIPP coordinator of the Public Body search for the records, rather than relying on the search conducted by members. In addition, he asked the Public Body to conduct a search of its backup media for deleted emails containing his personal information.

The Commissioner ordered the Public Body to release the personal information it had withheld because the persons were acting in their official capacities when they created the records and, in one case, because the author intended to be identified. The Commissioner found that the Public Body had not completed an adequate search for records and had therefore not met its duty to assist the Applicant. The Commissioner ordered the head of the Public Body to search for the requested records. The Commissioner specified that the search was to include the electronic backup files.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25, ss. 1,10, 14, 17(1)(4)(5), 55, 72, 93

Authorities Cited: AB: Orders 99-032, 2001-016, F2002-024

Cases Cited: *University of Alberta v. Pylypiuk*, 2002 ABQB 22; *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403

I. BACKGROUND

[para 1] On December 5, 2005, the Applicant requested access to the following records under section 7 of the Act:

> …all information regarding myself on all Edmonton Police Service Records including all paper and electronic records, on-line, off-line, archived, held, received or distributed between 1 January 2002 to 1 December 2005. This must include all email messages received or distributed internally or externally. This must also include all records maintained in the executive offices files.

[para 2] On January 18, 2006, the Public Body responded to his access request. The Public Body explained that it had located records containing his personal information, including two emails, from which it was severing personal information belonging to third parties pursuant to section 17 of the Act. The Public Body advised that it was unable to search through its back up files using its normal computer hardware and software and expertise.

[para 3] On March 18, 2006, the Applicant complained to my office that the Public Body had not completed a search of all its electronic records when responding to his access request. In particular, he complained that the Public Body had not conducted an "offline search of email transmissions."

[para 4] On April 10, 2006, the Public Body advised the Applicant that it had located four more pages of emails containing his personal information once an employee, who had been absent at the time of the access request, had returned to the office.

[para 5] I authorized mediation to resolve their dispute. However, as mediation was unsuccessful, this matter was scheduled for a written inquiry.

[para 6] Both parties provided initial and rebuttal submissions.

II. RECORDS AT ISSUE

[para 7] The records at issue in this inquiry are three email documents of one page each with certain personal information severed. In this Order, the email dated February 9 2005 12:31 a.m. is "email 1"; the email dated February 9 2005 8:12 p.m. is "email 2"; and the email dated February 10 2005 2:52 p.m. is "email 3".

III. ISSUES

Issue A: Does section 17 of the Act (personal information) apply to the records/information?

Issue B: Did the Public Body meet its duty to the Applicant as provided by section 10(1) of the Act?

IV. DISCUSSION OF ISSUES

Issue A: Does section 17 of the Act (personal information) apply to the records/information?

[para 8] "Personal information" is defined in section 1(n) of the Act, which states:

> *1(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 9] Section 17 prohibits disclosure of a third party's personal information if the disclosure of personal information would be an unreasonable invasion of personal privacy. It states, in part:

> *17(1) The head of a public body must refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy.*

17(4) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if

(g) the personal information consists of the third party's name when
(i) it appears with other personal information about the third party, or
(ii) the disclosure of the name itself would reveal personal information about the third party,

17(5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including whether

(a) the disclosure is desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to public scrutiny,
(c) the personal information is relevant to a fair determination of the applicant's rights,
(f) the personal information has been supplied in confidence,

[para 10] Section 17 does not say that a public body is never allowed to disclose third party personal information. It is only when the disclosure of personal information would be an unreasonable invasion of a third party's personal privacy that a public body must refuse to disclose the information to an applicant under section 17(1).

[para 11] When certain types of personal information are involved, disclosure is presumed to be an unreasonable invasion of a third party's personal privacy under section 17(4). When determining if a disclosure would be an unreasonable invasion of the personal privacy of a third party, a public body must consider and weigh all relevant circumstances including those set out in section 17(5). In *University of Alberta v. Pylypiuk*, 2002 ABQB 22, the Court commented on the interpretation of what is now section 17. The Court said:

> In interpreting how these sections work together, the Commissioner noted that s. 16(4) lists a set of circumstances where disclosure of a third party's personal information is presumed to be an unreasonable invasion of a third party's personal privacy. Then, according to the Commissioner, the relevant circumstances listed in s. 16(5), and any other relevant factors, are factors that must be weighed either in favour of or against disclosure of personal information once it has been determined that the information comes within s. 16(1) and (4). In my opinion, that is a reasonable and correct interpretation of those provisions in s. 16. Once it is determined that the criteria in s. 16(4) is (sic) met, the presumption is that disclosure will be an unreasonable invasion of personal privacy, subject to the other factors to be considered in s. 16(5). The factors in s. 16(5) must then be weighed against the presumption in s. 16(4).

