NORTHWEST TERRITORIES
INFORMATION AND PRIVACY COMMISSIONER
Review Report 20-237
Citation: 2020 NTIPC 38

Files: 19-218-4 and 19-233-4
July 24, 2020

BACKGROUND

On August 27th, 2019, our office received a notice from the Department of Education, Culture and Employment (ECE) that they had become aware that the identity of an employee who had submitted a report under the Safe Disclosure Program had been improperly, but unintentionally, disclosed through postings to an Outlook calendar open to a number of the employee's co-workers.

On September 16th, we received a privacy breach complaint from the employee indicating that he had discovered that his name had been disclosed to others in his work group in relation to a Safe Disclosure matter and asked our office to review ECE's handling of his personal information.

As the breach notification and the breach complaint relate to the same incident, this office combined the files and proceeded with one review.

The Complainant was contacted by a co-worker while he was on annual leave with a concern about information the co-worker had seen in a supervisor's "Outlook" calendar. The information was contained in two appointments appearing in the supervisor's open calendar, which had been made accessible to the Complainant's entire work group to allow for more efficient scheduling of meetings. One of these appointments contained a link to an email chain in which the Complainant's name was revealed as the individual responsible for a report made under the Safe Disclosure policy. The Complainant noted that the Safe Disclosure process was meant to be entirely confidential. He pointed me to a document entitled *Memorandum of Agreement for the Application of a Safe Disclosure* which states in its guidelines that:

> Consistent with the rules of natural justice and procedural fairness, care must be taken at all times to protect the identity of the employee making a disclosure, any witnesses and the alleged wrongdoer. This does not preclude advising the wrongdoer of the name of the person who made the disclosure, the nature of the disclosure, including relevant information as necessary. (pg.1).
>
> ....
>
> Disclosure files must be treated as strictly confidential and maintained in a secure location and manner.

THE DEPARTMENT'S RESPONSE

The Department confirmed that one of the two calendar entries in the Supervisor's Outlook calendar contained a link to an email chain. They state:

> While [the Complainant's] personal information is not disclosed within the meeting subjects, the second meeting invite contained an email string that was marked "Sensitivity: Confidential" for each of the six emails included in the string. It is only by opening the meeting invitation and reading the entire email string would one discover at the very bottom, that [the Complainant] made a safe disclosure of information submission.

The Department further confirmed that the Supervisor shared her Outlook calendar with all ten of her staff as well as at least two others "for the purpose of booking meetings and identifying her availability". The Supervisor was not the person who created either the email chain or the meeting notice. The meeting appeared in the Supervisor's calendar when she accepted an invitation to attend a meeting to discuss the Complainant's Safe Disclosure appeal. The string of emails attached to the meeting invitation was intended to provide background information for the proposed meeting.

The Department confirmed that the email string had not been password protected and that anyone with whom the Supervisor shared her calendar could have accessed the attached email string.

The Department indicated that “Outlook” does have a “private” function that can be enabled for specific meetings to protect the sharing of information. However,

> if an Outlook Calendar is shared with people who have "Read" permissions, the "Private" function will not prevent them from seeing the details of meetings. Additionally, anyone with "Read" access could use programmatic methods or other email applications to view details of private items.

They indicated, as well, another security function that Outlook offers is to provide “permission levels” so that permission can be granted to specific individuals to read, create or change items in Outlook as determined by the owner of that Outlook calendar. There is no indication, however, as to whether or not this feature was activated with respect to this meeting/email exchange.

The Director responding to the privacy breach complaint conceded that there were no policies or guidelines in place, or even any specific instructions on how to use the various security features of Outlook. The Director did, however, commit to providing a presentation at a senior management meeting to identify operational protections which should be used to avoid similar breaches in the future.

DISCUSSION

One of the purposes of the *Access to Information and Protection of Privacy Act* as set out in section 1 is to make public bodies more accountable to the public and to protect

personal privacy by preventing the unauthorized collection, use or disclosure of personal information by public bodies. Part 2 of the Act outlines the rules surrounding how and when a public body can collect, use and disclose personal information. Section 42 provides:

> 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.

Section 43 sets out those circumstances in which personal information can be used by a public body as follows:

> 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.

Section 48 sets out a series of purposes for which information can be disclosed, including:

- for the purpose for which the information was collected or compiled or for a use consistent with that purpose
- to an officer or employee of the public body where the information is necessary for the performance of the duties of the officer or employee

The issue in this case is whether there was a disclosure of the Complainant's personal information and, if so whether it was a disclosure authorized by the legislation.

