NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER
Review Report 20-215

File: 19-118-4
January 23, 2020
Citation: 2020 NTIPC 4

BACKGROUND

In February 2019, the Applicant wrote to this office and raised two privacy issues. The first issue related to an access to information request he had made to the Government of the Northwest Territories (GNWT) Department of Industry, Tourism and Investment (ITI). He claimed that, during the process of responding to his request, the department breached his privacy by disclosing to his supervisor that he was the person making the access request. He alleged that his name should not have been disclosed as being the Applicant.

Secondly, the Complainant alleged that his personal information was then inappropriately used by his supervisor when the supervisor used information he obtained as a result of his employment duties in a manner contrary to the use provisions in section 43 of the Access to Information and Protection of Privacy Act (ATIPPA) in accusing the Applicant of unauthorized viewing of certain correspondence.

ISSUES

This review raised two issues:

1. Was the Complainant's privacy breached when he was identified as the Applicant in an access to information request?

2. Was the Complainant’s privacy further breached when his supervisor used information garnered in the context of his employment duties in a context that was not anticipated by the Complainant?

DISCUSSION

1. Was the Complainant’s privacy breached when he was identified as the Applicant in an access to information request?

In this case the Complainant became aware, through comments made in an investigation report, that his supervisor knew his name when he submitted his access to information request. The Applicant claimed this was a breach of his privacy as the supervisor should not have been told that he was the person making the request.

The Department of ITI provided an explanation for why the Applicant's name was released to the employees who were the subject of his access to information request. The Department admitted that the individual tasked with responding to the request made an error in sending a single email to all individuals named in the request asking for responsive records. ITI said that this was not consistent with how requests are currently handled by the Department where emails asking for responsive records are sent to each person named in a request individually so that the named individuals are not aware of each other. They said that this error appeared to have contributed to the supervisor's allegations against the applicant, since the supervisor was thus made aware that another named employee (hereinafter referred to as "A") had also been named in the request.

In terms of their normal process, and particularly where the Applicant is requesting his/her own personal information, and there is evidence of conflict between the Applicant and individuals named in the request, the Department said that it would typically first conduct a search for all records without the aid of individuals named in the request. After the initial search, the Department would rely on individuals named in the

request to identify any additional records they may be aware of related to the request. In the normal course of this process, this would involve sending an email to each of these individuals informing them of the nature of the request. Since it is a request about a person's personal information, the name of that person would have to be communicated, though without necessarily indicating that they are also the requester.

Currently the Act is silent with respect to naming an applicant in an access to information request. However, it is important to note that Bill 29: *An Act to Amend the Access to Information and Protection of Privacy Act* has been assented to, though not yet brought into force. This Bill sets out section 6(4):

> 6 (4) The identity of an applicant shall be kept confidential by the head of the public body and the coordinator designated under section 68.1, and may be disclosed only to the extent required to respond to the request for access.

This section codifies the current general uncodified practice of not disclosing the identity of an individual making an access to information request. Under the new provisions, the Applicant's name will only be allowed to be disclosed to the extent required to respond to the request for records. This means that the public body must take steps to protect the Applicant's identity and only disclose it if it is absolutely necessary in order for a proper search of the records to be done.

That was not done in this case, as the Department has admitted. There was an error made and the supervisor was made aware of the Applicant's name when it was not necessary to respond to the Applicant's request for records.

Also set out in Bill 29 is the provisions with respect to breaches of privacy. When in force, section 49.8 will state:

49.8. For the purposes of this Division, a breach of privacy occurs with respect to personal information if

(a) the information is accessed and the access is not authorized under this Act;

(b) the information is disclosed and the disclosure is not authorized under this Act; or

(c) the information is lost and the loss may result in the information being accessed or disclosed without authority under this Act.