Burden of proof for s. 17

[para 12] Section 17 has a two-fold burden of proof. A public body has the initial burden to show that section 17 applies to the personal information withheld, pursuant to

section 71(1) of FOIP. The burden then shifts to the applicant to show that disclosure would *not* be an unreasonable invasion of the third party's personal privacy.

[para 13] The Public Body argues that it is required to refuse to disclose the identities of the email authors. It says that as the information is their personal information, it falls under Act s. 17(4)(g), and disclosure would consequently be an unreasonable invasion of those parties' personal privacy under section 17.

[para 14] The three emails were received by the same person; a serving police officer in the Public Body. The Public Body disclosed his identity to the Applicant. The Public Body severed information that would show the senders' identities. The information severed is personal information of those third parties, within the definition of "personal information" in the Act s. 1(n)(i) and (ix). They are identified by name, email address, and in email one, events that would identify by context. Their personal views or opinions are expressed. A small amount of the context information severed in the first email includes information about the Applicant.

Presumptions

[para 15] When information falls under one of the provisions in section 17(4) of the Act, disclosure of the personal information is presumed to be an unreasonable invasion of a third party's personal privacy. The Public Body says the presumption arises in this case under Act section 17(4)(g) where the third parties' names appear with other personal information about them, and I agree. However, as noted above, section 17(4) creates a presumption only. A Public Body must then consider the factors under section 17(5), as these factors may outweigh the presumption.

[para 16] The Applicant argues, based on what has been disclosed to him, that the people who wrote the emails were acting in their official capacities. On that basis, he argues that release of their information would not be an unreasonable invasion of their privacy.

Employee association business

[para 17] The Public Body argues that the severed information in the three emails should not be disclosed. Although the emails were between its members on its email system, it says they communicated in the course of their business as members of an employees' association. It argues they have some expectation of privacy when doing association business. The recipient was the President of the Edmonton Police Association (the Association).

[para 18] The Applicant says that the author of email 2 was not doing Association business. He argues that even if the authors of emails 1 and 3 were engaged in Association business, if they used the Public Body's email system to do that, the records are subject to the Act and should be disclosed to him.

[para 19] On the evidence before me, I find that the communications in all three emails were not made in the course of association business. They were simple information exchanges; members of the Public Body were sharing information and views on the situation unfolding around the position of Chief. In each case the evidence is insufficient to support the Public Body's assertion that this was Association business. The Association President forwarded one of the three emails to his Association email address, two days after he received it. The content, titles used, original addressing, and origin of email "replies" do not otherwise suggest Association business.

[para 20] The Public Body disclosed the identity of the recipient of the emails for the purpose of showing his connection with the Association. I find that the member received all three emails in his official capacity as a serving police officer of the Public Body and that disclosure of his identity was proper for that reason.

[para 21] The Public Body says the content of the emails shows the senders were not engaged in the business of the Public Body. It argues that the emails were sent by employees as private citizens or as members of the Association. In addition, the Public Body argues that the private acts of employees are not the actions of the Public Body under the Act.

[para 22] The Applicant denies that the communications were private. He argues that their content offends the Public Body's Electronic Communications Policy that its staff must observe.

[para 23] The records are in the custody or under the control of the Public Body. Consequently, the Applicant has a right to request them under section 6 of the Act, which I will discuss in greater detail in my analysis of section 10, below. In the present case, the emails in question were authorized by a policy of the Public Body that allows employees to use its domain for personal reasons during work hours. In addition, public bodies can only act through the actions of employees. In Order 99-032, the former Commissioner noted:

> The Act applies to public bodies. However, public bodies are comprised of members, employees or officers, who act on behalf of public bodies. A public body can act only through those persons

In other words, the actions of employees are the actions of a public body. As a result, I find that the senders were acting on behalf of the public body when they sent the emails.

[para 24] I find it is not an unreasonable invasion of those third parties' personal privacy to disclose the information.

[para 25] In *Pylypiuk* (*supra*) Gallant J. explained how section 17(5)(a) should be approached. He said:

> In my opinion, the reference to public scrutiny of government or public body activities in s. 16(5)(a) speaks to the requirement of public accountability, public interest, and public fairness.

The members in question wrote in their official capacity as employees of a public body in accordance with a policy of the Public Body to allow personal use of its email system. I find that disclosure of the emails is desirable for the purposes of subjecting the actions of the Public Body to public scrutiny, as the public body is accountable for the actions of its employees. I find that this is a factor that weighs heavily in favor of disclosure under section 17(5).

[para 26] The author of email 2 sent the email from his personal email address, to a group of elected public officials, at an email address dedicated to citizen concerns in the municipal government, about a current public issue – the process of the competition for a senior police service position. He copied the email to the Association President.

