

Commissioner’s Final Report

Report Number:	22-218-RR
CanLII Citation:	Department of Human Resources (Re), 2022 NUIPC 9
NUIPC File Number:	22-111
Date:	May 26, 2022

Summary

[1] The Complainant was a short-listed candidate in a job competition. An employee of the Department of Human Resources sent an e-mail to the short-listed candidates. The e-mail addresses were in the CC field, meaning that the candidates could see the other candidates’ addresses. HR apologized to all candidates. The Complainant filed a privacy breach complaint. The Commissioner finds there was a privacy breach. The employee made a mistake. The Commissioner makes certain recommendations that will, if implemented, reduce the risk of similar mistakes recurring.

Nature of Review and Jurisdiction

[2] This is a review of a privacy breach complaint. The complaint was made under section 49.1(1) of the *Access to Information and Protection of Privacy Act* (ATIPPA). I conducted my review under section 49.2(1).

[3] The Commissioner has jurisdiction over the Department of Human Resources: ATIPPA, s 2, definition of “public body”.

Issues

- [4] The issues in this review are:
- a. Did HR breach the Complainant's privacy?
 - b. If so, what changes to HR's practices would reduce the risk of recurrence of a similar privacy breach?

Facts

[5] The Complainant applied for an advertised job through the Department of Human Resources. The Complainant was short-listed for the position. There were four candidates on the short list.

[6] In January 2022, an employee of the Department of Human Resources sent an e-mail to all short-listed candidates. The employee put the e-mail addresses in the "CC" field. As a result, each of the short-listed candidates could see the e-mail addresses of the other short-listed candidates. The addresses contained the candidates' names.

[7] Within half an hour, the HR employee attempted several times to recall the e-mail. The HR employee then sent another e-mail to the short-listed candidates (although this time their addresses were not visible) saying "My apologies for making an error and sending the email as cc instead of bcc. Please delete the previous email from your inbox." There was some correspondence between the HR employee and the Complainant. There was also a phone call, during which the HR employee apologized to the Complainant.

[8] The Complainant filed a complaint with this office. The Complainant asked that I review the complaint without revealing their identity to HR. The Complainant also requested that I not start my review until the job competition was finished. I agreed.

[9] On March 1, 2022, I wrote to HR, informing them of the complaint and inviting their response. I noted that the focus of my review was on the institutional response to a kind of privacy breach, as opposed to an individual response to an individual incident. I requested HR's comments on policies,

procedures, training, and any other matters relevant to the use of e-mail by HR employees.

[10] On March 23, 2022, I received a reply from the deputy minister for HR. (The letter is dated March 18, 2022.) Attached to the reply were the following policy and procedure documents:

- a. Acceptable Email and Internet Usage Policy (CGS)
- b. Records Management Policy (CGS)
- c. Code of Values and Ethics (HR)
- d. My First Competition (HR)
- e. Confidentiality Form (HR)
- f. Staffing Manual (HR)
- g. Human Resources Manual 505: The Selection Committee (HR)
- h. Communications Policy (EIA)
- i. Privacy Breach Policy (EIA)

The deputy minister's letter also mentions ATIPP training, presented by the Department of Executive and Intergovernmental Affairs, which is part of the orientation program for new GN employees.

[11] The deputy minister's letter goes on to state the following steps HR has taken, or plans to take, to reduce the risk of privacy breaches in the course of a job competition:

- My department will continue to stress to Staffing Consultants and all hiring managers the importance of keeping all our competitions confidential and when communicating to candidates, to relay the same consistent message to all our candidates individually.
- My department will review and update the Staffing Manual to include more detailed communication process with candidates and panel members, detailed process for video screening, interviews and appeals.
- My department will review and update the Human Resources Manual to include the process for communicating with candidates during the hiring process, screening and conducting the interview.
- My department will develop training to guide departmental staff on candidate information privacy and protection.

[12] On March 31, 2022, HR sent to me a letter of apology, asking that it be forwarded to the Complainant. (As noted above, HR did not know the identity of the Complainant.) The letter includes the four commitments from the deputy minister's letter, quoted above. The letter is signed by HR's ATIPP Coordinator.

Law

[13] Part 2, Division C, of the ATIPPA deals with the disclosure of personal information. Section 47 lays down the general rule:

- 47. A public body may disclose personal information only
 - (a) in accordance with Part 1; or
 - (b) in accordance with this Division.

