NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER

Review Recommendation 14-125
13-187-4
March 31, 2014

In early December of last year, the Complainant received a letter from the Department of Justice, with whom he had been employed, indicating that the department had become aware that personal information pertaining to him had, inadvertently, been stored in a GNWT internal shared folder on the government network and that, as a result, there was a potential that in could have been accessed by GNWT employees outside of the Finance Division of the Department of Justice and the Department of Finance. The information was financial information and included copies of T4A slips. The department indicated to the Complainant that they had no evidence that anyone, other than employees in the Finance Division of the Department of Justice who were working on the preparation of those documents, had accessed the file but they could not confirm that. The letter explained that the electronic folder involved was at no time accessible to anyone outside of the GNWT. They admitted that there should have been security mechanisms that further restricted access to the contents of the folder to only those who needed to have access to the information for the purpose of their employment but in this case that was either not done or the security on the file had been changed. Those working with the file all mistakenly believed that the necessary security mechanisms had been in place. The letter went on to explain that the personal information was in a folder within a folder within a folder on the system and that the title of the document was such that it would be unlikely that anyone other than those who were working with the information would know what the document was without actually opening it. That said, there were no audit functions in place to determine who, if anyone, outside the Finance Division, had accessed the file.

The Complainant asked me to review the situation, and in so doing, posed a number of questions including:

- what were the circumstances of why his personal information was unsecured?
- over what period of time had the information been left unsecured
- why were audit mechanisms not in place so as to allow the public body to determine who had accessed the information?
- how is it possible that the Finance division of the department could "believe" that appropriate security mechanisms were in place, when they were not?
- how many GNWT employees are there who could have accessed the information?
- why was there a delay of almost a month from the date the problem was discovered before the Complainant was informed about it?
- what, if any, other personal information about the Complainant may have been compromised?
- how was the problem discovered?

THE PUBLIC BODY'S RESPONSE

The Department of Justice provided my office with a detailed explanation as to the issues raised by the Complainant. I would summarize those responses as follows:

1. In November, 2011, the Department of Justice identified a need to amend several T4A slips for a number of individuals, one of whom was the Complainant. This was communicated to the Department of Finance, whose responsibility it is to produce these records. The documents were produced and put in a secure Department of Justice data folder. In 2013, the GNWT instructed departments to review the contents of the "J" drive in preparation for the removal of that storage option. During that review, it was discovered that security on that drive had, without the knowledge of the Department of Finance or the Department of Justice, at some point been changed so that it was no longer secure.

2. The T4As for three years were placed on the shared drive between November, 2011 and February, 2012.

3. The Technology Service Center (TSC) is responsible for maintaining and supporting the networks used by government to store data. A security audit mechanism can give departments the ability to audit who has had access to any particular file or folder. This function, however, was not “turned on” for this folder.

4. Restricting folder access to specific individuals has been standard practice for ensuring information is accessed only by authorized personnel. Folders are automatically restricted down many levels from a department “file” share to a division and/or program level file share. Employees from one division cannot see another division’s folder and even within a division, there are protocols and practices in place to protect information within program areas.

5. Both the Department of Justice and the Department of Finance understood that security mechanisms were in place for the folder in question. The security could only be lifted by the TSC, but the TSC could not confirm when the security was lifted or, in fact, whether the security access restrictions were properly implemented in the first place. In reviewing this matter, the Department of Justice acknowledged that there had not been the appropriate follow up by the Department to ensure the folder was restricted. As a result of this incident they are reviewing their practices and protocols. The Information Security/Information Technology unit of the Department of Justice is now also reviewing drive structures and access privileges on a regular and ongoing basis.

6. Without security audit mechanisms in place, the Department was unable to confirm if any access to the records took place. The information was, however, in a nondescript folder and was also a folder within other folders so that someone would have to “drill down” to find the information. While the GNWT has approximately 2600 staff within the network who had potential access to the

information, it is unlikely in the circumstances that anyone who did not require access to it for their work would have seen it. The possibility did, however, exist.