Even though Bill 29 is not yet in force, I still find that the release of the Applicant's name to the supervisor without a need to do so for the access to information request was a breach of the Applicant's privacy. The new Act will state that it is a requirement to not reveal the Applicant's identity. This would be a clear contravention of section 6(4). Even with the Bill not yet coming into force, disclosing the Applicant's name when not necessary is an unauthorized disclosure pursuant to section 47 which provides that:

47. A public body may disclose personal information only

(a) in accordance with Part 1; or

(b) in accordance with this Division.

There is nothing in Part 1 or Section 48 that would authorize disclosure of the Applicant's name to the supervisor in the context of his access request. To do so was not authorized by the Act.

I find that a privacy breach occurred in these circumstances.

2. Was the Complainant’s privacy further breached when his supervisor used information garnered in the context of his employment duties in a context that was not anticipated by the Complainant?

The second issue in this review is whether the supervisor improperly used information about the Applicant that he had obtained as a result of his employment duties in a manner contrary to section 43 of ATIPPA by accusing the Applicant of unauthorized viewing of certain correspondence involving another employee (referred to herein as “A”). In an investigation report, the supervisor alleged the Applicant may have been using his access abilities through his employment to gather information about how to direct his ATIPP request. This was set out in an investigation report, of which only several pages were shared with this office during the review process.

In response, the Department said that while they did not feel they could confirm or deny whether the disclosure of this information may have been authorized under section 48 of ATIPPA, because the supervisor received the personal information through an error made in the handling of the original request, they concluded that the disclosure of this mistakenly acquired information was also inappropriate.

The Department of ITI said that while they felt that it is appropriate for employees to report in some fashion unauthorized access of government records by another employee if there is a reason to believe that this has occurred, they were not aware of any existing protocols or procedures in the Department of ITI that would inform employees on how to accomplish this in an appropriate manner. Therefore, they said the supervisor would likely have been unaware of the proper approach to raising his concern about the Applicant if in fact this was not one of the issues being investigated under the circumstances.

I agree with the Department in its conclusion that the disclosure of this mistakenly acquired information was inappropriate. The supervisor was not supposed to be made aware that it was the Applicant requesting the relevant records. He should not have known this information. He then took this information and used it in an investigation about the Applicant. Disclosing this information was not a disclosure authorized in Part 1 or section 48 of the Act.

It also was not an authorized use of the 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.

The information was not collected for the purposes of the investigation. It was collected for the purposes of processing an access to information request. The Applicant did not consent to this use. Finally, the use was not one that would have been authorized pursuant to Division C.

I find that by using the information from the access request for the investigation and disclosing that information to the investigators, the supervisor inappropriately used and disclosed the Applicant's personal information.

CONCLUSION AND RECOMMENDATIONS

I find that when the Department of ITI released the Applicant's name to his supervisor, that this was a breach of the Applicant's privacy. I make the following recommendations:

(a) I **recommend** that the Department of ITI review and update its policies to reflect the pending coming into force of Bill 29, including a requirement to protect the identity of applicants.

(b) I **recommend** that the Department of ITI provide updated and ongoing training to ATIPP Coordinators in the department to ensure consistent approaches and to reflect the new provisions coming into effect within the next few months.

I also find that there was an inappropriate use/disclosure of the Complainant's personal information when knowledge obtained by the supervisor inappropriately through the access request was then used in an investigation apparently in an attempt to discredit the Complainant. I make the following recommendations in that regard:

(c) I **recommend** that the Department provide privacy training to all employees in a supervisory position for the purpose of ensuring an understanding of how the personal information of employees can be used and/or disclosed in accordance with the *Access to Information and Protection of Privacy Act*.

(d) I **recommend** that the Department develop a policy or procedure to provide an appropriate process for employees to report privacy breaches to appropriate individuals within the division or department so as to avoid situations like the one outlined in this report where the disclosure was made in an inappropriate forum

Once privacy is breached, there often little, if anything, that can be done to address the harm done as a result of the breach. It is for this reason that it is important for all public bodies to educate their staff adequately to avoid inadvertent breaches of privacy.

Elaine Keenan Bengts
Information and Privacy Commissioner