NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER
Review Report 18-184

File: 17-225-4
July 3, 2018
Citation: 2018 NTIPC 12

BACKGROUND

The Complainant filed a request with my office to review whether or not his own personal information and the personal information of other employees was inappropriately collected, used and/or disclosed by the Department of Justice, his former employer. The complaints all arise from the Department's apparent failure to decommission the Complainant's email address at the end of his employment or to remove his permissions to access the GNWT servers. In particular, the Complainant alleged:

a) as a manager, he had had access to the "Peoplesoft" files of his employees and he continued to have access to sensitive third party personal information about his former employees through "PeopleSoft" long after he was no longer employed with the GNWT and no longer had any reason to have access to such information.

b) that he continued to receive automated email messages at his personal email account (@gmail.com) containing sensitive personal information about third parties in the workplace for up to eight months after his departure;

c) that his government email address remained active and monitored by another employee for at least six months after his departure;

He said that when he left his employment with the GNWT in 2014, his status in PeopleSoft was not properly updated to reflect his status as a former employee. Instead his access

rights as per his employment duties were delegated to his former supervisor without his knowledge or consent.

He noted as well that because his status in PeopleSoft was not properly updated, he retained access to the personal information of eleven employees within his former department. This allowed him access to information such as vacation leave accumulated and granted, sick leave accumulated and granted, overtime and lieu time as well as other personnel management information.

In addition to the information he had access to when logged into PeopleSoft, the program was also forwarding him auto-generated emails containing the personal information of other employees, including wage information, requests for approval of leave, and information about another employee's end of contract.

He said that he brought his concerns regarding this issue to the attention of various individuals within the GNWT over a period of several years. With respect to his apparent ongoing access to the PeopleSoft information of other employees, he was told that because of the circumstances of his departure (he was no longer working for the Department but was still an "employee" for the purpose of pay and benefits for a period of six months), though he was no longer an employee, he was still being paid, which meant that he still had to be attached to a position number and because that position number was that of a manager, it included various permissions needed to supervise employees.

He also noted that although he brought the matter to the attention of various individuals within the GNWT a number of times, he was never asked to delete, destroy or return the personal information in his possession. In fact, he retained that information at least until he filed his complaint with my office in late 2017 because he included several screen shots to support his complaint.

Finally, he noted that because the public body did not decommission his email address but instead had another supervisor monitoring it, his privacy was breached in that there

was a very real possibility that emails of a personal nature were sent to his former GNWT address and were read by the supervisor receiving his emails. He quoted from the 2016/2017 Annual Report of the Information and Privacy Commissioner of the Northwest Territories in which Review Report 17-158 was discussed:

> [...] the failure of the public body to decommission the Complainant's email address after his departure constituted a breach of the privacy of not only the Complainant, but also of others who sent emails to that address not knowing that someone other than the complainant was receiving them. She found that a public body email address is an identifier attached to a person's name and that 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 was an ongoing 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. She found that 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.

THE DEPARTMENT'S RESPONSE

I asked the Department to explain, firstly, how the breaches were allowed to occur and to continue, notwithstanding the Complainant's attempts to have his supervisor deal with the situation. The Department acknowledge that it was aware of the initial issues that led to the Complainant receiving notices through the PeopleSoft automated notification system which sent notices to his personal email address (not his GNWT email address) about the leave and step increments of some other employees. The Director of the division followed up with the designated Client Services Manager with the then Department of Human Resources (now the Department of Finance), and believed that the necessary steps had been taken to address the issue. The Department of Justice was unaware that the issue

had continued until December. They indicated that in investigating the matter, they determined that the incident took place due to an unusual situation where the applicant - who during this time period, was under a termination agreement with the Department - continued to be identified as an active employee in the PeopleSoft system. This occurred because the system is designed to identify employees as being either active or terminated. Because of the unusual nature of a termination agreement where the employee continued to be compensated, and therefore considered active by the system, a request for a manual override of the notification system should have taken place. The manual override would have allowed for the applicant to continue to be compensated but would have addressed the delegation notices that were sent to him during that time period. They noted that as a result of this incident, the Department of Justice was working with the Department of Finance to implement a process that will identify the need for manual overrides to the notification system for employees identified on a termination agreement.

In response to my request for more information about how access to the PeopleSoft program is controlled and what limits are in place to block access among employees, the Department advised as follows:

> The PeopleSoft system is structured as a role-based access control system. This type of system restricts access to authorized users, and within the user group access is further restricted to information necessary for the user to perform their duties. Authorized GNWT personnel may have access to an employee's personal information depending on the responsibilities of their position, what information they can access and view differs depending on those responsibilities.
>
> In PeopleSoft, managers/directors with direct report employees have access on PeopleSoft to their employee's leave information. They are able to view an employee's leave requests and leave balances, their PeopleSoft number and the types of leave requested. For example the code "AD/"

> indicates the leave is considered annual leave, whereas "SL1" identifies sick leave. Only the code is available for review, and no further detail on the underlying reason for the leave is identified.
>
> Managers and Directors who are also responsible for budgets in relation to salary dollars are also able to view limited budget information related to salary such as the employee's pay schedule and step. They are also provided with access to performance appraisal information if the employee falls under their supervision.
>
> ...The system is designed to limit the personal information of employees to those who are authorized to view it and use it.

