OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

A-2025-032

August 11, 2025

Department of Transportation and Infrastructure

Summary: The Complainant made an access request to the Department of Transportation and Infrastructure for a copy of the government-wide employee directory including names, titles, departments, government phone numbers, and email addresses. The Department provided the responsive records but redacted the email addresses under sections 31 (disclosure harmful to law enforcement) and 35 (disclosure harmful to the financial or economic interests of the public body). The Commissioner found that the exceptions were not properly applied and recommended release of the email addresses.

Statutes Cited: Access to Information and Protection of Privacy Act, 2015, SNL 2015, c A-1.2, sections 9, 31(1)(l) and 35(1)(b) and (g).

Authorities Relied On: NL OIPC Report A-2025-013.

Newfoundland and Labrador (Indigenous Affairs and Reconciliation) v. Newfoundland and Labrador (Information and Privacy Commissioner), 2021 NLSC 161.

Newfoundland and Labrador (Treasury Board) v. Newfoundland and Labrador (Information and Privacy Commissioner), 2024 NLSC 147.

ATIPP Office Manual: Access to Information Policy and Procedures Manual, October 2024.

BACKGROUND

[1] The Complainant made an access to information request to the Department of Transportation and Infrastructure under the **Access to Information and Protection of Privacy Act, 2015** (the "**Act**"), for the following records:

> the full employ [sic] directory for the Government of Newfoundland and Labrador. Please include each person's name, their title, the department (and which division of that department if that information is included) their government phone number, cell phone number and email address.

[2] The Department provided the responsive records with the email addresses redacted, citing sections 31 (disclosure harmful to law enforcement) and 35 (disclosure harmful to the financial or economic interests of the public body). The Complainant made a complaint to this Office.

[3] As informal resolution was unsuccessful, the complaint proceeded to formal investigation in accordance with section 44(4) of the Act.

PUBLIC BODY'S POSITION

[4] The Department cited increased cyber security risks as its reasoning for withholding the email addresses. The Department requested that all details relating to their submissions on the matter be kept confidential for the same reasons.

COMPLAINANT'S POSITION

[5] The Complainant noted that in all previous access requests they had never been refused government email addresses. Additionally, the Complainant stated that an email address does not reveal anything about the government's system, or anything related to cyber security, therefore section 31(1)(l) should not apply.

[6] The Complainant went on to note that simply possessing email addresses does not offer any special ability to access any government systems. The Complainant argued that if the

government's computer system is so vulnerable that just knowing an email address makes it easier to gain access to its systems, then this should be addressed by beefing up security rather than blocking access to information that is often publicly available.

[7] Finally, the Complainant argues that an employees' email address is public information as it is required for anyone from the public to contact an employee. The Complainant proposes that it is like arguing that a public body shouldn't be required to release addresses for government buildings because it would increase the risk of break and enters, even though there are plenty of other steps required (a key to the lock or the code to the alarm system) to access the building. Referencing Report A-2024-039 ("Information showing where doors are to be located in the building or the dimensions of the structure do not constitute a security arrangement"), the Complainant submits email addresses are the same as the windows, and knowing they exist is not in and of itself a security arrangement.

ISSUES

[8] Did the Department appropriately apply section 31 or section 35 in withholding the email addresses?

DECISION

[9] Section 31(1)(l) states that a public body may refuse to disclose information that could reasonably be expected to "reveal the arrangements for the security of property or a system". The Department argues that revealing government email addresses in aggregate form may allow threat actors to better tailor attacks on government systems.

[10] The Department pointed to the recent decision in **Newfoundland and Labrador (Treasury Board) v. Newfoundland and Labrador (Information and Privacy Commissioner)**, where the Court allowed for the withholding of computer file paths, as extrapolation from those paths could be used to generate usernames and IP addresses. The main difference here is that file paths are not available in other locations and have not been routinely released. Therefore, the release of the file paths would assist threat actors in their attempts to access government

systems by providing them with new information to work from. The release of more government email addresses, when so many are already publicly available, does not provide threat actors with any more information they already have, and as such reveals nothing that has not already been revealed. The same argument could be made regarding the names of government employees, extrapolations could be made from those as well, but that does not transform them into "security arrangements".

[11] While there may be some credence to the argument that there is risk in releasing aggregate data with email addresses, this does not transform a simple email address into "security arrangements". Therefore, section 31(1)(l) does not apply to government email addresses, in aggregate form, or otherwise.

