ᓄᓇᕗᒻᒥ ᑐᓴᐅᒪᔪᓕᕆᓂᖅᒧᑦ ᑲᙳᓇᖅᑐᓕᕆᓂᖅᒧᑦ ᑲᒥᓯᓇ
Nunavut Information and Privacy Commissioner
Nunavunmi Tuhaqtauyukhaliqinirmun Kanngunaqtuliqinirmun Kamisina
Commissaire à l'information et à la protection de la vie privée du Nunavut

Commissioner's Final Report

Report Number:	21-189
CanLII Citation:	Department of Community and Government Services (Re), 2021 NUIPC 8
NUIPC File Number(s):	20-163-5, 20-171-5
Date:	February 10, 2021

Summary

[1] An employee of a public body "leaked" to a third party the name of a person who had filed an access request, along with the subject-matter of the request. The public body did not discover the leak until about a year later. The public body took certain steps to respond to the leak. The Commissioner finds there was a privacy breach. The Commissioner also finds that the public body's response was mostly adequate, but recommends certain additional steps to help prevent similar breaches.

Nature of Review and Jurisdiction

[2] This is a privacy breach review under s 49.2(1) of the *Access to Information and Protection of Privacy Act* (ATIPPA).

[3] The Commissioner has jurisdiction over the Department of Community and Government Services: ATIPPA, s 2, definition of "public body".

Issues

[4] The issues in this review are:

a. Should the identity of the leaker be protected?
b. Was there a breach of privacy?
c. Did the public body take adequate steps to respond to the breach of privacy?

Facts

[5] The Complainant filed an ATIPP request with the Department of Community and Government Services (CGS).

[6] The fact that a request had been filed, and the subject-matter of the request, was "leaked" by someone within CGS to a third party who had an interest both in the subject-matter of the request and the name of the requester.

[7] About a year later, the fact that a leak had occurred was detected by CGS management. CGS notified the Complainant and the Information and Privacy Commissioner of the privacy breach. The Commissioner opened an investigation file (NUIPC File 20-163-5).

[8] In its letter to the Complainant, the department wrote that it had taken steps "to ensure that your personal information is no longer available to the individual who originally breached your privacy and will keep your personal information private going forward".

[9] The Complainant, once notified of the privacy breach by the department, filed a complaint with Information and Privacy Commissioner. The Commissioner opened a new investigation file (NUIPC File 20-171-5) and, in keeping with the Commissioner's usual practice, merged the notification file into the new file.

[10] The Commissioner then wrote to CGS with a series of questions about the privacy breach. The deputy minister of CGS responded to the Commissioner's questions, but asked that the response not be shared with

the Complainant because the response would identify the employee responsible for the leak.

Legislation

[11] "Personal information" means any information about an identifiable individual, including their name: ATIPPA, s 2.

[12] Personal information may be disclosed by a public body only in accordance with Part 1 (the access provisions) or sections 48, 48.1 or 49: ATIPPA, s 47.

[13] Section 6.1 was added to the ATIPPA in 2017. The purpose of s 6.1 is to protect the anonymity of ATIPP applicants. Section 6.1(1) says the head of the public body "shall ensure that the name of an applicant is disclosed only to a person authorized to receive the request on behalf of the public body." There are only a few exceptions. The exceptions are based on the principles of necessity and need-to-know.

[14] The unauthorized disclosure of information is a summary conviction offence, punishable by a fine up to $5,000: ATIPPA, s 59(1).

Analysis

Should the identity of the leaker be protected?

[15] A preliminary issue concerns the identity of the leaker.

[16] The deputy minister requested that the department's response to this office's questions not be shared with the Complainant. The department is aware of who leaked the information to the third party, as am I. The department believes that its original breach notification report to the Commissioner, and its written response to the Commissioner's questions, would reveal the leaker's identity. The department believes that doing so would itself be a breach of privacy.

[17] I agree that revealing a leaker's identity will, in most cases, serve no useful purpose. But I do not lay this down as a general rule: there may be cases

in which the name, position or methodology of the leaker is essential to an understanding of what happened, and revealing those details will reveal the leaker's identity.

[18] With some hesitation, I believe it is possible in this case to say what needs to be said without revealing the leaker's identity. I am hesitant for two reasons.

[19] First, it means the Complainant will not see, and will not have a chance to respond to, the department's submissions to me. No one is entitled as of right to have access to, or to comment on, representations made to this office by any other person: ATIPPA, s 32(3). Nevertheless, it is a good practice, and one which this office generally follows.

[20] The second reason for my hesitation is that this report will have to be more oblique than I would like. One purpose of a Commissioner's report is to educate government staff and the general public. Another purpose is to be transparent in ATIPPA administration. Those purposes are not well served if important facts are omitted.