I also asked the Department to advise me as to the protocol in place for decommissioning government email addresses after an employee leaves. They noted that the responsibility for decommissioning government email addresses rests with the home department of the former employee. The Department of Finance had provided guidelines outlining steps to be taken when an employee leaves, including decommissioning the email address. Each individual department, however, is responsible to send an appropriate request to the Technology Service Centre to undertake this step.

They were unable to explain why this particular account had been left open for almost six months, but noted that steps were being taken to address the issue, including a revision to its “offboarding” protocol. This revision will allow an employee’s email account to remain open for a maximum of two weeks to identify that the employee is no longer with the Department and to inform correspondents where their inquiries can be redirected. Further, employees will be made aware of this protocol prior to their departure.

The public body did confirm that the Complainant did not have access to his email account after his departure.

THE COMPLAINANT'S FURTHER SUBMISSIONS

I provided the Complainant with a copy of the Department's submissions and invited him to provide any further input he thought might assist me in my review. I asked him, in particular, to address why he was receiving automated messages from PeopleSoft at a personal email address. He noted that:

> The mechanism to change a preferred email in PeopleSoft is quite simple - the option appears under the "self service" tab under "personal information" (see page 4 attached). Note that setting a preferred email is as easy as selecting a check box. Please also note that it is possible to enter any email address to be used as the preferred email address.

Because he would no longer have direct access to his government email account, he changed his preferred email address before he left so that he could continue to receive important information and documents, such as notifications that his T4 slip was available. He notes that when the public body changed his preference back to his old government address, they also cut off his ongoing access to his own PeopleSoft information, which may have created a number of difficulties for him.

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, and
- 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;

1. Decommissioning of email address.

This is not the first time that the failure to decommission an email address has led to privacy concerns. I reviewed a similar issue last year in relation to an employee who had ceased working with Aurora College in Review Report 17-158. In that report I noted that:

> 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 noted 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. This means that giving any other person access to the retained emails in the account is a potential breach of privacy. It is also a potential breach for those thinking that they are communicating with the individual on a personal basis when someone else is monitoring those emails or they are being redirected to another employee. Keeping the email active without clearly indicating that the Complainant is no longer employed with the public body creates a risk of a breach of privacy for unsuspecting third parties.

I understand that when an employee ends his/her employment, 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. Most email in a GNWT account will be the information of the GNWT and it needs to be properly filed and indexed in accordance with good file management practices. It seems to me, however, that this can be done after the account has been shut down so that no new communications can be sent or received from that email address. What should happen when an employee leaves is that a message should be placed on the account immediately to make it clear that the email address is no longer in use. The message should be discrete (ie: If you are wanting to communicate with the [position], please contact abc@gov.nt.ca). This message should be left for a reasonable period of time (the two weeks suggested by the Department seems to be a good number) and then the email address should be completely shut down.

I **recommend** that the department do a thorough review of its policies and procedures with respect to the management of email accounts and, in particular, what must happen when an employee ceases to work for the GNWT. I further **recommend** that there be one or two individuals within the department or within each division of the department responsible for ensuring that these policies are followed when an employee leaves.

2. Ongoing Access to PeopleSoft

This situation creates a number of issues for me. The most significant of these is the fact that when the Complainant changed his preferred email address for receiving notices, it resulted in notices being sent to him not only with respect to his own employment matters, but also about other employees who he used to supervise. The fact that he received automatic email from the system about the employment status of his former staff members is clearly a breach of their privacy.

While the public body suggests that this is an “unusual” circumstance in that the Complainant remained on the payroll after his actual employment, I am not convinced that this situation is all that unique. Many people retire after many years with the GNWT and take unused holidays immediately prior to their retirement, sometimes several months. They are no longer “employees” with any authority or right to have access to the files of those they might have managed, though they will continue to be paid for a period of time after they are no longer in the office. Based on the public body’s comments, each one of these people will continue to be associated with a position number so that they can continue to be paid, which means that they will continue to have access to the PeopleSoft information of their former staff and, like the Complainant in this case, would likely to continue to receive automatic notifications from the system about those employees. This is unacceptable.

A second concern is that any manager or supervisor can designate a private email address, outside the relative security of the GNWT system, in his/her PeopleSoft preferences such that notifications about third parties’ employment and benefits are being

sent to that outside email address rather than to a secure GNWT address. This is a breach of the privacy of those employees and should not be allowed or even possible.

I therefore **recommend** that a technical solution be found and implemented immediately on a system wide basis that

a) allows a former employee to continue to have access to his/her PeopleSoft information for as long as needed to ensure that all employment-related correspondence is finalized; and
b) allows a supervisor/manager to set his/her preferences in PeopleSoft so that he receives notices about his own employment matters at a personal email address rather his/her GNWT assigned address;

BUT

c) does not give that former employee access to or notices about any other employee; and
d) does not forward messages from PeopleSoft about any other employee outside of the GNWT system

I further **recommend** that specific employees, either within the Technical Services Centre or within each department or division, be clearly designated as being responsible for appropriate "off-boarding" of employees so that these appropriate procedures become routine and consistent.

To the extent that this is outside the mandate of the Department of Justice, I **recommend** that this Report be provided to the appropriate department for implementation.

Finally, I **recommend** that steps be taken to ensure that any third party personal information received by/obtained by the Complainant since the end of his employment with the GNWT have been returned and/or destroyed.

Elaine Keenan Bengts
Information and Privacy Commissioner