NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER
Review Recommendation 17-158
File: 16-193-4
March 15, 2017

BACKGROUND

The Complainant wrote to me in late November, 2016 indicating that he believed that his privacy was being breached by his former employer, a public body. His employment with the public body (hereinafter referred to as Department A for ease of reference) ended early in the second half of August of 2016.

His complaints included the following:

a) that his supervisor at Department A had disclosed, to more than one third party, the circumstances of his departure;
b) that Department A had used his personal information (his signature) to process cheques after his departure;
c) that Department A failed to shut down his email account after his termination and one or more people continued to have access to that email account (including any personal email received at that address) and to receive and answer emails sent to that account after his departure.

THE COMPLAINTS

1. Inappropriate disclosure of personal information by the Complainant's Supervisor

With respect to the first complaint, the Complainant alleged several instances in which he believed that his former supervisor at Department A had discussed with third parties the circumstances of his departure from the public body.

i) Several days after his departure from his position, the Complainant decided he needed to call an important client to apologize for not calling as he had promised. The client told him that his former supervisor had already told him about the

situation. He did not, however, press for details on what "situation" his supervisor had described.

ii) Several days after his departure from his position, the Complainant called another public body (Department B) with which he had worked prior to transferring to Department A. He was told that the Assistant Deputy Minister had disclosed that the Complainant's former supervisor had made certain negative comments about the Complainant.

iii) Several weeks after his departure from his position with Department A, he had coffee with a friend who told him that the Complainant's former supervisor had called him and told him about the circumstances of his departure.

iv) Approximately two months after the Complainant's departure from his position, the Complainant ran into a former colleague in the workplace who told him that he "couldn't talk" to the Complainant because of the "stuff" he knew he wasn't dealing with well and that he (the Complainant) needed to get over it.

2. Use of the Complainant's signature after the end of his employment.

With respect to the second complaint, the Complainant questions how his signature could be used to authorize a cheque run on the day his employment ended but after he was no longer an employee. He says that because the authorizations weren't changed quickly enough, the public body allowed his signature to be used on the cheque run. He says he never saw it and has no idea what went out under his signature that day.

3. Failure by the public body to properly shut down his email address following his departure.

Finally, the Complainant says that his email address was allowed to remain active and others within the public body were receiving and sending email from this account in his name. Further, he says that one or more people had access to his personal emails which remained on the system (and perhaps were received after his departure).

The Complainant took steps to check to see if his email was still active approximately two weeks after his departure by sending an email to the address he had been assigned while employed with Department A. He says that the message went through "as per usual without a notice bounce back the account was shut down and no out of office response put on". When the public body was asked to address this issue, it appears that an automatic message was placed on the account which noted that the Complainant was "out of the office". Almost three months later, the Complainant once again tested the system by sending another email to his former work email address. Once again he says nothing happened - there was no out of office notice or any message that the recipient was out of the office. To test the system further, he sent emails to two similar but bogus addresses and each of them returned with a message that the email could not be delivered because the email address used "could not be found". He considered this proof that his work email address was still active in the employer's system and being used.

He also complained that as of November 24th, he was still listed in the online staff directory on the college website even though he had not been working there for three months.

In correspondence with the employer in mid November, the Complainant says he was told that since his departure only his former supervisor had had access to the account, suggesting that this individual had been monitoring and using the account throughout that period of time.

THE PUBLIC BODY'S RESPONSE

1. Inappropriate disclosure of personal information by the Complainant's Supervisor

The public body admits that the Complainant's supervisor contacted an important client of Department A to advise that the Complainant was no longer working with the public body. The supervisor indicates that, because of the nature of the relationship between the client and the public body, it was important for the client to know that the vacancy was due to a simple "personnel change" and not related to any wrongdoing on the part of the Complainant. No details were provided about the circumstances surrounding the Complainant's departure.

The public body also admits that the Complainant's former supervisor contacted an Assistant Deputy Minister of Department B and advised Department B of the circumstances surrounding

the Complainant's departure from Department A. This was necessary, they say, because of a direct funding relationship between Department A and Department B.

Department A further admits that the Complainant's "friend" had been advised of the circumstances of Complainant's departure. The friend, however, was also an employee of Department A in a position senior to the Complainant and discussions were necessary to ensure that the Complainant's position was filled as quickly as possible because of ongoing and urgent work being done.

Finally, the public body acknowledges that the circumstances surrounding the Complainant's departure from Department A were discussed at an "in camera" meeting of senior officials of the public body. All participants at the meeting were asked to leave during the discussion except for those required to make a decision. This discussion was required to identify a possible financial settlement with the Complainant arising out of his departure from the public body.