[21] I will say only this: the leaker was, at the time the Complainant's ATIPP request was filed, a departmental employee whose duties included being able to see ATIPP requests. Without knowing that fact, the rest of this report would make little sense.

Protecting a requester's identity

[22] When someone files an ATIPP request for information, the request itself becomes information held by the public body, and is therefore subject to the access and privacy provisions of the Act.

[23] An ATIPP request includes, at a minimum, the requester's name and contact information, all of which is "personal information" as defined in the Act. There may also be other pieces of "personal information" on the request form.

[24] Even the subject-matter of the request may be "personal information", if it is worded in such as way as to identify, directly or indirectly, personal information about the applicant. That is what happened in a recent Manitoba case (Ombudsman Report 2019-0345), where the requester's name was not disclosed, but other information was disclosed that permitted an accurate inference about who the requester was.

[25] Across Canada, privacy commissioners have held consistently that a requester's identity is protected information:

a. Ontario (Privacy Complaint Report M117-3, 2018): the lawyer for a municipality revealed in correspondence the name of an access requester. An investigator for the Information and Privacy Commissioner found that the municipality failed to take reasonable measures to prevent or respond to the privacy breach.

b. New Brunswick (Report of the Commissioner's Findings, Complaint 2014-1738-AP-947, 2015): ATIPP staff within a public body shared a requester's identity with the public body's communications staff. The department acknowledged this should not have happened and took steps to ensure it could not happen again.

c. Quebec (CAI reference 1006661, 2015), a researcher for a political party filed an access request. The researcher's name, and the name of their party, was revealed to a third party. An administrative judge with the Commission d'accès à l'information found that there had been no breach of privacy, because the name of a political party (or any corporate body) is not "personal information", nor in the circumstances was the name of the researcher who filed the request on behalf of the political party. It is nevertheless clear that the decision would have been different if the requester had been an individual.

[26] These cases, from a variety of jurisdictions and legislative schemes, show that a public body's duty to protect a requester's identity flows from the public body's duty to protect "personal information".

[27] This existing legal requirement to protect an ATIPP requester's identity was reinforced in Nunavut in 2017, when s 6.1 was added to the ATIPPA. For educational purposes, I repeat it here in full:

> *6.1. (1) The head of a public body shall ensure that the name of an applicant is disclosed only to a person authorized to receive the request on behalf of the public body and, where necessary, the Information and Privacy Commissioner.*
>
> *(2) Subsection (1) does not apply to a request*
>
> > *(a) respecting personal information about the applicant; or*
> >
> > *(b) where the name of the applicant is necessary to respond to the request and the applicant has consented to its disclosure.*
>
> *(3) The disclosure of an applicant's name in a request referred to in subsection (2) shall be limited to the extent necessary to respond to the request.*
>
> *(4) The limitation on disclosure of an applicant's name under subsection (1) applies until the final response to the request is sent to the applicant.*
>
> *(5) The disclosure of an applicant's name after the final response to the request is sent to the applicant shall be limited to circumstances where such disclosure is necessary*
>
> > *(a) to avoid harm to a public body; or*
> >
> > *(b) to allow a public body to enforce a legal right that it may have against any person.*

[28] If I were to summarize these rules in plain language, I would say: a requester's identity must be known by as few people as possible within a public body, and usually no further than the designated ATIPP Coordinator; and even when further disclosure is required, it must still be limited to a need-to-know basis.

[29] By enacting s 6.1, the Legislative Assembly has underlined the fundamental importance of anonymity in the ATIPP process. And I repeat that s 6.1 added to the existing legal requirement to protect an ATIPP requester's identity.

[30] The current Nunavut ATIPP policy manual does have a brief section on anonymity (Volume 1, section 3.3), but it is essentially a restatement of section 6.1 in plain language. That is useful, but it is not enough.

[31] A number of Canadian jurisdictions have issued detailed guidance documents to public bodies about how and why to protect a requester's identity. I will return to these documents later in this report.

Was there a breach of privacy in this case?

[32] A public body may not disclose personal information except in accordance with Division C of Part 2 of the ATIPPA. Needless to say, leaking personal information to a third party is not one of the authorized circumstances.

[33] One can perhaps excuse an accidental or inadvertent leak. For example, sometimes a document will be e-mailed to the wrong person. Or a redaction is forgotten or improperly carried out. Or something is said on the spur of the moment that, on reflection, should not have been said.

[34] In the Manitoba case cited above (Ombudsman Report 2019-0345), the public body revealed enough information that an accurate inference could be made about the requester's identity. The public body did not mean to do so. It acknowledged its inadvertent error and apologized to the applicant.