1. Was the information identifying the Complainant as the person who had made the complaint under the Safe Disclosure policy the personal information of the Complainant?

The Safe Disclosure program is contained in a memorandum of agreement between the GNWT and the Union of Northern Workers. The agreement was intended to provide procedures for employees to safely disclose allegations of wrongdoing in the workplace. The Memorandum of Agreement includes the following intention behind the agreement:

> The parties desire to create an environment where employees who in good faith believe a wrongdoing has occurred can bring that forward freely in a confidential and safe manner. The parties agree that employees should never have to fear reprisal when they come forward in good faith and raise concerns about wrongdoing.

The Agreement goes on to outline how the Agreement will be implemented:

> Providing employees with access to an independent mechanism for them to confidentially report situations where the employee in good faith believes that there has been a misuse of public funds, an illegal act, gross mismanagement or a substantial and specific danger to health and safety or to the environment;...
>
> Providing employees who in good faith make such a report, protection from reprisal by the Employer.

With this in mind, it is clear that those who submit reports under this process are entitled to the utmost confidentiality so as to protect them from reprisals not only from superiors but from others who might not appreciate being implicated in such a report of wrongdoing. The fact that an identifiable individual had made such a complaint clearly constitutes that individual's personal information. Furthermore, the disclosure of the name, combined with the fact that this person had made such a complaint would be protected from disclosure under Part I of the Act, as disclosure would definitely result in an unreasonable invasion of the individual's privacy, particularly in light of the clear intention to provide confidentiality. I have no hesitation in concluding that the Complainant's name, combined with a statement that he was the person who made the complaint is the Complainant's personal information.

2. Was there a disclosure of that information and, if so, was it an authorized disclosure under the Act?

The Department concedes that information about a confidential process was included a calendar entry in the Supervisor's Outlook calendar. They seem to feel, however, that because the calendar belonged to the supervisor, because the only way that the offending email could be accessed would be to click on a link clearly intended only for the Supervisor, and because every one of the chains in the email containing the information in question was clearly marked with the words "Sensitivity: Confidential", the problem was not with the link but was rather with the other employees (including the Complainant) who clicked on the link knowing that the communication was intended for the Supervisor only.

While all of that may be true, the fact is that by including a link to the email chain in an open Outlook calendar to which many people had access, the otherwise confidential communication became accessible to all those who had access to the calendar, whether they looked at it or not, and whether they should have looked at it or not.

Someone clearly did look at it, opened the link and alerted the Complainant who in turn also opened the link. As soon as the appointment was listed in the Supervisor's calendar, the information in the linked email was "disclosed" for a purpose inconsistent with the purpose for which it was collected. Furthermore, other than the Supervisor, no one else who had access to the calendar had an operational need for the information – it was not needed by any of the other employees with access to the Outlook calendar for the performance of their employment duties. This constitutes a breach of the Complainant's privacy.

CONCLUSION AND RECOMMENDATIONS

I find that there was an unauthorized disclosure of the Complainant's personal information when the appointment containing a link to an email chain in which reference was made to the Complainant in the context of a Safe Disclosure process was posted to the open calendar. While the disclosure was inadvertent, and it is concerning that other employees who were not involved in the proposed meeting took it upon themselves to click on the link and then follow the email chain through a series of emails with the word "Confidential" clearly included several times, the posting of the link itself constituted an unauthorized disclosure because it gave easy access to individuals who had no operational need for the information included.

Ultimately, this breach could have been avoided in several ways:

a) by configuring the security settings in the Outlook calendar appropriately to restrict access to links;
b) by encrypting or password protecting the attached email;
c) by sending sensitive information in separate encrypted emails rather than attaching it to the meeting invitation.

I have no doubt that neither the individual who sent the meeting message nor the Supervisor gave much thought to what was included in the meeting invitation. That, ultimately, is the cause of the breach. More attention needs to be paid to what is put in email communications, and who will see them, even within the organization.

I therefore recommend:

1. that the Department of Education, Culture and Employment take immediate steps to ensure all employees who use an open Outlook calendar ensure that the security and privacy functions of the application are properly configured so as to manage who can see what;

2. that the Department take steps to ensure that managers and executives who use an open Outlook calendar are fully and properly trained in the use of the privacy/security features of the application and are using the privacy functions appropriately;

3. that the Department provide all employees with clear direction to encrypt or otherwise protect access to correspondence containing personal information, including confidential personal information of employees.

Elaine Keenan Bengts
Information and Privacy Commissioner