2. Use of the Complainant's signature after the end of his employment.

Department A noted that the cheques referred to by the Complainant are printed through an automated system. The Complainant had authority to authorize payments and, with respect to the cheque run printed on the day he left the public body's employ, he had already authorized the payments. Since the approvals took place in advance of the Complainant's departure, the Department considered the run to have been authorized appropriately. The public body argues that this is not a privacy issue, but an operational one. No further cheque runs were printed with the Complainant's name other than the one done on the date of his departure.

3. Failure by the public body to properly shut down his email address following his departure.

Department A advises that the Complainant's email address was not shut down following his departure as it was anticipated that emails would be directed to that email address relating to the Complainant's position. They say, that,

> Only [the Complainant's supervisor] had access to emails received on this account and [s]he could view but not respond to emails in [the Complainant's]

name other than redirect from his own email inquires relating to the position vacancy and who else someone may contact.

They argue that the Complainant's email address was related to his position with the public body and that it is not unusual that an employee's work email would be accessed by their direct supervisor following a position vacancy. This is required, they argue, as generally the most current decision making relating to active issues and concerns are done through email exchanges.

THE COMPLAINANT'S RESPONSE

The Complainant was given the opportunity to respond to the submissions made by Department A. He pointed out:

a) that nothing in Department A's submissions suggested that the supervisor's discussions about the circumstances of his departure from the public body were limited to the discussions he knew about;

b) the Department's policies require two of four signing authorities to sign all cheques and, since the Complainant was no longer an employee of the public body when the cheques were "written", the requirement for two signatures was not met, even though his signature was printed on the cheques. He argues that the signatures to go on the cheques can be changed at any time before they are printed and another signature could have been quite easily substituted for his before the cheque run was done. He essentially alleges that the failure to change the signature on the cheque run was simple laziness. He further notes that normally he would have been given the entire batch of physical cheques along with the printouts from the financial system so that he could verify each cheque before it was sent out. Because he was unable to do so in this case, he says he has no idea what cheques went out under his name.

c) the Complainant says that as of the date of his response in early February his email address at the public body still remained active, though it did return a message saying "I am presently out of the office" with a direction to contact another employee. He argues that leaving the email account open "continues to

represent that I am employed" by the public body in question and that the note sent by the system misrepresents the facts to the public. He also notes that his name continued to be listed on a government website as the contact person for a particular function until November 21st, 2016 and that his name remained on the public body's web site with his position noted until December 19th, even though he had asked that it be removed.

He notes further that his former supervisor "has a history" of giving people access to other people's email accounts. He uses an example of when he was given access to the email accounts of two other employees who were on leaves of absence so that he had full access to their email. He has concerns about who has access to his email account and notes that there were items of a personal nature saved to the account, including information about the reasons for his departure from the public body.

It is to be noted that in his response, the Complainant freely admitted that when he was given access to the email accounts of other employees for the purpose of monitoring incoming email in their absence, he took the opportunity to look at past content and sought to use the information gleaned from the emails for other purposes. While there is no complaint before me about this clearly inappropriate use and disclosure of the other employee's personal information, it is relevant to this review in that it points to the need for this public body to make some drastic changes with respect to the way in which it manages email, as discussed below.

DISCUSSION

The *Access to Information and Protection of Privacy Act* defines personal information as information about an identifiable individual, including:

- the individual's name, home or business address or home or business telephone number,
- an identifying number, symbol or other particular assigned to the individual,
- information about the individual's educational, financial, criminal or employment history,

Section 42 of the Act requires public bodies to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. This applies to the personal information of employees as much as to the personal information of the general public.

Section 47.1 prohibits employees from disclosing any personal information received by the employee in the performance of services for a public body, except as authorized.

Sections 43 and 48 set out when public bodies can, respectively, use or disclose personal information in their possession and/or control. These purposes include, among other things:

- for the purpose for which the information was collected or compiled or for a use consistent with that purpose;
- where the individual the information relates to has identified the information and consented, in the prescribed manner, to its disclosure;
- for the purpose of hiring, managing or administering personnel of the Government of the Northwest Territories or a public body;
- to an officer or employee of the public body or 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;

The first thing that has to be considered is whether the concerns raised by the Complainant in this case relate to his "personal information" as defined in the Act.

I have no problem finding that the following constitute the Complainant's personal information:

a) his name and position within the public body;
b) the specific circumstances surrounding his departure from the public body;
c) his signature;
d) the email address assigned to him by the public body during his employment.

The next question is whether or not the use and/or disclosure of this personal information was in contravention of the Act. On this issue, I am not convinced that all of the Complainant's complaints about the uses and/or disclosures of this information are well founded. In making this finding, I am not suggesting that everything the public body did was perfect or that changes

do not need to be made by the public body. There are certainly issues that need to be addressed which I will discuss below.

