NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER

Review Recommendation 09-074
File: 08-190-4
January 7, 2009

BACKGROUND

On approximately August 18th, 2008, my office received a request from the Applicant to review the response which he received to a request which he had made to the Department of Education, Culture and Employment. He had requested information about himself contained in the records of that department in connection with his Student Financial Assistance (SFA). In his original request to the department, he asked for:

> Any information regarding myself, my SFA number or my Millennium Scholarship, that was handled or commented on by [two named individuals] from the dates of October 1, 2005 to November 1, 2006. Any information would be excellent, but to be more specific I would like any e-mail sent, received, deleted or created during the time and any filed in their personal G: drives

The public body responded to the request, but the Applicant was not satisfied with the results and requested that the public body search through its backup system to recover deleted e-mails for the two named individuals for the relevant date range. It appears that he expected that the two named individuals had been discussing him or his application for funding and that that discussion was in some way inappropriate, although he did not elaborate on his suspicions or the reason he held such suspicions.

The public body took the position that they had done a thorough search in the first instance and had concluded that all relevant records had been provided. They advised the Applicant that they did not feel that it was necessary to resort to the back up systems. It was the department's position that that level of search was not necessary in this case, particularly in light of the fact that it was an established practice in the Student Financial Assistance program that e-mail messages about clients are saved, not deleted.

The Applicant then requested a review solely on the issue of whether or not the public body was required to search its backup e-mail records in order to fully comply with a request for information.

THE RELEVANT SECTIONS OF THE ACT

The relevant sections of the *Access to Information and Protection of Privacy Act* appear to be as follows:

Section 1, which outlines the intents and purposes of the Act, and which is always relevant when considering the application of exceptions to disclosure:

> 1. The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by
>
> (a) giving the public a right of access to records held by public bodies;
> (b) giving individuals a right of access to, and a right to request correction of, personal information about themselves held by public bodies;
> (c) specifying limited exceptions to the rights of access;
> (d) preventing the unauthorized collection, use or disclosure of personal information by public bodies; and
> (e) providing for an independent review of decisions made under this Act.

The definition for “record” as contained in section 2 of the Act:

> "record" means a record of information in any form and includes information that is written, photographed, recorded or stored in any manner, but does not include a computer program or other mechanism that produces records;

Section 3 of the Act which outlines what records are covered by the Act:

> 3. (1) This Act applies to all records in the custody or under the control of a public body, including court administration records, but does not apply to the following:...

It should be noted that none of the exceptions to this section are applicable to this case.

Section 5 of the Act provides that any person has the right to access to any record in the custody of or under the control of a public body.

Section 7 of the Act outlines the responsibility of a public body to assist an individual who has made a request for information:

> 7. (1) The head of a public body shall make every reasonable effort to assist an applicant and to respond to an applicant openly, accurately, completely and without delay.
>
> (2) The head of a public body shall create a record for an applicant where
>
> (a) the record can be created from a machine readable record 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.

THE PUBLIC BODY'S POSITION

The public body takes the position that section 7(1) is the most relevant section of the Act. They say that they have "made every reasonable effort to assist this applicant in locating the records pertaining to his request". They also refer to and rely on the "standard policy" within the division for e-mail messages relating to clients to be saved either on the client record or by the officer working with the client and conclude, therefore, that there are unlikely to be any deleted records responsive to the Applicant's request, particularly in light of the fact that their search was wide ranging. They advised that they searched the following records:

a) the Applicant's SFA client file, all ECE post-secondary funding, including loans, grants, Millenium Scholarships etc;
b) their case management Administration System - SFA Module under the Applicant's name;
c) all e-mails relating to the Applicant held by the manager of the SFA program
d) all e-mails relating to the Applicant held by the Student Loans Officer in charge of the Applicant's file;

e) the SFA Appeals file for client requests for internal review and appeals;

f) the Ministers “BF” (Bring Forward) file for the Income Security Division in relation to the Applicant.

The public body indicated that they found and provided the Applicant with 132 pages of responsive records, with only a minimal amount of information related to third parties having been severed.

It is the public body’s position that the parameters used to conduct the search for the records were entirely consistent with the scope of the request and that the department made every reasonable effort to be responsive to the request. They pointed out that the Applicant did not provide any evidence to support his suspicion that the e-mail records in particular might have been “sanitized’ so as to avoid the disclosure of embarrassing exchanges and no evidence on which one could reasonably conclude that other e-mails ever existed. Furthermore, it is their position that even if such e-mails had been created and then deleted, they may not exist in the backup system, depending on when it was deleted and how often the backups were made during the relevant time period.

