NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER
Review Report 20-212

File: 18-201-4
January 9, 2020
Citation: 2020 NTIPC 1

BACKGROUND

In late 2018, the Complainant wrote to the Information and Privacy Commissioner (IPC) and alleged that his personal information had been inappropriately accessed and disclosed by a person who worked in the Government of the Northwest Territories (GNWT) Department of Finance. The Complainant is a counselor who works for the GNWT. One of the Complainant's clients (hereinafter referred to as "A") told him that another GNWT employee (hereinafter referred to as "B") with whom he had a relationship, had snooped into the Complainant's personnel file and gathered information about the Complainant for the specific purpose of discrediting the Complainant professionally. Specifically, A said that B had told him that B had looked up the Complainant on PeopleSoft (the GNWT's electronic file system) and said that the Complainant was "just a [designated profession]" and not a counselor. A said that B also told him how much the Complainant earned, where the Complainant lived, what the Complainant's education was and all about a medical travel trip including that the Complainant had gone to a named Southern community with a named medical escort.

The Complainant raised this concern with his supervisor on October 23, 2018. By December 12, 2018, he had not been provided with an update into his concerns so he filed this complaint with the Office of the Information and Privacy Commissioner. On January 12, 2019, the Department of Finance appointed two investigators to look into the alleged breach of privacy (note here that the investigation summary was dated 2018 but I believe this was an error and should have been 2019). The investigators submitted their report on March 1, 2019, only a summary of

which was provided to this office. The investigators concluded that the Department of Finance had not addressed the alleged breach in a timely manner. They also indicated, however, that on a balance of probability they could not conclude that B had breached the privacy of the Complainant by accessing and disclosing personal information contrary to the *Access to Information and Protection of Privacy Act* (ATIPPA), as alleged by the Complainant.

ISSUES

This review raised the following issues:

1. Did B have access to either paper or electronic records in relation to the Complainant's employment and, if so, is it reasonably possible to conclude that B accessed that information, either as an employee authorized to do so in the course of employment or because of unauthorized snooping?

2. Is it reasonable to conclude that B disclosed personal information about the Complainant, which was known to B because he had access to the Complainant's personnel records (whether or not access was authorized) contrary to section 47.1 of ATIPPA?

4. Did the Department of Finance fail to address the complaint in a timely manner?

DISCUSSION

As a preliminary matter, I have a number of concerns about both the investigation and the findings of the investigators. The GNWT has a clear duty under the Act to protect information from unauthorized collection, use or disclosure. Section 42 of the Act specifically says:

> 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 of ATIPPA sets out when the public body (and by extension, an employee of a public body) may "use" personal information. 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 term "use" is not defined in ATIPPA but it is in the Health Information Act (HIA):

> "use", in relation to information, means to handle, deal with or apply information for a purpose, including to reproduce or transform it, but does not mean to collect or disclose information.

In Review Report 088-2013, the Saskatchewan Privacy Commissioner found that looking at personal information without a work-related cause to do so is a "use" of the Complainant's personal health information and also an unauthorized use, as the Act did not authorize it. I find HIA and the case law instructive. Looking at personal information within the course of one's employment with the GNWT constitutes a "use" of that information. When an employee looks at a person's records and sees that person's personal information without an authorized reason to do so, or so-called "snooping", it constitutes an unauthorized use of personal information.

Similarly, pursuant to section 47, a public body (and by extension employees of a public body) may only disclose personal information obtained or retained by it in the circumstances outlined in the Act. Section 47.1 further clarifies that an employee "shall not, without authorization, disclose any personal information received by the employee in the performance of services for a public body". If B disclosed information to A that was obtained by B as a result of his employment responsibilities, or as a result of unauthorized snooping, this is all that is necessary to establish a breach of privacy contrary to the legislation.

It is to be noted that the Department's investigation into this matter was not done from the perspective of the *Access to Information and Protection of Privacy Act*, but rather from the perspective of an internal workplace incident or event. The focus for someone investigating a workplace complaint is about labour relations. The focus of an investigation under the ATIPP Act must be the Act. And because we did not receive the report itself, but only a summary of the report, there are clearly gaps in our understanding of the conclusions reached by the investigators. That said, what we did receive suggests a poorly executed investigation which, frankly, reaches conclusions that do not accord with the facts.

