ᓄᓇᕗᒻᒥ ᑐᓴᐅᒪᔪᓕᕆᓂᕐᒧᑦ ᑲᙳᓇᖅᑐᓕᕆᓂᕐᒧᓪᓗ 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:	22-211-RR
CanLII Citation:	Department of Community and Government Services (Re), 2022 NUIPC 2
NUIPC File Number(s):	21-151
Date:	January 28, 2022

Summary

[1] A network drive used by the GN permitted users to share files between departments within the same community. There was no active control over what was posted. The Commissioner was tipped to a large amount of privacy-invasive material on the drive. In response, the GN immediately removed the most obviously privacy-invasive material, and later decommissioned the drive entirely. The Commissioner requested that each public body prepare a privacy breach report for files originating with their employees. Only two did so. The Commissioner recommends that each public body with material on the V: drive complete a privacy breach assessment and, where appropriate, submit a privacy breach report to the Commissioner.

Nature of Review and Jurisdiction

[2] This is a privacy breach review. My review was self-initiated under s 49.1(2) of the *Access to Information and Protection of Privacy Act* (the ATIPPA) and conducted under s 49.2(1).

[3] The Commissioner has jurisdiction over the Department of Community and Government Services, as well as all other public bodies with files on the V: drive: ATIPPA, s 2, definition of "public body".

Issues

[4] The issues in this review are:

a. Was there unauthorized disclosure of personal information on the V: network drive used by the Government of Nunavut?
b. Did the GN take appropriate steps to identify and eliminate the privacy breach?
c. Did the GN take appropriate steps to mitigate the damage caused by the breach?

Facts

[5] On July 20, 2021, an employee of the Government of Nunavut (GN) contacted my office to express concern about documents they were able to see on the so-called "V: drive" of their networked computer. The files were unrelated to the employee or their department. From the file names alone, it appeared likely the documents contained sensitive personal information.

[6] Most GN employees had three drives on their office system. The U: drive contained their own documents. The Y: drive contained departmental documents. The V: drive was intended to be used to share documents between users who did not have access to the same Y: drive. The V: drive was also referred to as "Clipboard".

[7] When used correctly, a GN employee wishing to post documents to the V: drive would request creation of a secure folder, with roles-based access. The shared documents would then be placed in the secure folder. The documents could be viewed only by GN employees with the correct permission.

[8] But the V: drive was often used incorrectly. Documents could be posted outside secure folders.

[9] There was a separate V: drive for each of Nunavut's twenty-five communities, plus another for GN employees based in Ottawa, for a total of twenty-six. If a document was posted outside a secure folder, it could be viewed by any other GN employee on the same V: drive.

[10] After learning of the possible V: drive privacy breach, I contacted the Territorial ATIPP Manager. I also contacted the acting deputy minister of the Department of Community and Governments Services (CGS), which is the department that runs the GN's computer systems. A meeting of myself, the Territorial ATIPP Manager, and CGS's most senior IT officials was arranged for the following morning.

[11] As a result of that meeting, CGS produced file lists for all twenty-six V: drives. Those lists were ready by mid-morning on July 22, 2021. Eight communities had no documents on their V: drives, so there were eighteen lists. By mid-afternoon, I had reviewed seventeen of them. The Territorial ATIPP Manager reviewed the list for Iqaluit. We flagged all files that, from the file name alone, appeared to create the risk of a privacy breach.

[12] All the flagged files were isolated by CGS before the end of the next day. That meant casual users could no longer access them.

[13] This was not the first time that the V: drive had been looked at from a privacy perspective. In early 2021, the Territorial ATIPP Manager had asked ATIPP Coordinators to review the V: drive for files belonging to their public body, and to document any files that represented a privacy breach. The manager does not have records of who completed the review. Only one privacy breach arising from this review, from Nunavut Arctic College, was reported to my office. In any event, the Territorial ATIPP Manager did not realize at the time that there were twenty-six different V: drives. He was looking only at the V: drive for Iqaluit.

Law

[14] Section 42 of the ATIPPA lays down the general obligation of a public body with respect to protection of personal information:

> 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.

[15] Section 49.9 requires a public body "that knows or has reason to believe" a privacy breach has occurred to report the privacy breach to this office, as soon as reasonably possible. The threshold for reporting is that the breach must be "material". The factors relevant to materiality are spelled out in section 49.9(2).

Analysis

Was there unauthorized disclosure of personal information on the V: drive?

[16] The employee who first brought the V: drive files to my attention was being a good citizen. They were not filing a privacy breach complaint under s 49.1(1) of the ATIPPA. The personal information was not theirs. They merely wanted to bring to my attention that there appeared to be a problem. "I should not be able to see this," they said to me.

[17] I obtained screenshots of what the employee could see. Based on the file names alone, I could see it was likely the material was privacy-invasive. At that point, I initiated a review under s 49.1(2). It was obvious to me that a review was "warranted in the circumstances", which is the test in s 49.2(1).

[18] After the entire V: drive had been vetted (details are in the next section), there were at least dozens, and maybe hundreds, of files with privacy-invasive content on the V: drive. I saw files with personal information touching on health, education, corrections, child protection, human resources, and more. Some of it was highly sensitive, like diagnoses, prescriptions, and medical photographs. Some of it, if publicly released,

could have endangered the health and safety of GN employees and others. None of it should have been left unprotected on the V: drive.

[19] The V: drive served a useful purpose: it allowed cross-departmental collaboration within a community. If used correctly, file access could be restricted only those who had an operational need to see it.