[para 27] In the email he identifies himself as a 25-year member of the Public Body, signs his name with specific reference to his position in the Public Body, and refers to his experience with public duties and accountability in that role. He makes no mention of confidentiality, but requests that his email be forwarded, in its entirety, to various public officials.

[para 28] I find that the author of email 2 intended his identity, associated with that email, to be public. Consequently, the author had no expectation of privacy in relation to the email for the purposes of section 17(5)(f) and it is not an unreasonable invasion of his personal privacy for the Public Body to now disclose it.

Issue B: Did the Public Body meet its duty to the Applicant as provided by section 10(1) of the Act?

[para 29] Section 6 of the Act establishes an applicant's rights to access information. It states, in part:

> *6(1) An applicant has a right of access to any record in the custody or under the control of a public body, including a record containing personal information about the applicant.*
>
> *(2) The right of access to a record does not extend to information excepted from disclosure under Division 2 of this Part, but if that information can reasonably be severed from a record, an applicant has a right of access to the remainder of the record.*
>
> *(3) The right of access to a record is subject to the payment of any fee required by the regulations.*

[para 30] The Applicant therefore has a right to access any of his personal information in the custody of or under the control of the Edmonton Police Service, unless an exception under Division 2 applies to the information.

[para 31] Section 10 of the Act explains a public body's obligations when an applicant makes an access request. It states:

> *10(1) The head of a public body must make every reasonable effort to assist applicants and to respond to each applicant openly, accurately and completely.*
>
> *(2) The head of a public body must create a record for an applicant if*
>
> *(a) the record can be created from a record that is in electronic form and in the custody or under the control of the public body, using its normal computer hardware and software and technical expertise, and*
>
> *(b) creating the record would not unreasonably interfere with the operations of the public body.*

[para 32] Consequently, the Public Body has the onus to establish that it has made every reasonable effort to assist the Applicant. Previous orders of my office have established that the duty to assist includes the duty to conduct an adequate search for records. In Order 2001-016, I said:

> In Order 97-003, the Commissioner said that a public body must provide sufficient evidence that it has made a reasonable effort to identify and locate records responsive to the request to discharge its obligation under section 9(1) (now 10(1)) of the Act. In Order 97-006, the Commissioner said that the public body has the burden of proving that it has fulfilled its duty under section 9(1) (now 10(1)).
>
> Previous orders… say that the public body must show that it conducted an adequate search to fulfill its obligation under section 9(1) of the Act. An adequate search has two components: (1) every reasonable effort must be made to search for the actual record requested and (2) the applicant must be informed in a timely fashion about what has been done.

[para 33] The Applicant argues that the Public Body has not made reasonable efforts to search for the information he requested, and has not conducted an appropriate electronic search. He takes the view that the Public Body has the capacity to search through deleted files. He points to the Public Body's electronic communications policy which states:

> Similarly, e-mails into and out of the EPS net-works are monitored for known virus of high-risk file extensions and inappropriate content; these too are recorded to individual user level by specialist software.

[para 34] Finally, the Applicant argues that the Public Body has not conducted an electronic search for responsive records that may exist in the emails of its executive officers. He contends that requesting members to provide records without more is inadequate.

[para 35] The Public Body argues that it has made every reasonable effort to assist the Applicant. It submits that it made reasonable efforts to search for the records requested by the Applicant. It contends that:

a) The Applicant's request could not be completed using normal hardware and software capabilities of the Public Body.

b) No backups for internal e-mails existed prior to 2004 January.

c) The hours of labour required to conduct the e-mail search requested by the Applicant would be unmanageable by the Public Body and an unreasonable use of public resources.

d) Approximately $50,000 of computing hardware would have to be assigned to complete this specific task, which would be an unreasonable and unmanageable use of public resources.

e) The search would be speculative. Even if members have sent/received emails, if the sender and recipient deleted the e-mails prior to the backup "snapshot" being taken the emails would not be recoverable.

[para 36] The Public Body submitted affidavit evidence to explain how it conducted the search for records. According to the affidavit, the Public Body's FOIPP unit sent out a memo to 32 members requesting responsive records. In addition, the FOIPP unit confirmed with its technology department that while searches of backup electronic records are made occasionally for law enforcement purposes, that these searches are not routine, and would take weeks and weeks of time. The FOIPP unit received records or confirmation that members did not hold responsive records from 31 of the 32 members. The affidavit does not comment on the steps the members took to locate responsive records.

[para 37] The Public Body argues in points a, c, and d of its submissions that it has not searched all the records in its custody or under its control because it would be expensive, difficult, and time consuming to do so. In my view, if a public body could refuse to search on this basis, the effect would be to render an applicant's rights to records under section 6 effectively meaningless.

