Office of the Information and Privacy Commissioner for Nova Scotia
Report of the Commissioner (Review Officer)
David Nurse

REVIEW REPORT 25-12

November 28, 2025

Halifax Regional Police

Summary:

The applicant submitted 13 access requests for copies of emails and text messages sent between identified employees of the public body during specific periods of time. The public body said it found no responsive records in its custody or control. The applicant asked the Office of the Information and Privacy Commissioner for Nova Scotia (OIPC) to conduct a review of the public body's search efforts. The OIPC requested that the public body conduct another search.

As required under the duty to assist provision set out in section 467(1)(a) of *Part XX* of the *Municipal Government Act* (*MGA*), the Commissioner finds that the public body did conduct an adequate search for email records in 10 of the 13 files and did not conduct an adequate search for email records in 3 of the 13 files. Further, the Commissioner finds that the public body did not conduct an adequate search for text message records in all 13 files.

The Commissioner recommends that, within 45 days of this report, the public body: (1) issue and copy the OIPC on a decision to the applicant for the email record it located in OIPC file 21-00211, or if already done, provide the OIPC with a copy of the disclosure decision, (2) conduct a new search of the email account of the current employee named in 3 of the access requests, and (3) conduct a search for text message records of the 2 current employees named in these access requests. Within 6 months of this report, the Commissioner also recommends that the public body review and revise its record management policies and procedures to adequately address text messages and other instant messages.

INTRODUCTION:

[1] The applicant filed 13 access requests (files) for copies of records in the custody and control of the public body. The applicant asked for copies of emails and text messages sent between identified employees of the public body during specific periods of time. In response, the public body said it found no responsive records in its custody or control.

[2] Section 467(1)(a) of *Part XX* of the *Municipal Government Act* (*MGA*) provides that a public body has a duty to assist an applicant; this duty includes the obligation to make "every reasonable effort" to locate requested records.

ISSUE:

[3] Did the public body meet its duty to assist the applicant by conducting an adequate search as required by s. 467(1)(a) of the *MGA*?

DISCUSSION:

[4] The legal test for deciding if a public body has conducted an adequate search has been addressed before; in this excerpt from NS Review Report 21-05, former Commissioner Tricia Ralph discussed the legal duty existing under the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*), however, the duty to assist under the *MGA* is the same:

> …
>
> The requirement to conduct an adequate search arises out of the duty to assist provision in s. 7(1)(a) of *FOIPOP*. Section 7(1)(a) of *FOIPOP* states:
>
> > 7 (1) Where a request is made pursuant to this Act for access to a record, the head of the public body to which the request is made shall
> >
> > (a) make every reasonable effort to assist the applicant and to respond without delay to the applicant openly, accurately and completely;
>
> [6] A provision outlining the duty to assist applicants is found in access to information legislation across Canada. Most jurisdictions have review reports canvassing the effort that public bodies must exert to meet this duty when searching for records. The leading case in Nova Scotia is NS Review Report FI-11-76. In that case, former Information and Privacy Commissioner Tully reviewed decisions from across Canada and concluded that where an applicant alleges a failure to conduct an adequate search, the applicant must provide something more than a mere assertion that a document should exist. In discharging this burden, the applicant must provide a reasonable basis for concluding that such records exist and sufficient particulars to identify the record(s). In providing sufficient particulars, the applicant should specify the subject matter of the record sought as precisely as possible and provide sufficient detail such as information relating to the time, place and event whenever possible.
>
> …
>
> [7] When an applicant discharges their burden, the burden then shifts to the public body to make "every reasonable effort" to locate the requested record(s). **The public body's response should include a description of the business areas and record types searched (e.g., emails, physical files, databases), and identify the individuals who conducted the search (by position type). Also, the public body's response should**

> **include the time taken to conduct the search. If there is an explanation for why a record may not exist, it should be provided.** These principles are further outlined in this Office's document entitled *Duty to Assist #2: Conducting an Adequate Search*.
>
> [8] A public body must demonstrate how it conducted a reasonable search or provide a reasonable explanation as to why it determined that responsive records do not exist. However, a public body does not need to prove this with absolute certainty. **The standard is reasonableness, not perfection. (emphasis added.)**

Email records: public body conducted an adequate search in 10 of 13 files

[5] During the investigation, the Office of the Information and Privacy Commissioner for Nova Scotia (OIPC) Investigator requested that the public body conduct a new search, and the public body complied. The public body located one email record responsive to OIPC file 21-00211 and said it would be processed and disclosed to the applicant with a copy to the OIPC. As of the date of this report, it is unclear if this record has been disclosed to the applicant because the OIPC has not been copied on a disclosure decision as offered by the public body in their representations and as typically requested as part of the review process.