In undertaking the investigation, the investigators interviewed the Complainant, B and a Department of Finance employee who provided general information regarding the content and administration of Human Resources files maintained by the GNWT. They also interviewed a supervisor in relation to the lack of timeliness in responding to the Complainant. They did not interview A, indicating that B had made allegations of violence and abuse at the hands of A and they felt that the potential of harm to B therefore outweighed the probative value of the evidence they might receive during an interview. A's evidence, however, was critical to understanding the sequence of events and whether or not there was a breach of the *Access to Information and Protection of Privacy Act*. The decision to not interview A tainted the investigator's ability to properly assess the truthfulness of B's self-serving denials.

This brings me to another concern. In the course of my review of this matter, I requested a copy of the Investigation Report prepared by the investigators. However, I was provided only with a summary of that report and not the full investigation report. Pursuant to section 49.3 of ATIPPA, reviews are conducted in private. The IPC is entitled to the production of any record to which the Act applies, pursuant to section 49.4 of ATIPPA. My office indicated that it would not share the report with the Complainant and the issue of providing it to the Complainant was not even at issue in this case. Without the full investigation report, I have no way to fully assess why the investigators reached the conclusions which they did, which on the face of the summary report, are contrary to the evidence received.

1. Did B have access to either paper or electronic records in relation to the Complainant's employment and, if so, is it reasonably possible to conclude that B accessed that information, either as an employee authorized to do so in the course of employment or because of unauthorized snooping?

The Complainant alleged that B snooped into his personal information. B was alleged to have looked up and disclosed information about the Complainant's home address, education and salary. B was also alleged to have looked at information about the Complainant's previous employment and the circumstances of the Complainant's departure from another community as a result of an "incident". Finally, B was alleged to have accessed and disclosed specific and detailed information about the Complainant's recent medical travel, including the name of the person who accompanied the Complainant on that trip.

The Department of Finance's investigation concluded that these allegations were not able to be confirmed and that all of the information in question could have come from sources other than the Complainant's personnel files.

The investigators reviewed the paper version of the Complainant's personnel files, as well as his electronic personnel files and copies of documents relating to medical travel (the benefits file) which they believed were the files B would have had to access in order to have viewed the information, as alleged. No audit appears to have been done to determine who had accessed the Complainant's electronic files. This may be the most glaring gap in the investigation of the matter. Surely the GNWT has the ability to audit who has access to an electronic file, particularly where, as here, the file contains significant amounts of sensitive personal information. The fact that this step was not taken was a serious flaw of this investigation. I suppose it is possible that an audit was done but the results of it were not included in the summary of the investigation report, which was all that I received. However I doubt that is likely as the results of an audit would have shown clearly whether B had accessed the Complainant's personnel and/or benefits files and so would be enormously relevant to the investigation's findings.

When interviewing B, the allegations of "snooping" were, not surprisingly, vehemently denied. B told the investigators that he believed that A made these allegations to further a vendetta resulting from strained relations between A and B. B told the investigators that he knew nothing about the Complainant's employment, but this is clearly not entirely true because it was part of B's job description to assist employees with medical travel and everyone acknowledges that B assisted the Complainant with his medical travel. This taints the rest of the statements made by B in the investigative process.

One of the factors the investigators considered in concluding that it was unlikely that B had done what was alleged was that there was a "no contact" court order in place between A and B at the time when the Complainant had been working in his previous employment where the alleged "incident" which led to the Complainant's relocation had taken place. They also noted that B was on leave from his employment when the incident occurred. However, these factors

are not particularly helpful as A could have told B this information after the “no contact” order was completed, or even while it was still in place. The existence of a no-contact order is not evidence that it was respected by either A or B and, in light of the clearly acrimonious relationship between these two, it is not unreasonable to consider that there may well have been ongoing contact, despite the order. Similarly, it is clear, as outlined below, that B did have access to many of the Complainant’s personnel records at the time the allegations of the breach were made. B could have accessed information about the Complainant’s previous employment and the circumstances of his departure, to the extent that this information was included in the Complainant’s records, any time after it happened. The fact that B was on leave at the time of the incident is, frankly, an irrelevant consideration and certainly not a fact that serves in any way to exonerate B, or even to serve to raise a reasonable doubt that he used or disclosed the Complainant’s personal information.

A factor that the investigators found to be determinative in finding that it was unlikely B had access to information regarding the Complainant's qualifications was that paper based personnel files containing this information were kept in a locked cabinet, on a different floor from where B worked. This conclusion, however, is also not clearly supported.

