NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER

Review Recommendation 08-069
File: 07-214-4
April 2, 2008

BACKGROUND

On July 23rd, 2007, the Complainant asked this office to review a situation in which appeared that her personal information had been improperly used or disclosed. The Complainant alleges that she made an application for financial assistance from the NWT Housing Corporation under one of their funding programs. She was hoping to purchase a house. She indicates that on a Friday afternoon she was informed by a member of the community (who I will refer to in this recommendation as "A.B.") that a friend of his who worked at the Yellowknife Housing Corporation had told him that she had applied for funding from the Housing Corporation and that she had lied on her application form about his child support. A.B. had indicated to the Complainant that he was aware that the Complainant

a) had a file open at the office of the Yellowknife Housing Corporation
b) had made an application for funding under one of the Corporation's programs; and
c) had provided the Corporation with certain specific details relating to her financial circumstances

The following Monday, the Complainant says she went to the offices of the Yellowknife Housing Authority and asked to see her file. She spoke with a Programs Advisor about her concerns that her personal information may have been inappropriately disclosed to a third party. She requested the contact information for the President of the Corporation.

The following day, she says she received a voice mail message from A.B. He wanted to

assure the Complainant that he had been contacted by the individual working for the Housing Authority and that he had not been seeking the information.

On that same date, the Complainant wrote a letter to the President of the NWT Housing Corporation outlining her concerns in writing. In her complaint, she identified an employee of the Corporation who had a close personal relationship with A.B. who could have been the source of the inappropriate disclosure of her information.

The public body responded to the Complainant's concerns by letter of November 28th in which the President indicated that it offered its employees various courses regarding the *Access to Information and Protection of Privacy Act* and that it was a priority for the NWT Housing Corporation that all employees receive appropriate training and guidance in this area. He further indicated that all employees are bound by the terms of their Code of Conduct which prohibits the disclosure of personal information to third parties. He indicated that her application for funding was being considered and she would be advised of the outcome in due course.

In her correspondence to me, the Complainant also points out that the employee who she suspects was the source of the disclosure was either transferred or fired shortly after this incident.

ISSUE

The issue in this review is whether an employee of the public body either did or is likely to have improperly disclosed personal information about the Complainant to A.B. without the Complainant's knowledge or consent. Secondarily, did the public body deal with the Complainant's concerns appropriately, regardless of their findings.

THE RELEVANT SECTIONS OF THE ACT

The relevant provisions of the *Access to Information and Protection of Privacy Act*

provides as follows:

42. The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

47. A public body may disclose personal information only
(a) in accordance with Part 1; or
(b) in accordance with this Division.

47.1. An employee shall not, without authorization, disclose any personal information received by the employee in the performance of services for a public body.

48. A public body may disclose personal information
(a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose;
(b) where the individual the information relates to has identified the information and consented, in the prescribed manner, to its disclosure;
(c) for the purpose of enforcing a legal right that the Government of the Northwest Territories or a public body has against any person;
(d) for the purpose of
(i) collecting a fine or debt owed by an individual to the Government of the Northwest Territories or a public body, or
(ii) making a payment owed to an individual by the Government of the Northwest Territories or a public body;
(e) to a public body or a law enforcement agency for law

enforcement purposes;

(f) where disclosure is by the Minister of Justice or an agent or lawyer of the Minister of Justice to persons responsible for a place of lawful detention;

(g) for the purpose of hiring, managing or administering personnel of the Government of the Northwest Territories or a public body;

(h) to the Maintenance Enforcement Administrator for the purpose of enforcing a maintenance order under the Maintenance Orders Enforcement Act;

(i) to the Information and Privacy Commissioner, where the information is necessary for the performance of the duties of that officer;

(j) to the Auditor General of Canada or to any other prescribed person for audit purposes;

(k) to an officer or employee of the public body or to a member of the Executive Council, where the information is necessary for the performance of the duties of the officer or employee or the member of the Executive Council;

(l) for use in the provision of legal services to the Government of the Northwest Territories or a public body;

(m) to the Northwest Territories Archives for archival purposes;

(n) for the purpose of complying with a subpoena or warrant issued or an order made by a court, person or body that has the authority to compel the production of information or with a rule of court that relates to the production of information;

(o) for the purpose of supervising an individual under the control or supervision of a correctional authority;