[12] Sections 35(1)(b) and (g) state:

> 35. (1) The head of a public body may refuse to disclose to an applicant information which could reasonably be expected to disclose
>
> . . .
>
> (b) financial, commercial, scientific or technical information that belongs to a public body or to the government of the province and that has, or is reasonably likely to have, monetary value;
>
> . . .
>
> (g) information, the disclosure of which could reasonably be expected to prejudice the financial or economic interest of the government of the province or a public body

[13] Section 35(1)(b) is a categorical exception as noted in Report A-2025-013 and it requires that the information be "financial, commercial, scientific or technical". The Department asserts that email addresses may fall under the definition of "technical". The ATIPP Office in its ATIPP Manual, defines "technical information" as information relating to a particular subject, craft, or technique. It provides system design specifications and plans for an engineering project as examples of such.

[14] The Supreme Court of Newfoundland and Labrador considered the definition of "technical" in the context of the Act in **Newfoundland and Labrador (Indigenous Affairs and Reconciliation) v. Newfoundland and Labrador (Information and Privacy Commissioner)**. In that case the court was looking at section 39, which also references technical information. The Court stated:

> [75] The same dictionary suggests the following definitions of the word "technical": Of or relating to technique: a technical procedure; great technical skill in playing the violin.
>
> > 2.a. Having or demonstrating special skill or practical knowledge especially in a mechanical or scientific field: a technical adviser; technical expertise in digital photography.
> >
> > b. Used in or peculiar to a specific field or profession; specialized: technical jargon.
> >
> > c. Requiring advanced skills or specialized equipment: technical mountain climbing.
> >
> > 3. Of or relating to the practical, mechanical, or industrial arts or to the applied sciences: a technical institute.
>
> [76] Although the primary definitions of both scientific and technical refer to the physical sciences, the alternate definitions are broad enough to include the work of social science where that work employs a systematic approach and the application of special skill or knowledge.
>
> [77] The interpretation of the Act requires a broad and purposive approach [...]

[15] Even allowing for a broad and purposive approach, an email address does not fit into the definition of "technical". It is more akin to a telephone number or street address, simply a piece of information used to facilitate communication. In and of itself it does not communicate any specialized skill or knowledge.

[16] Therefore, as with section 31, an email address simply does not fit into the type of information contemplated by the section and, as such, the exception cannot apply.

[17] Section 35(1)(g) requires that the Department show a reasonable expectation of harm in the release of the information. A reasonable expectation of harm requires a clear and causal

link between the disclosure of the specific information and the alleged harm. This link must be convincing and not just theoretically possible.

[18] There is no doubt that cyber attacks can have negative effects on the financial or economic interests of the Province. The potential damage is well-known, as Newfoundland and Labrador faced significant damage during the cyber attack involving the health care system in 2021. Costs included rebuilding a system, installing safer protocols, offering credit monitoring to current and former clients or employees, legal fees, and hiring Investigators post-attack.

[19] The question is, however, whether there is a clear and causal link between the release of these particular email addresses in aggregate form, and any expectation that the release will have an appreciable impact on the likelihood of a successful cyber attack.

[20] The Department did provide information on the risks associated with cyber attacks and the reasons it believes that the release of email addresses alongside other information could potentially increase the likelihood of a successful attack. However, given the number of government email addresses that are already publicly available and the sophistication of publicly available software, the release, or in some cases, re-release, of the email addresses, is not likely to significantly increase any of the risks identified by the Department. Additionally, a review of the emails that are already publicly available makes it fairly obvious what the conventions used to create government email addresses are. Given the already publicly available information, it is just a small step to guess a government employees email with significant accuracy. It is not apparent that withholding the email addresses would significantly mitigate risks. As such section 35(1)(g) would not apply to these emails either.

RECOMMENDATIONS

[21] **Under the authority of section 47 of the Access to Information and Protection of Privacy Act, 2015**, I recommend that the Department of Transportation and Infrastructure release the email addresses previously withheld under sections 31 and 35.

[22] As set out in section 49(1)(b) of the **Access to Information and Protection of Privacy Act, 2015**, the head of the Department of Transportation and Infrastructure must give written notice of his or her decision with respect to these recommendations to the Commissioner and any person who was sent a copy of this Report within 10 business days of receiving this Report.

[23] Dated at St. John's, in the Province of Newfoundland and Labrador, this 11th day of August 2025.

Kerry Hatfield
Information and Privacy Commissioner
Newfoundland and Labrador