Firstly, even if all of the personnel files were in paper form (which they clearly are not), there was no attempt made to assess any security measures in place with regards to protecting the privacy of these files or whether B would have been able to bypass any such security. It appears from the descriptions provided that, while the records were in a cabinet, that cabinet was in an area open to employees (and perhaps others). There does not appear to have been any log- in system to track who had access to the paper files nor was there any confirmation that the “locked” cabinets remained locked during the work day or were simply locked at night. The “keeper” of the paper records does not appear to have been interviewed. Nor was there any effort to determine who had access to the key to the cabinet or whether there was more than

one key, where the key (or keys) was located or who knew where the key(s) was stored. Without having explored these issues, I find it difficult to accept the “finding” that B had no access to the paper personnel records of the Complainant.

Secondly, while there was an indication that the paper file contained information in relation to the Complainant’s work history with the GNWT, including his earlier employment in another community, there is no indication that these paper records were the only records containing this information. The GNWT operates in an electronic world and I expect that any paper records were also electronically available. In fact, the report summary we received confirmed that the electronic personnel file included job offers “and correspondence” from early 2016 to the present, as well as the Complainant’s resume and information in relation to the Complainant’s medical travel.

The investigators conceded that an employee in B's position would have had access to information about the Complainant's home address, salary and medical travel in the electronic Peoplesoft program. Again, I am concerned that no audit was done of this system. A thorough investigation would not have relied solely on the word on B, who had much to lose by admitting he had access to this information. An audit would have confirmed much more definitively whether or not B had looked at the Complainant’s file.

The investigators also conceded that "there is evidence that B knew the information regarding the Complainant's medical travel". Without the full investigation report, it is not possible to fully understand what that sentence means. However, the Complainant told the investigators that he had dealt with B when he made arrangements for medical travel, so it is likely that this was the evidence the investigators were referring to. Again, an audit could have confirmed that B had had access to these files, even if that access was in the course of his employment duties. Regardless, it is apparent that B did have access to this information.

With regards to whether B had looked up information about an "incident" at the Complainant's former employment, the investigators pointed out that there was no record of an "incident" in the Complainant's personnel or benefits files, or in Peoplesoft. However they said that there was a "passing reference to" facts surrounding a response to a first level grievance. I do not understand how the investigators could have concluded that there was no record of an incident when there was a grievance document on file. Again, it would have been helpful to see the full investigation report in this regard. In any event, grievance documents typically set out that there was some kind of incident, and discipline which was being grieved as a result of it. This grievance document could have been the document that B was alleged to have viewed to tell B that there had been an incident following which the Complainant had left his employment.

Even if we accept that the information about the "incident" may not have come from a GNWT record but was, as the investigators conclude, more likely gleaned this from more public sources (i.e. local gossip), this does not address the source of the other detailed information about the Complainant's employment including his employment history, his training, his specific income and/or his medical travel. Because one piece of information was from a non-GNWT source does not lead to the inevitable conclusion that none of the information came from a GNWT source, which is what the investigators concluded.

In fact, it is clear that B had access to specific information about the Complainant's educational background, credentials, employment history, salary and medical travel via the Complainant's electronic personnel and travel records and the PeopleSoft system and it is reasonable to conclude that B did see this information as a result of his employment duties with the GNWT. Just because some of the information passed on to A may have been acquired through gossip (assuming that is the case), that does not mean all of it was. The investigators gave far too much weight to this possible anomaly and not nearly enough weight to the fact that B clearly had access to all of the other information alleged to have been improperly disclosed.

I find that B had access to most, if not all, of the Complainant's personal information which is alleged to have been improperly disclosed.

2. Is it reasonable to conclude that B disclosed the Complainant's personal information?

The Complainant alleged that B had taken the information obtained as a result of his employment duties, or as a result of snooping, and disclosed the information to A.

Although the investigators conceded that B had access to information regarding the Complainant's salary, address and medical travel, they came to the conclusion that there was not enough evidence to find that B disclosed personal information as alleged. They based this finding on 4 pieces of evidence.

Firstly, they were not convinced that there was any information which B might have had access to as a result of his employment duties that referred in any way to the "incident" which resulted in the Complainant leaving his previous employment. They noted that B was living outside the Northwest Territories during the relevant time frame of the Complainant's previous position. Further, they state that the files that B had access to did not contain any documentation regarding an "incident", nor did they contain any information about the Complainant's decision to leave his employment. The investigators concluded that, because it was a relatively major issue for the Complainant to have left his previous position early, it was more likely than not that this information was the subject of gossip within the community and that this is the most likely source of B's knowledge about the "incident".