[6] As required by the above-noted test, the public body provided a description of the business areas searched and the types of records searched; specifically, the archived "Halifax.ca" emails of the identified employees who were retired at the time of our investigation. The public body provided the title of the individual who conducted the search and the time taken. After carefully considering the public body's efforts, the OIPC Investigator determined that "every reasonable effort" was made in 10 of the 13 requests, based on the standard of reasonableness – not perfection. I agree with the Investigator and conclude that the public body met its duty to assist by conducting an adequate search in 10 of the 13 files.

Email records: public body did not conduct an adequate search in 3 of 13 files

[7] The OIPC Investigator also determined that the public body did not meet its duty to assist by conducting an adequate search in 3 of the 13 files. In these three cases, the applicant had requested email communications between a now retired employee and a current employee. The public body took the unusual position that it did not need to search the active email accounts of current employees; the public body staff searched only the archived records of the retired employee.

[8] The public body's position was that a search of the retired employee's emails was adequate as any records would be contained in the sent or archived folders of both inboxes. However, I am not satisfied that the search was adequate, and that there was no potential for responsive records to be missed. The public body did not provide any evidence, such as confirmation from its IT Department, that there was no potential for a file to be deleted or removed from the archived records, and, therefore, that there was no risk of the search missing responsive records. I agree with the Investigator and conclude that the public body did not meet its duty to assist by conducting an adequate search in 3 of the 13 files.

[9] I would also note that it is reasonable and expected that the records of current employees will be searched when an access request is made; staff should expect this, and frankly it should

be a routine part of their work. Searching a current employee's email account or having the employee search their own email for responsive records, is not a complex or time-consuming task. Although the public body indicated it expects and directs current employees to search inboxes, there was no evidence provided as part of this review to substantiate this. In my understanding, it could be completed in a matter of minutes. This further contributes to my finding that the public body's choice not to search email records of current employees is unreasonable.

Text message records

The public body's submissions

[10] The public body stated that it did not have the capacity to retrieve text messages. Subsequently it submitted it did not have custody or control of these records. It appears that no search of the physical devices of employees was conducted at the time of the processing of the initial requests.

[11] With respect to records related to several retired employees, the public body explained that a secondary search for text message records was not possible:

> With respect to the searches of the named parties text messages, I wish to advise that a secondary search was not possible for the following individuals as they are no longer employed with HRP and all cell phones are wiped by HRM's Information Technology Business Unit when employees leave the organization.
>
> …

[12] The public body stated further that there is no specific guidance regarding the retention of text messages in its retention plan but that "text messages pertaining to specific files, or cases would be stored within the appropriate file and would fall under the retention schedule for the specific file type."

[13] In December 2021, the public body checked with its service provider, Bell Media Inc. (Bell), which confirmed it does not store text messages. This is also confirmed on Bell's website.[1]

[14] Despite the public body's stated practice of wiping phones of departing employees, the public body did not provide records showing when the specific phones in question were wiped, reset, re-deployed or destroyed. It did not provide a policy setting out this practice of wiping or resetting phones upon an employee's departure. The public body did not provide evidence to show that it initially searched the physical phones for any of the 10 individuals listed in these requests, including 2 individuals still employed by the public body.

[1] https://aliant.bell.ca/Security_and_privacy/Privacy_FAQ.