Finally, the public body takes the position that back-up tapes contain data that must be retrieved and reconstituted before it is usable and that the GNWT backup system is not designed or intended to manage or retrieve individual messages, but to back up the system itself so that in the case of disaster, the system could be re-created. They advise that the criteria for requesting a search through the Technology Service Center for back up tapes is typically when they can identify specific records that did exist, and not when all they have is a broad search for records which may, or may not, have ever been created. It is the department’s position that Section 7 does not require a public body to prove to an absolute certainty that the email messages requested do not exist. There is an element of reasonableness built into the system so that it would be a rare circumstance in which the public body would be required to search the back-up records in response to a request for information.

The Department also referred me to several cases from southern jurisdictions in which this same issue has been discussed in the context of other provincial access and privacy legislation. Based on those cases, I asked the department to provide me with further information about the nature of the GNWT’s backup system and, in particular, more specifics about the ability of the

system to regenerate records and why it would, in the department's opinion, unreasonably interfere with the operations of the department. The public body provided me with a further explanation, including a letter from the Director of the Technology Service Center responsible for the maintenance of the government's computer system, including the backup system.

In their second submission to me, the public body reiterated their position that although the onus is on a public body to establish that an individual is not entitled to receive a particular record, they had met that onus. They pointed out, again, that the Applicant had not provided any evidence, other than his own personal belief, that such records existed. The search done covered all of the relevant files and there were no obvious gaps in the records provided. When asked, the employees involved indicated that they retained all relevant records. The department feels that, based on the searches and interviews which they did in response to this request for information, they have met their obligations under section 7(1) and there is, therefore, no need to rely on section 7(2). However, because I asked them to address the issue, they provided further materials relating to the nature of the backup system.

The Department provided the following information about the back-up system, all of which was supported and confirmed in a letter from the Technical Services Centre,

a) it would take at least 40 hours to attempt to retrieve and reconstruct back-ups for the two individuals named in the Applicant's request for information. The public body argues that this time commitment would interfere with the Technology Service Centre's work and delay other projects.

b) there is no certainty that restoration would be successful because some of the information requested was more than three years old and the technology had changed in the fall of 2006 so that some of the back ups may no longer be readable. This could not be determined until the work was done.

c) restoration would not be possible if the individual accounts were not stored as "pst" files and, once again, this could not be determined until the back ups were actually read.

d) if backup restoration is successful, the restored e-mail file may not contain all the records from that period of time. Backups for 2005 and 2006 would probably just cover

one day per month (as a snap-shot of what was on the system on that date) and anything received and deleted in the intervals between backups would not have been saved on the backup stystem.

e) the time required to review restored e-mails would also have a large impact on the Department of Education, Culture and Employment, and that impact would be sufficient to constitute an unreasonable interference with department operations. They estimate that it would take between 56 and 140 man-hours to review the restored records which would cause weeks of delay to other requests and other urgent work.

THE APPLICANT'S POSITION

Although the Applicant was given the opportunity to respond to the department's submissions, no further submissions were received from him. His position, as stated in his Request for Review is as follows:

> I believe that the people I have requested information on about my SFA didn't handle my file correctly and didn't follow proper SFA procedures. All of the information given to me so far was given by the people in question and therefore I feel could have been sanitized by these people before being handed over. The only way to verify this is to have access to the emails and documents I have requested through restores of backups.

DISCUSSION

I would first like to thank the Department for its thorough and thoughtful submissions in this case. The issue raised is one of general application to all public bodies. How far does a public body need to go to comply with a Request for Information? What is reasonable and when does the time and effort necessary to comply with a request become an unreasonable interference with the operations of the public body generally? In my opinion, this is a question of balance and each case must be considered on the basis of its own facts.

The first issue to consider is whether deleted records contained on a backup system are "records" under the Act and, if so, whether there is a right to access to them under the Act.

Clearly, e-mail records are “records” as defined in the Act. The Information and Privacy Commissioner of British Columbia, David Flaherty, as he then was, in Order 73-1995 made a similar finding:

> I have no difficulty in accepting the applicant’s submission, supported by FIPA, that e-mail is indeed a record under the Act. This means that there must be proper rules in place for the collection, retention, dissemination and destruction of such records.

Do they remain “records” when they end up in a backup system? In my opinion, they do. Nothing presented to me suggests that an e-mail which finds its way into a backup system changes from a “record” into something else. I note that, according to the information provided, the backup consists of machine readable data or records, although significantly more effort than ususal would be required to access them. By definition, it seems to me that backup systems have been created for a specific purpose and that is to allow the public body to recover, to a limited degree, the data contained in the system in the event of a catastrophic failure. If a public body ever really needed to recover a record from the backup system for its own purposes, it could do so, although it would be costly and time consuming. The question is whether the ATIPP Act imposes an obligation on the public body to undertake such an effort on every ATIPP request or even on every ATIPP request in which the Applicant requests it.

In this case, the public body relies primarily on section 7(1) of the Act. They feel that they made “every reasonable effort” to respond fully and accurately to the Applicant’s request and that they have, therefore, met their obligations under the Act without going the extra step of restoring backup records which may, or may not, produce further responsive records. The issue, therefore, is what is “reasonable”?