(p) for the purpose of complying with a law of the Territories or Canada or with a treaty, written agreement or arrangement made under a law of the Territories or Canada;

(q) when necessary to protect the mental or physical health or safety of any individual;

(r) so that the next of kin of an injured, ill or deceased individual may be contacted;

(s) for any purpose when, in the opinion of the head,

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(ii) disclosure would clearly benefit the individual to whom the information relates;

(t) where the information is otherwise available to the public;

(u) for any purpose in accordance with any Act that authorizes or requires the disclosure; or

(v) to a member of the Legislative Assembly who has been requested by the individual to whom the information relates to assist in resolving a problem

DISCUSSION

The public body's position is that they simply could not determine whether or not their employee did, in fact, improperly disclose information to A.B. They do not suggest that if A.B. obtained the information alleged, that it was justified pursuant to section 48. Therefore, if things transpired in the way that they are alleged to have by the Complainant, any such disclosure was wrongful.

At least three pieces of personal information were involved here. Firstly, that the Complainant had an open file with the Corporation. Secondly, that the file involved an application for funding. And thirdly, that some of the financial information in the application was allegedly not true. Although the disclosure of this last piece of information may be the most serious breach of the Complainant's personal information, the disclosure of anyone of these tidbits of information would be wrongful. If, therefore,

matters transpired in the way they are alleged to have transpired by the Complainant, the disclosure of her personal information was in breach of the provisions of the *Access to Information and Protection of Privacy Act* and, therefore, wrongful, regardless of what specific personal information about the Complainant was disclosed.

In responding to my request to the Housing Corporation for its comments on the allegations made, the ATIPP Co-Ordinator for the public body advised that he had not been informed of the complaint at the time it was made and that he could not, therefore, comment on how the investigation was undertaken, by whom, or what steps were involved. He indicated, however, that in his review of the matter in response to this review process, he determined that an investigation had, in fact, been undertaken by the Housing Corporation's Executive Office and North Slave District Office. He says that upon receipt of the Complainant's letter, a directive was issued from the President of the Corporation to the North Slave District Director to investigate and provide a letter of response for the President's signature. As a result of this process, it appears that the Complainant met with the Manager of Programs for the North Slave District Office to discuss confidentiality issues and that the Manager understood, at the end of the meeting, that the Complainant was satisfied that an appropriate resolution to her concerns had been reached. As a result of this meeting, the letter of November 28th noted above was sent to the Complainant. As also noted above, that letter did not outline the steps being taken to address the issues. It stated only that employees were encouraged to participate in ATIPP training and were, furthermore, bound by their Code of Conduct. The letter also confirmed that the Complainant's application for funding was being considered and she would be advised as to the outcome in due course.

It does not appear that the Complainant was told about the specific results of the investigation, at least until she received the public body's response to this office during this review process, a copy of which was provided to the Complainant.

The public body indicated that at the end of their investigation they were unable to find any evidence to suggest that the employee suspected of disclosing the information had,

indeed, done so. They pointed out that the complaint specifically referred to private conversations held between the suspected employee and A.B., a person with whom the employee had a "close personal relationship". The public body suggests that, as the Corporation was not privy to those conversations, they were unable to confirm whether or not they actually took place. When asked, the employee "stated that she had not disclosed any private financial information related to [the Complainant]." They also point out that this employee was assigned responsibility to review applications from a different community and that there were, therefore, no records to suggest that the employee was privy to the information on the Complainant's file or any other application by residents in the Complainant's community.

I would make a couple of comments about these submissions. Firstly, it seems to me that when a concern is raised about a possible breach of confidentiality, any investigation into that breach should involve the ATIPP Co-Ordinator for the public body in some way. This is the one person in each public body assigned, as part of his/her job duties, to deal with access and privacy issues. This suggests that this person is likely the one person who has the most extensive knowledge about access and privacy issues within the public body. If the *Access to Information and Protection of Privacy Act* is to be given the respect that it demands, complaints such as this one should be handled by someone at least semi-independent and by someone who has some background in the requirements of the Act. Furthermore, there should be a written record of the steps taken in undertaking the investigation and the findings. Once the investigation is complete, the complainant should be provided with a detailed report setting out the process, the findings and the steps that will be taken to address any deficiencies.