As noted above, I have concerns with the determinations the investigators made from this evidence. As noted above, B did have access to both paper and electronic records containing the Complainant's employment information. This information could have been viewed by B at

any time. It is not information that would likely be removed from an employment record. The files available to B contained a grievance document that likely outlined or mentioned an incident. While it is, indeed, possible that this information was received by B by way of community gossip, it is equally possible that B found it in the Complainant's employment records and disclosed it.

Secondly, the allegation was that A was told that the Complainant was "just" a member of his former profession (implying that he was not qualified as a counselor). The investigators said that because the files show that the Complainant was a member of both professions it was unlikely that anyone who saw this file would conclude that the Complainant was "just" a member of his former profession. I do not come to the same conclusion. Particularly in light of the clear animosity between A and B it is very likely that this reference was intended more as a taunt than as an accurate portrayal of what was in the Complainant's file. If the intent was to negatively impact the relationship between A and his counselor, demeaning the Complainant in this fashion, regardless of the facts, would not be unexpected. On the other hand, this comment does support the allegation of inappropriate disclosure as it is clear that B knew the Complainant's previous profession and there is no evidence that B knew this from any source other than his access to the Complainant's employment records.

Third, the investigators noted that although information regarding the Complainant's address and salary was available to B on PeopleSoft, this information was also generally known in the community. They said that it was also hard to imagine how disclosure of this information could be used to discredit the Complainant as alleged. Again, I disagree with this assertion. I do not agree that salaries are generally "known" in the community. One would have to take steps to look up this information on the public GNWT site and even then only ranges are provided to the public and you would have to have some specific knowledge of the job title and other details about the employee, including how long they had been employed etc.. On the other hand, an

employee's salary is set out clearly in PeopleSoft. As to motive, one might make any number of conjectures about motive, including using this information as a means of confirming that B did, in fact, have details not otherwise available to the public, lending weight to the veracity of the other disclosures made by him. Conjecture, however, does not bring us closer to the facts.

Finally, the investigators said that while there is evidence that B knew the information regarding the Complainant's medical travel, they said there was no evidence, other than the allegations by A that B disclosed this information. They noted that in a small community, it was entirely possible numerous people knew that the Complainant had flown on medical travel, where that medical treatment was received and that an individual named "x" had been the medical escort. Again, I disagree with this. In order to know this information, one would have had to have been at the airport on the exact same day and seen who the Complainant was traveling with. Furthermore, the Complainant would have been traveling first to Yellowknife, so how would someone observing the Complainant and his medical escort leaving their community reveal what southern community the Complainant was traveling to or, in fact, that the travel was for medical purposes? It is, frankly, far more likely that the information was disclosed to A by B. B had direct access to the information as part of his employment duties.

Overall, I find that the conclusions reached by the investigators are based on poor investigative techniques and weak analysis. The information that A provided to the Complainant was very detailed and specific. This suggests that he got the information from someone who had access to the Complainant’s personnel files. The most logical and reasonable conclusion is that B was the person who disclosed it.

I conclude that it is more likely than not that B disclosed information to A in the course of their interpersonal dispute. While the evidence of this is likely not strong enough to prosecute B under section 59 of the Act (at least not without an audit being done to determine actual access

to the Complainant's electronic records), that does not equate to a necessary conclusion that it did not happen. I find that the Complainant's personal information was inappropriately disclosed, and that B was, more likely than not, the source of that disclosure.

3. Did the Department of Finance fail to address the complaint in a timely manner?

The Complainant said that he brought this issue to the attention of a Human Resources Manager in October 2018. He said he was told to hold off filing a complaint with the IPC or making an application with the WSCC related to the significant mental stress this situation caused. The Complainant said he had not received any information regarding the status of his complaint when he filed his complaint with our office in early December, 2018.

The investigators met with the Complainant's boss's supervisor who said she became aware of the allegations on October 23, 2018. She contacted Labour Relations the next day. On October 25, 2018, she spoke to an Adjudication Advisor, who confirmed her suggested approach to conduct an internal fact-finding investigation. On November 7, 2018, she met with the Complainant's boss and they prepared a list of questions to ask the Complainant. After this meeting, she contacted the department's ATIPP contacts to discuss concerns about releasing confidential information during the investigation. She forwarded the Complainant's memo and the redacted e-mail to the ATIPP contact. On November 30, 2018, the supervisor followed up with the ATIPP contact. She did not receive a response until December 12, 2018, after the Complainant had already filed a request for review to the Office of the Information and Privacy Commissioner.