7. The department wanted to be able to provide the Complainant with as much information as they could before disclosing the possible disclosure to him so they did a thorough review of the matter before advising him. In doing this, and therefore delaying advising the Complainant, it was hoped that they could have been able to confirm, one way or another, whether a breach actually occurred.

8. The Department of Finance maintains tax information for statutory purposes. The copies of the T4As were held on the folder in order for DOJ Fianance staff to copy and attach them to letters sent to the individuals affected by the amendments.

DISCUSSION

Section 42 of the *Access to Information and Protection of Privacy Act* puts a positive onus on public bodies to protect the personal information about individuals from unauthorized access, collection, use or disclosure:

> 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.

There are currently no breach notification provisions in our Act. This means that there was no legal obligation on the public body to disclose the problem they discovered in this case. I therefore applaud the Department for being pro-active in this instance and informing both my office and the Complainant when they discovered the possibility that personal information may have been compromised. The public body recognized the potential seriousness of this situation and chose to address it directly. While there is nothing they can do, at this point, to give the Complainant any comfort that his personal information (including Social Insurance Number) was not improperly accessed, the

situation does provide the opportunity to review policies, procedures and protocols so as to attempt to avoid similar problems in the future.

RECOMMENDATIONS

Having reviewed the submissions provided by the Department of Justice with respect to what transpired in this case, it is clear that the Complainant's personal financial information, including his name, address and Social Insurance number, was mistakenly left in a file open to any one of several thousand G.N.W.T. employees. While it is probable that no actual breach occurred, it is the responsibility of the Government of the Northwest Territories to protect personal information. In this case, the Department of Justice failed in that responsibility and have recognized that failure by disclosing the problem to the Complainant and to this office. What stands out about this case is that, despite the fact that these are electronic records, there is apparently no way to monitor or determine whether any non-authorize personnel viewed the record. There are lessons to be learned from this situation, even if we cannot "undo" the fact that there was a mistake made which potentially exposed sensitive personal information about the Complainant. I therefore make the following recommendations with a view to improving the security of sensitive personal information on the GNWT network system.

a) I recommend that the GNWT Technology Service Center take steps to "turn on" or add audit capabilities to all of it's network systems so that when human error occurs, which is inevitable as evidenced by this case, public bodies can audit the system to determine whether, and by whom any particular piece of electronic information was accessed. One of the strengths of electronic records from a security standpoint is that such auditing can be done. Because government deals with personal information all the time, and because the GNWT has a legal obligation to protect such information, this seems to me to be a logical capability for the entire system to have. The GNWT net work system is complex enough that it most likely already has audit capabilities built in to most of the system. If so, it needs to be "turned on". If, however, the capability does

not currently exist, I recommend that the GNWT invest in technology that would enable such audits, particularly in departments and divisions within departments which deal with significant amounts of personal information.

b) I also recommend that the Technology Service Center conduct a systematic review of its network system and each department's "file shares", together with senior staff within each department, to ensure that all "drives" which are intended to be secure and with restricted access do, in fact, have these attributes. I further recommend that this exercise take place at least annually.

c) In this particular case, as I understand it, the Department of Finance was responsible for preparing the T4As and for reporting to the Canada Revenue Agency, as well as for historical record keeping required by federal legislation. The Department of Justice, Finance Division was responsible only for confirming accuracy of the amended T4As and for distributing the amended T4As. There was no reason for the Department of Justice to have retained those records after they had been checked for accuracy and distributed. I therefore recommend that those responsible for information management review policies and procedures with respect to the management of this kind of information and, in particular, retention and destruction schedules. The fewer places that such information exists, the less the likelihood that a breach can occur.

d) I recommend that these recommendations be shared with all departments as they apply and are relevant to the entire GNWT.

Elaine Keenan Bengts
Information and Privacy Commissioner