[20] But there were no controls, either human or technical, to ensure the V: drive was in fact being used correctly. As a result, files could be placed on the V: drive without controlled access. Some files were probably put there by accident, or because the employee did not realize the privacy risks. Once a file was up, there were no controls over when or if it would be taken down. Privacy-invasive files accumulated over a period of years.

[21] The V: drive for a particular community was visible only to GN employees in that community. For that reason, there was never general public access to the files on the V: drive. That is some comfort.

[22] GN employees who did have access to the V: drive are bound by a code of ethics. That may have guided their actions not to look at or misuse information they should not have been able to see on the V: drive. At the very least, it would have given management some means of responding to unauthorized access, if management became aware of it.

[23] On the other hand, far too many GN employees had access to personal information for which they had no operational need. For anyone whose personal information was posted unprotected to the V: drive, it would be cold comfort to know only GN employees could see it. The duration of the vulnerability, and the turnover in the GN workforce, means that many people currently outside the GN workforce may have seen information they should not have seen. Moreover, the small size of Nunavut's communities means that special care must be taken to protect personal information, even when it is only GN employees who are involved.

Did the GN take appropriate steps to contain or eliminate the privacy breaches?

[24] The day after I first learned of the V: drive vulnerability, I met with the IM/IT management team in the Department of Community and Government Services, together with the Territorial ATIPP Manager. They immediately grasped the potential seriousness of the privacy breach. Over the following week, they worked diligently with me to identify the most obviously problematic files and to prevent further access to them.

[25] I commend the IM/IT management team and the Territorial ATIPP Manager for the work they did during this initial flurry of activity.

[26] On September 9, 2021, I wrote to the deputy minister of CGS, to say that my investigation was ongoing, and would likely take several months at least. In the interim, I recommended that planning begin to replace or reconfigure the V: drive.

[27] On October 29, 2021, CGS issued a technical bulletin to GN employees, informing them the V: drive would be decommissioned effective November 1, 2021. CGS said that it was moving to a "more secure enterprise solution" with multiple advantages over the V: drive, including a reduction of the risk of privacy breaches.

[28] Again, I commend CGS for taking this initiative. The new enterprise solution may have privacy vulnerabilities of its own, though they are unlikely to be on the scale of the V: drive. But at least the V: drive, a privacy nightmare, was eliminated.

Did the GN take appropriate steps to mitigate the breaches of privacy?

[29] The GN, and specifically the IM/IT division of CGS, responded appropriately to the privacy vulnerability of the V: drive once it was brought to their attention.

[30] The issue of mitigation is entirely different. That is not the responsibility CGS. It is the responsibility of every public body with unprotected files on the V: drive.

[31] Once the suspect files were isolated, I turned further investigation over to the Territorial ATIPP Manager. He developed a tracking system for each suspect file, which included instructions for ATIPP Coordinators on how to go through the files.

[32] The public bodies were supposed to do a privacy breach assessment and, where appropriate, file a privacy breach report with this office. That is what the law requires.

[33] I then waited for the privacy breach reports to roll in.

[34] And waited.

[35] And waited.

[36] In the end, I received only two privacy breach reports about the V: drive, one from the Department of Justice and one from the Department of Economic Development and Transportation.

[37] The Justice report concerned a file containing information about one of the department's operational divisions that, if it got into the wrong hands, could have had significant negative consequences, and might even have put people at risk of harm. Justice concluded (correctly, in my view) that the breach was material, and so went on to investigate who within the GN had viewed the file while it was exposed on the V: drive.

[38] The investigation included a file audit. The audit revealed that a surprisingly large number of GN employees had viewed the information, even though there was no operational need for them to do so. The department would not have known that if it had not investigated. That is exactly why other departments need to do the same.

[39] The privacy breach report submitted by the Department of Justice was well done and stands as a model for other departments to follow. I was satisfied with the steps taken by Justice in mitigation, and concluded that no further action was required by me under sections 49.12 or 49.14 of the ATIPPA.

[40] The EDT report concerned information about a departmental program. The exposed information was relatively old and, in any event, not especially sensitive. It likely would have been released if anyone had asked for it. EDT concluded that any privacy breach was not material. I agree.

Conclusion

[41] There were multiple unauthorized disclosures of personal information on the V: drive used by the Government of Nunavut. The unauthorized disclosures resulted in multiple privacy breaches across multiple departments. Some of these privacy breaches have the potential to be very serious.

[42] The GN, and specifically the IM/IT division of CGS and the Territorial ATIPP Manager, took appropriate steps to identify and eliminate the privacy threat posed by the V: drive. CGS quickly isolated the suspect files, preventing any further access. Later, the CGS decommissioned the V: drive entirely.

[43] With respect to assessment and mitigation, the Territorial ATIPP Manager worked diligently to create a tracking system. The tracking system is a practical tool to complete the remaining work correctly and efficiently. But other than the two reports mentioned in paragraphs 36 to 40, the public bodies with suspect files on the V: drive did not take appropriate steps to assess and mitigate the damage.

Recommendations

[44] **I recommend** that each public body with exposed files on the V: drive complete a privacy breach assessment for each suspect file and, where appropriate, submit a privacy breach report to my office in accordance with section 49.9 of the ATIPPA.

[45] **I recommend** that each public body use the tracking system developed by the Territorial ATIPP Manager as an essential component of its response to the first recommendation.

[46] I will send this Review Report to the Minister of Community and Government Services, since CGS was responsible for the V: drive. However CGS is not responsible for ensuring that public bodies comply with their statutory obligations under the ATIPPA. I will therefore also send this Review Report to the Minister for Executive and Intergovernmental Affairs, since EIA is responsible for overall administration of the ATIPPA.

Graham Steele
ᑲᒥᓯᓇ / Commissioner / Kamisina / Commissaire