NUNAVUT
INFORMATION AND PRIVACY COMMISSIONER

Review Recommendation 13-067
November 5, 2013

Review File: 13-140-5

BACKGROUND

The Complainant in this matter asked me to review how his personal information had been collected and used by people within his workplace, the Nunavut Housing Corporation. In November of 2011, the employer circulated a spreadsheet showing phone calls made from the office. The report showed that a telephone number which the Complainant had had in another part of Canada prior to accepting employment in Nunavut had been dialed, several times, from the desk of one of his co-workers. At the time of the Complaint, the Complainant felt that the only way that the phone number could possibly be known to anyone in the office would have been from his resume in his personnel file. It was not in the phone book, nor could the phone number be found under “Canada 411" on line. The Complainant even called the number to see if, by chance, the number had been allocated to someone else but the call indicated that the number was not in service.

At the time of this incident there had been some conflict in the workplace involving the Complainant. The Complainant had, in fact, initiated a complaint about harassment in the workplace and had asked for an intervention by management. He was convinced that his supervisor either made the phone calls with a view to trying to “dig up dirt” on him or gave the phone number to a co-worker for the same purpose. The Complainant says that he raised his concerns with management but his concerns were dismissed.

THE RESPONSE FROM THE PUBLIC BODY

The public body confirms that, as part of normal business practice, long distance charges are reviewed periodically to monitor use and to ensure that there was no misuse of the system. They indicate that the phone log (a copy of the statement received from Northwest Tel) shows all phone calls made from each unique phone extension in each government office. They also confirmed that the telephone number identified by the Complainant had, in fact, been dialed several times from a phone extension within the Complainant’s workplace, and that the extension was assigned to a co-worker of the Complainant’s. Finally, they confirmed that the

co-worker was at work on the date in question. They could not, however, confirm that the co-worker was, in fact, at his desk, when the telephone calls were made and the co-worker denies having made the calls.

The public body also advised that the personnel records for this office are, in fact, retained in an office of the public body in another community. The Complainant's personnel file was not, therefore, available to anyone in the office. That said, however, some information about employees is retained in the local office. This does not include documents such as resumes, or applications for housing (which might contain a new employee's pre-employment telephone number), but only leave and overtime applications, and items dealing with performance management issues. Furthermore, these limited files are secured in locked offices. The supervisor indicated that at no time did he have access to the Complainant's resume, which contained the phone number in question, either before the Complainant was hired or since.

The public body could provide no explanation as to how the Complainant's old phone number might have surfaced or who might have made the phone call or why. There was a suggestion that someone in the office had suggested that the Complainant's name had been listed on the internet as the owner of a named business which operated in Nunvaut and the phone number in question was listed on the business's web site. There was, however, no explanation as to why anyone would be looking that information up, collecting that information or calling that number from the office.

I asked the public body whether it was possible that someone within the public body had been looking into the Complainant's background for some purpose related to employee management, and the answer was "no".

THE RELEVANT SECTIONS OF THE ACT

As always, it is always appropriate to review the most relevant provisions of the *Access to Information and Protection of Privacy Act* in relation to the issues before me. The starting point should always be Section 1 which sets out the purposes of the Act:

> 1. The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by...

(d) preventing the unauthorized collection, use or disclosure of personal information by public bodies; and...

Part II of the Act deals with the collection, use and disclosure of personal information. The rules apply not only to the personal information of third parties, but also to the personal information of employees, such as the Complainant. Section 40 of the Act provides that:

40. No personal information may be collected by or for a public body unless
(a) the collection of the information is expressly authorized by an enactment;
(b) the information is collected for the purposes of law enforcement; or
(c) the information relates directly to and is necessary for
(i) an existing program or activity of the public body, or
(ii) a proposed program or activity where collection of the information has been authorized by the head with the approval of the Executive Council.

Section 43 of the Act deals with the use of personal information:

43. 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;
(b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use; or
(c) for a purpose for which the information may be disclosed to that public body under Division C of this Part.

Division C (specifically Section 48) outlines a number of circumstances in which a public body may disclose personal information. The most relevant subsections of Section 48 allow for disclosure:

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

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

(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;...

Finally, section 42 of the Act creates a positive obligation on all public bodies to protect personal information:

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.

DISCUSSION

I am satisfied, based on the information provide to me by the public body, that the Complainant's telephone number did not come from his personnel file. There was no inappropriate use or disclosure of information from the Complainant's personnel file.

This, however, does not end the matter. It is clear from the information provided by the Complainant and confirmed by the public body that someone made a number of phone calls to the Complainant's discontinued phone number from an extension in the workplace, during work hours. As noted by the Complainant, the phone number had belonged to his company. If someone had somehow connected the company name to the Complainant, it was because they would have conducted a search, probably on the internet. The business name and the phone number did not just appear out of nowhere. If there was someone in the office who found the business name, as stated by the public body, that person would have had to be looking for it. The information was clearly "collected" from somewhere. There is no explanation as to why it was collected. The public body acknowledges that there was no employee management purpose for such phone calls to be made by anyone in the office. Nor has the public body provided me with any other legitimate explanation for anyone in the office either collecting the

Complainant's personal information or for using it. While there is no way to pinpoint who in the office collected or used the information, I believe that it is fairly clear that SOMEONE within the public body did so, during work hours. It is likely that the person who made the phone calls was the employee assigned to the desk from which the calls were made, but this cannot be confirmed with certainty.

As noted above, the *Access to Information and Protection of Privacy Act* puts the onus on public bodies to protect against unauthorized collection, use or disclosure of personal information. It is not good enough for this public body to say "we can't confirm who made the phone calls" and simply dismiss the complaint in result. Someone, whether instructed by management or acting on their own, collected personal information about the Complainant and then used that information to try to call the number attached to his name. The calls were made during regular business hours from the employer's equipment. One can only assume that the collection of personal information also happened during regular business hours. The circumstantial evidence, including the fact that there were issues in the workplace between the Complainant and others, points inexorably to the conclusion that someone in the employ of this public body improperly collected and used the Complainant's personal information, even if it cannot be said with certainty which employee it was.

Section 42 makes it the public body's legal obligation to address the issue more directly than shrugging it off and saying "we can't prove anything".

I find that the public body in this case failed to comply with sections 40, 42 and 43 of the *Access to Information and Protection of Privacy Act*.

SUMMARY AND RECOMMENDATIONS

As noted above, I have concluded that the public body, through one of it's employees who cannot be identified with certainty, breached the Complainant's personal privacy by improperly collecting and using personal information about him. Privacy, once breached, cannot be "unbreached". The breach added to the tension within an already tense office dynamic.

This is far from a unique situation. Employers are not always going to be able to prevent employees from doing things that they are not supposed to do. It is troublesome, however, when management itself fails to recognize that a breach has occurred or, having recognized it, fails to address it.

I recommend:

a) that this public body provide all management and supervisors with basic training with respect to its obligations under the *Access to Information and Protection of Privacy Act* to protect the privacy of individuals, including the collection, use and disclosure of such information;

b) that this public body create and send consistent and repeated messaging to it's employees to remind them of the employer's (and therefore their) responsibilities under the Act.

I have not formally recommended an apology to the Complainant because such a recommendation would not result in a sincere apology. A sincere apology, however, would not be out of order.

Elaine Keenan Bengts
Nunavut Information and Privacy Commissioner