The public body's search for text message records was not adequate

[15] I find that the public body's search for text message records in all the 13 files was not adequate, as required under the duty to assist provision set out in section 467(1)(a) of the *MGA*. As noted above, the public body stated that it did not have the capacity to retrieve text messages. Subsequently it submitted it did not have custody or control of these records. Based on our investigation, it appears that no search of the physical devices of employees was conducted at the time of the processing of the initial requests. This was not a reasonable approach; text messages and instant messages sent on government devices are government records and are subject to the *MGA*. Any available devices should have been searched and relevant records collected at the time of the initial processing of the requests.

[16] Further, while the public body conducted a secondary search for email records, the public body does not appear to have done a secondary search for text message records – either of the phones themselves or of other records of the two current employees. In addition to any text messages on the devices themselves, there may also be printed copies or screenshots of text messages that were subsequently deleted by the system. A search should have been done in the first instance – when the applicant's requests were initially received, and it was more likely that messages would have been retained (if they existed). As noted above, there is no evidence this was done, and no secondary search for text message records was done. I acknowledge that it is highly unlikely that text messages exist today after the lengthy passage of time in this case, but – again – it appears that the public body has avoided searching the records of current employees.

[17] Further, the public body did not provide any evidence to demonstrate that the retired employees' phones were in fact wiped; it is reasonable to expect that a public body would maintain some type of inventory or tracking system for valuable digital devices, and that they could demonstrate with a degree of certainty - with reference to their internal records - that the specific devices used by employees were returned, wiped of data, and either assigned to another employee, or disposed of. Without records to rely on, I cannot conclude whether the phones – and any records they may have contained - were wiped or not.

Best practices regarding text messages and other instant messaging tools

[18] It is beyond the scope of our mandate to provide detailed advice to the public body on its records management practices, but I will offer a few suggestions for the public body's consideration.

[19] First and foremost, it is important to remember that text messages and messages shared via other instant messaging tools (such as Facebook Messenger, Microsoft Teams, etc.) are records, as that term is defined in the *MGA*. I would therefore recommend that the public body review its advice to staff on the proper use of text messaging and other instant messaging tools when conducting business on behalf of the public body. Further, as government records, text messages and other types of instant messages should also be directly addressed in the public body's records retention plan. While many of these types of records may be properly characterized as transitory, and their immediate or scheduled destruction or deletion may be appropriate, this should be addressed in the public body's records retention plan. Staff should not be left to decide on the retention or destruction of government records on an ad hoc or individual basis. Useful guidance

on these matters can be found in the OIPC guide on *Instant Messaging and Personal Email Accounts*.

FINDINGS & RECOMMENDATIONS:

[20] As required under the duty to assist provision set out in section 467(1)(a) of the *MGA*, I find that the public body did conduct an adequate search for email records in 10 of the 13 files and did not conduct an adequate search for email records in 3 of the 13 files;[2] I further find that the public body did not conduct an adequate search for text message records in all 13 files.

[21] I recommend that, within 45 days of the date of this review report, the public body issue its disclosure decision to the applicant for the email record it located in OIPC file 21-00211, with the OIPC copied. If the public body has already done so, I recommend that, within 45 days of this review report, it provide the OIPC with a copy of the disclosure decision it has already provided to the applicant.

[22] I also recommend that, within 45 days of the date of this review report, the public body conduct a new search of the email account of the current employee named in 3 of the access requests, conduct a search for text message records of the 2 current employees named in these access requests, and inform the applicant of the outcome and include the following:

> a. If no records are found, the public body's response should include a description of the business areas and record types searched (e.g., emails, physical files, databases) and identify the individuals who conducted the search (by position type). Also, the public body's response should include the time taken to conduct the search. If there is an explanation for why a record may not exist, it should be provided.
>
> b. If additional records are found, I recommend the public body issue the applicant a new decision and provide them with any records for which access is granted.

[23] I further recommend that the public body review and revise its record management policies and procedures to adequately address text messages and other instant messages within 6 months from the date of this decision.

November 28, 2025

David Nurse
Information and Privacy Commissioner for Nova Scotia

OIPC Files: **21-00202; 21-00203; 21-00205; 21-00206; 21-00207; 21-00209; 21-00211; 21-00212; 21-00213; 21-00216; 21-00217; 21-00222; 21-00223**

[2] OIPC review files: 21-00205, 21-00207 and 21-00213.