[35] Of course the consequences of an accidental leak can be just as serious as an intentional leak. But as long as the recommended four-step response to a privacy breach (contain, notify, investigate, prevent) is carried out promptly, completely, and in good faith, an accident may be forgiven.

[36] In this case, the breach was no accident. The leaker intended to leak the information, and did leak it. It would be difficult for me to overstate the seriousness of the leaker's actions. It strikes at the heart of the ATIPPA process.

[37] I think Nunavummiut would be surprised at how much the ATIPPA process depends on all of the participants acting in good faith. Keeping and managing proper records, assisting applicants, performing diligent searches, cooperating with ATIPP coordinators, obeying statutory timelines, claiming only necessary and limited exemptions, producing all responsive documents, and assisting the Commissioner to perform the oversight role: all depend on a commitment by GN staff to the public-policy objectives of the ATIPPA. In the absence of good faith, the access system quickly crumbles.

Did the department respond appropriately to the breach?

[38] An adequate response to a privacy breach has four steps: contain, notify, investigate, prevent.

[39] The department did not learn of the leak for about one year. I know how the department detected the leak, but I omit it from this report because it would tend to identify the leaker.

[40] Some people might say that leaks are to be expected in a jurisdiction with a small population like Nunavut. People know people; they are going to run into people involved in their files, whether it's at the grocery store, at the school, or on the street; there are more relationships and interconnections than in a larger population.

[41] That may be true, but it is not a reason to accept a certain amount of leakage in the ATIPP process. In fact I draw the opposite conclusion: the fact that Nunavut and its communities have small populations means that public bodies in the Government of Nunavut have to take special care and extra precautions to keep personal information from being leaked.

What did the department do to contain the leak?

[42] The root of the problem is that it does not seem to have occurred to departmental management that an ATIPP request could be leaked in the way that it was. There were no apparent safeguards. I will return to this point in the Recommendations section.

[43] Once the probability of a leak became known to departmental management, swift action was taken to contain the leak. In particular, administrative responsibilities were immediately re-arranged so that the leaker would have no further access to the Complainant's file.

What did the department do to provide notification about the leak?

[44] About one week after learning of the leak, the department notified the Complainant under s 49.10 of the ATIPPA, and this office under s 49.9 of the ATIPPA.

[45] The notification requirement under s 49.10 is premised on the department's concluding that "it is reasonable in the circumstances to believe that a breach of privacy creates a real risk of significant harm to the individual". The department concluded correctly that this threshold had been met.

[46] Similarly, the notification requirement under s 49.9 is premised on the department's concluding that the breach is "material". Materiality is to be judged according to the factors in s 49.9(2), including "the sensitivity of the personal information" and "the likelihood of harm to the individuals whose personal information is involved". The department concluded correctly that this threshold had been met.

[47] I am satisfied the department's notification to this office met the requirements in subsections 49.9(3), 49.9(4), 49.10(3) and 49.10(4) of the ATIPPA. Departmental management treated the breach as the serious matter that it was, and issued the statutory notifications accordingly.

What did the department do to investigate the leak?

[48] I have less information about the department's investigation. That may be because the investigation was, in the circumstances, brief.

[49] Once alerted to the probability of a leak, departmental management appear to have confronted the employee concerned, who appears to have admitted the leak.

[50] I have already noted, and will repeat here, that the leaker had access to ATIPP requests as part of their normal duties. There was no reason for departmental management to believe that the leaker had taken any special steps to obtain the information, or that anyone else was involved. With the leaker's admission in hand, departmental management appear to have concluded their investigation.

What did the department do to prevent future leaks?

[51] When privacy is breached, the breach cannot be undone. The breach can be contained, and the consequences can be mitigated, but the breach itself has already happened. That is why prevention is so important. What lessons has the department (or the GN) learned, and what concrete steps has it taken to prevent the future leaking of an ATIPP requester's identity?

[52] I am generally satisfied with the department's response on the first three steps (contain, notify, investigate). I am not persuaded that the department has taken adequate steps on the fourth step, which is prevention. In any event, this kind of leak could happen in any public body, and so the preventative response needs to be across the GN, not just within CGS.

[53] I will address three specific aspects of a preventative response: deterrence, policy and training.

Deterrence as a preventative measure

[54] When there is an intentional leak, I think it is important there be some attempt at specific and general deterrence: that is to say, a clear message (a) specifically to the leaker, and (b) generally to other GN staff with access to ATIPP requests, that leaking personal information is entirely unacceptable and will have consequences.

[55] With respect to specific deterrence, it is not within my authority to impose workplace discipline. I do not consider it within my authority even to recommend workplace discipline, though I am aware that some of my colleagues across Canada disagree. In my view, workplace discipline is the sole prerogative of departmental management.