With respect to the ATIPP contact's actions, the contact said that after speaking with the supervisor, she checked the ATIPP Manual because she had never dealt with this kind of situation before. She could not find anything to help in addressing this situation so she set the

matter aside and did not do anything further until she received the IPC complaint. On December 13, 2018, she consulted with the GNWT Access and Privacy Manager, and asked for guidance on how to proceed. She did not take any further action after this point because a decision had been made to refer the matter to external investigators.

Based on the above, the investigators concluded that the Department of Finance did not address the alleged breach in a timely manner. I agree with the investigators' conclusions on this issue. It appears that the Department was taking some steps but they never communicated this to the Complainant. Furthermore, the steps taken were not sufficient to address this issue in a timely manner, especially when the ATIPP contact just set the matter aside and did not take any concrete steps to address the complaint. Once an allegation of a privacy breach has been made, the public body should take immediate steps to commence a privacy breach investigation. The Complainant should be made aware that an investigation is commencing so that they are not left in the dark thinking that nothing is being done by the public body.

CONCLUSION AND RECOMMENDATIONS

Frankly, I am dismayed with the conclusions reached by the Investigators tasked with looking into the allegations that the Complainant's personal information had been breached. The information known by A was very specific. It is very unlikely that A would have known most of this information without someone working at the GNWT and having access to the Complainant's personnel files providing him with those details. I find, in fact, that it is more likely than not that someone accessed the Complainant's GNWT files and disclosed this information to A. I also find that it is reasonable to conclude that B was the likely person who did this, though this is not "provable" on a balance of probabilities.

The investigators in this case were clearly approaching this investigation from a labour relations point of view and not a privacy point of view. Because they could not "prove" fault or culpability beyond a reasonable doubt, they concluded it did not happen. The discussions and the conclusions reached, in my opinion, demonstrate significant bias and an overt and fairly clumsy attempt to avoid a finding of a breach.

I find that there is plenty of evidence from which to conclude that there was a breach of the Complainant's privacy and that the source of the breach was the Complainant's personnel records, though perhaps somewhat less proof from which to conclude definitively who perpetrated the breach. The fact that a breach occurred still has to be addressed, even if the source of the breach cannot be definitively determined. In this case, the nature of the relationship between A and the Complainant was such that these allegations should have also flagged additional security concerns for the safety of the Complainant which do not appear to have been addressed.

I **recommend**

a) that if not already the case, access to all electronic personnel records be controlled by means of carefully crafted and stringently applied roles-based access, capable of audit;

b) that audits be conducted regularly and randomly to identify and address inappropriate access to such records on a pro-active basis;

c) that all staff dealing with personnel records for any purpose receive basic and ongoing privacy training, including clear messaging about consequences for unauthorized use or disclosure of employee information;

d) that all paper-based personnel records be digitized and placed in the employee's electronic employment record, with necessary and appropriate conditions and safeguards in place to protect that information from inappropriate use and/or disclosure;

e) so long as there continue to be paper-based personnel records, that these be placed in a locked cabinet, in a locked room with clearly defined controls on access to the files (when access is required to a specific physical file, it should be requested and retrieved as part of a prescribed process which is managed by one person and access to files should be documented and logged, with an indication of the authorization for such access and the purpose of the access)

f) that anyone appointed to investigate an allegation of a breach of privacy under review by the Office of the Information and Privacy Commissioner, be required to:

i) have a working knowledge of the relevant privacy legislation and be able to address the issues from the point of view of a breach of privacy, as opposed to the point of view of a labour relations matter;

ii) be independent of the department and free of bias and/or conflicts of interest that might colour the investigation or the outcome of the investigation;

iii) understand that a privacy breach investigation is about identifying the root causes of a breach and gaps in the system that might lead to a breach and about determining how to prevent similar breaches in the future, rather than only being about assigning blame as appears to have been the focus in this investigation;

iv) understand that while allegations of “snooping” are serious and require a careful and in-depth investigative approach, the inability to definitively confirm snooping does not mean that no breach occurred.

I find that the public body did not address this complaint in a timely manner. In this regard, I **recommend** that the Department of Finance establish a written protocol to deal with allegations of privacy breaches generally and intentional breaches by staff in particular and that ATIPP staff receive educational support to allow them to address such complaints in a methodical and timely way.

Elaine Keenan Bengts
Information and Privacy Commissioner