Secondly, it is indeed difficult in these kinds of circumstances to confirm with any certainty whether there was, in fact, a breach of an individual's privacy. Unless there is some means of confirming who has had access to a particular file and for what purpose, it will almost always come down to the Complainant's word against the employee's. The natural tendency is to protect the employee and the conclusion is that,

if you can't prove what happened, there's nothing that can be done. I disagree with this approach. In any given set of facts, if you look at all of the facts and circumstances, it is possible to conclude that it is "more likely than not" that there was an inappropriate use or disclosure of an individual's personal information. In this particular case, I think that the circumstances and human nature are such that it is more likely than not that the employee passed on information to A.B. about the Complainant. That cannot be established with any certainty and any disciplinary proceedings against the employee, therefore, would have to reflect the uncertainty. In this case, the employee is no longer working with the public body and discipline is, therefore, a moot point in any event. I think, however, the reasonable conclusion is that some information was inappropriately passed on to A.B. either by that employee or by someone else within the Corporation.

Thirdly, I note that although the employee denied having disclosed any financial information to A.B., I am left to wonder what specific questions were asked of the employee. Was she asked if she had seen, in the course of her employment, any records concerning the Complainant. Was she asked whether she had spoken with any other employee about the matter? I wonder, as well, if the employee's definition of "financial information" might not be nuanced so as to deflect responsibility and avoid discipline. In short, I am left to wonder how thorough the questioning of the employee might have been and what was left unsaid or unasked.

To the credit of the public body, they did say that in response to the complaint they would be providing regional staff with a workshop on protection of privacy issues. In addition, materials related to the Act would be made available on the Corporation's internal website as an additional resource.

Finally, the public body indicated that they had no specific policies in the area of confidentiality other than those which had been developed for the Government of the Northwest Territories as a whole. It was also pointed out that all employees are required to comply with the Code of Conduct and to take an Oath of Office upon hire.

Although, as the public body points out, it is impossible to confirm with certainty that there was an inappropriate disclosure of the Complainant's personal information, I have to say that the circumstances of this case suggest to me that the probability is fairly high that the employee did provide A.B. with some information she had seen or heard at work about the Complainant. In the end, I cannot make a definitive finding, but I would suggest that it is likely that it happened.

In the north, where the low population base means that there is always going to be a high probability that public employees will be privy at some point to personal information of someone else that he or she knows, it is important to make sure that there are adequate safeguards in place to prevent improper use or disclosure of that information. Based on the information provided to me by the public body in this case, this public body does appear to have some basic policies and precautions in place with respect to protection of privacy, but I would suggest that those precautions are not sufficient. It is good to have a code of conduct and an oath of office. Unless these are reviewed or renewed from time to time, however, they are easily overlooked or forgotten in the day to day grind of the workplace. It is also good to "encourage" employees, especially those who, for any reason, might have access to the personal information of third parties, to participate in seminars and workshops on privacy issues in the workplace. However, if it were up to me, every employee of every public body would be required to undertake training on hire with refreshers on an annual or bi-annual basis.

Quite apart from privacy policies, public bodies are also required to give thought to the physical security of records within the workplace. Who has authorization to look at what files? How are limits to authorization enforced? Are file cabinets locked? Are the records systems designed to provide broad access to records to everyone in the office or are records compartmentalized so that there is some control over access to records, for example, from different communities? In other words, can any employee who has a "reason" to review a record from Deline also easily access a record from Yellowknife, even when there is no apparent reason for such access, or are there some physical controls in place to prevent that kind of "snooping"? Is there any method of recording

who is accessing files and for what reason (this is most easily accomplished where records are electronic and audit trails can be created)?

This situation is somewhat similar to that discussed by the Ontario Information and Privacy Commissioner in Order HO-0002. In that case, a woman sought medical attention in an Ottawa hospital. Both her ex-husband and his girlfriends were employees at the hospital and she made a specific request that precautions be taken to prevent either of them having access to her medical records or charts. Despite this, the girlfriend, who as a nurse at the facility but in a different ward, accessed the records a number of times over a period of time. In the postscript to the Order made by the Commissioner, she made the following comments which are apropos here:

> Despite having alerted the hospital to the possibility of harm, the harm nonetheless occurred. While the hospital had policies in place to safeguard health information, they were not followed completely, nor were they sufficient to prevent a breach of this nature from occurring. In addition, the fact that the nurse chose to disregard not only the hospital's policies but her ethical obligations as a registered nurse, and continued to surreptitiously access a patient's electronic health record, disregarding three warnings alerting her to the seriousness of her unauthorized access, is especially troubling. Protections against such blatant disregard for a patient's privacy by an employee of a hospital must be built into the policies and practices of a health institution.
>
> This speaks broadly to the culture of privacy that must be created in healthcare institutions across the province. Unless policies are interwoven into the fabric of a hospital's day-to-day operations, they will not work. Hospitals must ensure that they not only educate their staff about the *Act* and information policies and practices implemented by the hospital, but must also ensure that privacy becomes embedded into their institutional culture. As one of the largest academic health sciences centres in

> Canada, the Ottawa Hospital had properly developed a number of policies and procedures; but yet, they were insufficient to prevent members of its staff from deliberately undermining them.

She concludes with the following comments:

> Upholding compliance with the *Act* is not simply a matter of following the provisions of an enacted law, but ensuring that the use and disclosure of sensitive personal information such as health information is strongly monitored, and access controlled to those who truly need it in the performance of their duties.

Although the privacy breach in that case was in the context of health information and, therefore, potentially more serious than the breach involved in this case, the comments made are applicable across the board. It is not sufficient to rely simply on ethical behaviour of employees, even when the ethical rules are outlined in policies and codes of conduct. Public bodies must recognize that employees are driven by human nature and that human nature sometimes makes people do things they know are absolutely wrong, even when they know, or ought to know, that they will be caught doing it.

SUMMARY AND RECOMMENDATION

When asked what, if anything, could be done to compensate her for the improper disclosure of her personal information if I were in fact to find that this had happened, the Complainant made it clear that she was frustrated generally with the service she had received from the Housing Corporation and suggests that the fact that she filed this complaint might have had an unfair negative impact on her application as a whole. She provided no support for that allegation, however. She feels that there has been inordinate delay, as a result of which the prices of housing have gone up significantly and she has had to pay ongoing rent in the meantime. She seeks compensation in the form of cash and suggests a sum of about $49,000.00. Even were I in a position to

make a recommendation to that effect, I would not do so in this case. There is no evidence whatsoever that the improper disclosure of the Complainant's personal information or the Complainant's decision to complain about that disclosure has had any impact whatsoever on the funding application process or how the Housing Corporation has dealt with it. Nor is there any suggestion that A.B. used the information he received or appears to have received from the Housing Corporation for any purpose other than, perhaps, to challenge the Complainant about the truth of the information.

In conclusion, therefore, I find that it is likely that there was some improper disclosure of the Complainant's personal information in this case, although that cannot be determined with certainty. I would make the following recommendations in the hope that in the future, such improper disclosures are less likely to occur:

a) this public body should develop a protocol to deal with complaints about possible breaches of the privacy provisions of the *Access to Information and Protection of Privacy Act* and this protocol should include the ATIPP Co-Ordinator for the public body as an active participant in the process. This protocol should include the creation of a written record of the steps taken in undertaking the investigation and the findings and a requirement that once the investigation is complete, the complainant be provided with a detailed report setting out the process, the findings and the steps that will be taken to address any deficiencies.

b) this public body should review and/or create procedures, practices and protocols relating to the third party information collected and the privacy of that information, to ensure that they comply with the requirements of the *Access to Information and Protection of Privacy* Act and its regulations, taking into account the concerns expressed above, including:

    i) the physical security of the records (i.e. location, limited access, locked cabinets, filing procedures, etc.)

ii) the possibility of creating a system to produce audit trails to record when files are reviewed, by whom and for what purpose;

iii) role based access to records

c) the public body should implement a long term program to ensure that all employees who might have access to third party information are knowledgeable about their responsibilities with respect to such information, including:

i) regular training opportunities on privacy issues together with strong incentives for employees to participate in such training;

ii) regular reminders about the importance of ensuring that no third party information is improperly used or disclosed, perhaps in the form of short "scenerios" demonstrating either good or poor information practices in the Corporation's internal newsletters or internal web site;

iii) periodic reminders of the content of the Code of Conduct and the Oath of Office;

Elaine Keenan Bengts
Information and Privacy Commissioner