[56] Having said that, this office should at least be informed of workplace discipline that has been imposed for a privacy breach. Workplace discipline is "personal information" under ATIPPA, and so is not normally disclosed; but a public body may disclose any personal information to the Information and Privacy Commissioner: ATIPPA, s 48(i). I am bound to keep that information confidential, but I do consider it necessary to have it in order to assess the adequacy of the deterrent effect.

[57] The department has told me that, in this case, "the department will follow its Human Resources disciplinary processes regarding this issue and has brought the matter to the attention of both the departmental Human Resource division and the GN Human Resources department". What the department has not told me is whether discipline was actually imposed, and if so, what that discipline was. I am therefore unable to assess whether the discipline (if any) is likely to have had any specific deterrent effect.

[58] With respect to general deterrence, I believe it is important that everyone within the GN with access to ATIPP requests should know that

intentionally leaking personal information has consequences. There is no general deterrent effect if the fact of discipline, never mind the extent of discipline, is unknown to anyone outside senior management at CGS or the Human Resources department.

Policy as a preventative measure

[59] CGS informs me that their department policy division is working on a "process document" which will consider appropriate steps to prevent similar breaches from occurring again. I have not seen the result of that policy work.

[60] In any event, an intradepartmental policy response is not sufficient to deal with this sort of privacy breach. A GN-wide policy response is required.

[61] I have already noted that the current Nunavut ATIPP manual has a brief section on anonymity, but it is no more than a plain-language restatement of ATIPPA section 6.1. That is fine, as far as it goes, but more is needed.

[62] I am aware of at least the following policy documents on this topic from across Canada:

a. Saskatchewan: Best Practices for Responding to Access Requests (January 2018)

b. New Brunswick: Anonymity of Applicants (November 2019)

c. Manitoba: Protecting the Privacy of Access Requesters (May 2007)

All of these documents are available online. They provide helpful models for a more detailed GN-wide policy.

[63] This final report, like all final reports from this office, is directed at the specific public body at which the breach occurred. I am aware that revising the GN-wide ATIPP policy manual is outside the authority of CGS. That is why the recommendations at the end of this report are also directed to the Department of Executive and Intergovernmental Affairs (EIA).

Training as a preventative measure

[64] I am not persuaded that this is a case in which training would have made a difference. The leak was intentional, and I suspect the leaker knew that what they were doing was wrong.

[65] Nevertheless, my review of cases in other Canadian jurisdictions suggests that most cases in which an ATIPP requester's identity is disclosed involve an accident, or inadvertence, or lack of knowledge of the law. Training will not prevent every disclosure, but it should, if done well, prevent many of them.

Conclusion

[66] The identity of the leaker need not be disclosed, either by the department or by this office.

[67] There was a breach of the Complainant's privacy when the Complainant's name, and the subject-matter of their ATIPP request, was intentionally leaked to a third party by a CGS employee.

[68] The department's response to the privacy breach was mostly adequate. Stronger steps could be taken to prevent future breaches. Some of those steps need to be GN-wide.

Recommendations

[69] The Commissioner may review the practices of a public body with respect to the collection, use and disclosure of personal information: ATIPPA, s 49.1(2). In addition, a privacy breach review may include recommendations with respect to the collection, use or disclosure of the individual's personal information: ATIPPA, s 49.5(a). These recommendations may go beyond the facts of the specific case under review.

[70] The findings of this report go beyond CGS. **I recommend** that the department share this report with the Department of Executive and

Intergovernmental Affairs (EIA), which has overall responsibility for the administration of the ATIPPA. The report should be shared at least with the associate deputy minister of EIA responsible for ATIPPA administration, and the Territorial ATIPP Manager.

[71] The existing policy on protecting requesters' identities is insufficient. **I recommend** that EIA review and revise the section of the ATIPP policy manual dealing with the anonymity of requesters. In doing so, it should consult policies on that topic from other Canadian jurisdictions, including the ones cited in this report.

[72] Training will not prevent intentional leaks, but it will help to prevent accidental or inadvertent disclosures. **I recommend** that training for ATIPP coordinators include a section on protecting the anonymity of requesters.

[73] CGS did not appear to anticipate a leak happening the way that it did, and I assume other public bodies are similarly unprepared. **I recommend** that EIA develop, as part of the ATIPP policy manual, a conflict of interest policy. There should be an established procedure for identifying, disclosing, and handling ATIPP requests for which departmental staff may be in a conflict of interest.

[74] **I recommend** that CGS disclose to this office details of the discipline, if any, imposed on the employee who leaked the Complainant's personal information. That information may be disclosed under s 48(i) of the ATIPPA and will be kept confidential by this office.

Graham Steele
ᑲᒥᓯᓗ / Commissioner / Kamisina / Commissaire