In Order 02-03, the Information and Privacy Commissioner of British Columbia, David Loukidelis, summarized what a public body must do to comply with its obligation to make all reasonable effort to assist an Applicant:

> Although the Act does not impose a standard of perfection, it is well established that, in searching for records, a public body must do that which a fair and rational person would expect to be done or consider acceptable. The search must be

> thorough and comprehensive. The evidence should describe all potential sources of records, identify those searched and identify any sources that were not searched, with reasons for not doing so. The evidence should also indicate how the searches were done and how much time public body staff spent searching for records.

In Order F2007-028 the Alberta Information and Privacy Commissioner Frank Work considered a similar application to this one. In that case, Commissioner Work concluded, based on the wording of section 10 of the Alberta Act, which is identical to the wording of section 7 of our Act, that the public body has the onus to establish that it has made every reasonable effort to assist the Applicant, which includes the duty to conduct an adequate search for records. As in this case, the public body in the Alberta case argued that it had not searched backup records because it would be expensive, difficult and time consuming to do so. Commissioner Work's response to that argument was this:

> In my view, if a public body could refuse to search on this basis, the effect would be to render an applicant's right to records under section 6 effectively meaningless.
>
> 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.

In that case after considering all of the materials before him, Commissioner Work determined that the public body had not conducted an adequate search and ordered the public body to search the backup tapes for responsive documents.

In my opinion, each case must be taken on its own facts when considering this issue. Because the Act makes "reasonableness" the standard, there are no absolutes. What is reasonable in one case, on one set of facts and evidence, may not be reasonable in another case with another set of facts and evidence.

The question, then, is whether in this case, with the facts and the evidence I have been provided with, the department made every "reasonable" effort to find the records responsive to the Applicant's request. In this case, I believe they did. I reach this conclusion because:

a) the search of current and existing records appears to have been thorough and wide ranging;

b) I am satisfied that, because of the nature of the backup system, there is a very good possibility that any e-mails that might have been deleted would not exist on the backup system in any event, because they were not on the system when the backups were done;

c) although given the opportunity to do so, the Applicant did not provide this office with any evidence, other than the Applicant's own suspicions, that other records existed

It seems to me that when an Applicant is asking a public body to search backup records, which would normally be considered above and beyond the normal search methods, there is an onus on that individual to provide something to support the need for that kind of search. The Applicant in this case has been able to provide nothing more than his own belief that the records were created. He has not provided me with any background or evidence which would support his belief, merely the statement that he does believe that the records he requests existed at some point. I am satisfied, therefore, that the public body made all reasonable efforts, in this case, to respond completely and fully to the Applicant without resorting to the

reconstitution of backup records and I make no further recommendations to the public body.

I do, however, accept and adopt the words of David Flaherty, the former Information and Privacy Commissioner from British Columbia who pointed out in Order No. 73-1995 that:

> My order may become technologically obsolete, in the short term, if developments in backup technology makes it a relatively simple and inexpensive matter to reconstitute backup tapes. Even at present, adoption of newer methods could facilitate that process. If backup can be reconstituted very efficiently and effectively, there will be more moral pressure on public bodies to make records accessible to requesters.

I note, as well, that that order was made in 1995, some 14 years ago and that technology has changed significantly in that time period. Public bodies will not be able to hide behind the complexity of reconstituting backup systems forever or in every case.

I would also make some general observations. The public body in this case relied extensively on their "policies" and "established practices" to support their contention that even if the backup searches had been done, there was little likelihood that the records being asked for would exist in the backup files. This is not the only government agency that depends on policies and practices to support their positions that no responsive documents exist. I would caution all public bodies to remember that policies and procedures are not, by any stretch of the imagination, flawless. By definition, they are implemented by individual human beings who may not always follow the rules, whether by premeditation or by reason of simple mistake or misunderstanding. We all do stupid things from time to time which we are later embarrassed about and try to hide. It would certainly not be surprising to learn that at some point two employees within a public body exchanged gossip about a third party by e-mail, thinking that no one else would ever see it or, probably more to the point, not even thinking about the possibility that it might be seen by anyone else. Furthermore, it would not be surprising to find out that those kinds of e-mail records are routinely deleted. There is no evidence that that happened in this case and I am not suggesting that it did. What I am pointing out is simply that reliance on established policies and procedures will not, in and of itself, constitute an adequate response to an Applicant seeking information and, furthermore, as I have pointed out on many occasions,

there must be a government wide protocol for the management of electronic records, including e-mail, similar to the one used for paper records.

CONCLUSIONS AND RECOMMENDATIONS

Based on the above, it is my opinion that the Department of Education, Culture and Employment made every reasonable effort to assist the Applicant and to respond to him openly, accurately, completely and without delay. I make no further recommendations.

Elaine Keenan Bengts
NWT Information and Privacy Commissioner