[para 38] Laforest J, with whom the majority of the Supreme Court of Canada agreed on this point, commented on the purpose of access to information legislation in *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403. He said:

> The overarching purpose of access to information legislation is to facilitate democracy by helping to ensure that citizens have the information required to participate meaningfully in the democratic process and that politicians and bureaucrats remain accountable to the citizenry.

This important legislative purpose would be defeated if a public body could simply refuse to search its records on the basis of cost and labour.

[para 39] The Act recognizes that it can be costly and time consuming for a public body to conduct searches. This is why it allows a public body to charge fees in section 93 and to extend time limits for responding to applicants under section 14.

[para 40] In addition, section 55 allows a public body to ask the Commissioner to authorize it to disregard certain types of requests that would unreasonably interfere its operations. Section 55 states, in part:

> *55(1) If the head of a public body asks, the Commissioner may authorize the public body to disregard one or more requests under section 7(1) or 36(1) if*
>
> *(a) because of their repetitious or systematic nature, the requests would unreasonably interfere with the operations of the public body or amount to an abuse of the right to make those requests, or*
>
> *(b) one or more of the requests are frivolous or vexatious.*

[para 41] Section 55 details the only circumstances in which a public body may disregard an access request. In my view, the Public Body is attempting to disregard a significant portion of an access request, even though the circumstances do not meet the requirements of section 55.

[para 42] The Public Body's argument that it does not have backup records prior to January 2004, is only valid in relation to records prior to that date. The Applicant requested records containing his personal information from January 1, 2002 to December 1, 2005. Clearly, electronic backup records from January 2004 to December 1, 2005 are available and within the scope of the access request.

[para 43] There may be situations where a public body is unable to search or access electronic backup records. In such a case, the public body may establish that it has performed an adequate search for records without searching those records. However, the evidence of the Public Body in this case is that it has the ability to access and search its electronic backup records, but has chosen not to.

[para 44] The Public Body appears to suggest that because it has provided a list of responsive records, the onus now shifts to the Applicant to prove that the records he seeks exist. However, the Public Body has never actually searched all its records. This is not a case where the Public Body has conducted a thorough search of all its records, such that the onus shifts to the Applicant to prove the existence of the requested records it is unable to locate. The Public Body has not yet conducted a search within the meaning of section 10.

[para 45] The Public Body also argues that the search would be speculative. In fact, most requests for records have a speculative element, as an applicant is not in the same position as a public body to know what records it has in its custody or under its control. However, in the present case, the Applicant has provided sufficient detail for the Public Body to identify the records he is seeking. In addition, the Public Body has located emails within the scope of the access request, which indicates that the Applicant's request is not merely speculative. Electronic records meeting the requirements of the access

request therefore exist not only in the computer system, but most probably in the backup files as well.

[para 46] Section 10 places the duty to assist an applicant on the head of the public body, not simply employees of the public body, or the public body in general. As a result, the head, or the person to whom the head has delegated authority, must be in a position to establish that he or she did in fact conduct an adequate search for records as part of the duty to assist an applicant. In a situation where the head or the delegate does not have direct knowledge of the steps taken to search for records, the head will be unable to establish that the search for records was adequate. I do not mean that the head of a public body is required to seek out every record personally. However, the head, or the head's delegate, should take a supervisory role and be aware of exactly what steps have been taken to locate records, as the head is accountable for the quality of the search under section 10.

[para 47] The evidence simply does not establish that the Public Body conducted an adequate search. The author of the affidavit who described the steps taken to locate records is not in a position to comment on the adequacy of the search conducted, as he does not have direct knowledge as to the steps members took. Instead, the evidence establishes that he asked members to conduct their own searches for records. The evidence does not establish the steps members took to locate records. In fact, the evidence of the Public Body is that it failed to produce records when it originally responded to the access request because one of the members did not supply the records. Clearly, the head of the Public Body did not take sufficient steps to ensure that a search was being conducted, let alone an adequate search.

[para 48] For these reasons, I find that the Public Body did not conduct an adequate search for the requested records and has failed to meet its duty to assist the Applicant. It did not search all the records in its custody or under its control, and it has not provided satisfactory evidence as to the steps it took to locate records among the records it did choose to search.

V. ORDER

[para 49] I make this Order under section 72 of the Act.

[para 50] I order the Public Body to disclose to the Applicant the information severed in emails 1, 2, and 3.

[para 51] I order the head of the Public Body to comply with the duty under section 10 of the Act by conducting an adequate search for the records requested by the Applicant and by responding to the Applicant's request openly, accurately, and completely. The search for records will include a search of the back up system for the period from February 1 2005 to March 31 2005.

[para 52] I further order the Public Body to notify me, in writing, within 50 days of receiving a copy of this Order that it has complied with the Order.

Frank Work, Q.C.
Information and Privacy Commissioner