Dealing firstly with the disclosure by the Complainant's former supervisor of the circumstances of his departure from the public body. The public body admits that the Complainant's former supervisor disclosed some details about the Complainant's departure from the public body in four circumstances:

a) To advise an important client that the Complainant was no longer working with the public body.

Based on the specific circumstances of this case and the identity of the third party client involved (which have not been specified in this report in order to protect the identity of the Complainant) I am satisfied that it was a business imperative that the public body advise the third party that the Complainant was no longer employed with the department. There is no evidence that any specifics were provided other than to confirm that there was a vacancy in the position and the vacancy was due to a "personnel change" and not related to any wrongdoing on the part of the Complainant.

b) To advise an the Assistant Deputy Minister of another department of the circumstances surrounding the Complainant's departure from Department A.

Again, based on the specific circumstances of this case, and the fact that there were direct funding implications for both departments, I am satisfied that this disclosure was authorized pursuant to section 48 (g) and (k).

c) the disclosure to the Complainant's "friend"

While the third party to whom the Complainant's personal information was disclosed was a friend of his, the third party was also an employee, in a position senior to the Complainant and there was, once again, a legitimate business reason for disclosing the details of the circumstances surrounding the Complainant's departure to this individual so as to ensure that the Complainant's position was filled as quickly as possible because of ongoing and urgent work being done.

d) the disclosure in an “in camera” meeting

Again, this disclosure was necessary for the purpose of dealing with a possible settlement for the Complainant and I am satisfied that this disclosure was authorized pursuant to section 48 (g) and (k).

I find, therefore, that in the particular and specific circumstances of this case, none of the disclosures reported by the Complainant were contrary to the *Access to Information and Protection of Privacy Act*.

Moving on to the use of the Complainant’s electronic signature on a cheque run which occurred on the day of his departure but after he was no longer an employee of Department A, once again I cannot conclude that the public body improperly used the Complainant’s personal information. The Complainant had approved the use of his signature on the cheques while he was still an employee. There was, therefore, consent and no inappropriate use of his signature.

More problematic, however, is the continued use of the Complainant’s assigned email address long after he was no longer an employee. A public body email address is an identifier attached to a person’s name. As such, the email address assigned to the Complainant during his employment with the public body was his personal information, even though the address itself belongs to the public body. As such, keeping that email active means that there is an ongoing and significant breach of the privacy of not only the Complainant, but potentially of third parties communicating with that email address thinking that the person reading the correspondence is the identified person. Six months is far too long to allow an email address to remain active after an individual is no longer an employee of the public body.

I note that although government email addresses are intended primarily to allow employees to communicate with others within the public body and for the purpose of conducting the business of the public body, employees are also allowed to use these accounts for at least limited personal use which means that giving any other person access to the retained emails in the account is a potential breach of privacy. Furthermore, as pointed out by the Complainant in this case, there is a very real possibility that third parties have and will continue to direct emails to the email address which are meant to be personal to the Complainant. Keeping the email active without clearly indicating that the Complainant was no longer employed with the public body creates a significant risk of a breach of privacy for unsuspecting third parties.

Based on the information provided to me during this review, it appears that this public body does a very poor job of managing its email accounts. I can understand that when an employee leaves, the content of his/her email must be available, at least for a period of time, to allow it to be reviewed and important records retained. It seems to me, however, that can be done after the account has been shut down so that no new communications can be sent or received from that email address.

I am also concerned about the practice of monitoring the emails of employees who are not physically present in the workplace for one reason or another. This should not happen. There are other ways to ensure that important emails are received even when a person is not physically present at their computer. Whether someone is expected to be away for an extended period of time (for instance, on leave) or a shorter period, (such as a vacation), an automatic message can be placed on the address so that those who need to communicate with the department are re-directed to another employee who can assist. When someone leaves the organization, a message should be placed on the account immediately and left for a reasonable period of time and then the account should simply be shut down. The message should be discrete (ie: If you are wanting to communicate with the [position], please contact abc@gov.nt.ca). There is simply no good reason for keeping an email address active or for allowing access to email accounts by other employees when one is absent.

I therefore **recommend** that the public body in this case do a thorough review of its policies and procedures with respect to the establishment of email accounts, the management of those accounts, and the discontinuance of those accounts when an employee leaves the organization. This should be done in consultation with a technical expert and, once done, the new policies and procedures need to be communicated to all staff and put into effect. There should be one or two designated individuals within the department who are responsible for monitoring and enforcing these policies and for ensuring that email accounts are dealt with when an employee leaves.

Elaine Keenan Bengts
Information and Privacy Commissioner