Part 1 deals with access to information, and so is not relevant to this case.

[14] Section 48 lays down twenty-three circumstances in which disclosure of personal information is authorized. None applies to this case.

[15] "Personal information" is defined in section 2:

"personal information" means information about an identifiable individual, including

- (a) the individual's name, home or business address or home or business telephone number, ...

[16] Section 49.1(2) gives me the authority to "review the practices of the public body with respect to the collection, use and disclosure of personal information". Section 49.5(a) gives me authority to make recommendations "with respect to the collection, use or disclosure of the individual's personal information".

Analysis

Was there a privacy breach?

[17] The e-mail address of a private citizen is “personal information” within the meaning of the ATIPPA. It is “information about an identifiable individual”. That is particularly the case where the address contains an individual’s name, as is typical for an e-mail address used for professional purposes.

[18] Further support for this conclusion is found in paragraph (a) of the definition, quoted in the Law section above. The definition was written in the mid-1990s, but was based on 1980s-era legislation in other jurisdictions. It predates the widespread use of e-mail. Nevertheless, the reference to “home or business address” is, applying the purposive approach to statutory interpretation, broad enough to capture an e-mail address.

[19] That does not mean that all personal e-mail addresses are automatically protected from disclosure. Whether they are so protected depends on the application of section 23 (in an access case) or section 48 (in a privacy case). For example, if a GN employee is using a personal e-mail address to transact government business, the address is not necessarily exempt from disclosure: *Department of Health (Re)*, 2021 NUIPC 11 (CanLII) at paragraphs 47 and 48.

[20] In this case, however, none of the circumstances in section 48 apply.

[21] To put it simply, the HR employee made a mistake. They should not have put the short-listed candidates’ e-mail addresses in the CC field. They quickly realized their error. Although they tried to recall the message, that was not possible. The best the sender could then do was to contact the recipients, apologize for the error, and ask them to delete the errant e-mail.

[22] The disclosure of the Complainant’s e-mail address to the other short-listed candidates was contrary to section 47 of the ATIPPA. It was, in short, a breach of the Complainant’s privacy.

General observations on e-mail hygiene

[23] The harder part of this decision is crafting recommendations that respond effectively and proportionately to the facts of the case. I begin with some general observations on the use of e-mail and the BCC field.

[24] E-mail is everywhere within the GN. It is used almost every day, by almost everybody. Its frequent use obscures the fact that e-mail software is complicated. Few people master all the features. It is easy to make mistakes. Some of the more common mistakes having privacy implications, in addition to the CC/BCC error, are:

- a. Mistyping a recipient's address.
- b. Using auto-fill for a recipient's address and not noticing that the wrong recipient has been selected.
- c. Using an outdated address.
- d. Using an outdated or inappropriate group of recipients.
- e. Using "Reply All" when discussing personal information that should not be disclosed to all recipients of the original message.

[25] Sometimes these mistakes cause no harm – perhaps because the message bounces back to the sender, or the message goes to a mailbox that is not seen by anyone, or the recipient alerts the sender to the error without reading the message. But the potential for a privacy breach is always there.

[26] Avoiding e-mail mistakes requires training, and experience, and effort. More than anything, it requires good habits, or what might be referred to as "e-mail hygiene".

General observations on the BCC field

[27] E-mail programs typically provide three fields in which the sender can insert the address of a recipient:

- a. TO: This field is for the principal recipient(s). Typically this includes to whom the e-mail is addressed, and from whom action (if any) is expected.
- b. CC: This field is for recipients to whom the e-mail is “copied”. (CC stands for “carbon copy”, which is a throwback to a different era of office technology.) Typically this includes those who the sender wants to see the e-mail, but from whom the sender expects no particular action. The CC field is also used when the sender wants recipients to know who else is receiving the email.
- c. BCC: This field is for recipients to whom the e-mail is “blind copied”. (BCC stands for “blind carbon copy”.) Typically this includes those who the sender wants to see the e-mail, but whose identity the sender wants to conceal from recipients in the TO and CC fields.

[28] The BCC field does have good, convenient uses. One common use of the BCC field is for mass mailings. If the list of recipients is large, using the BCC field means that no recipient can see the names of the other recipients. If every recipient could see the entire list of recipients, it would be both tedious (because it requires scrolling through the list before getting to the message) and privacy-invasive.

[29] But good e-mail hygiene includes very careful use of the BCC field. It takes only a moment’s inattention to put addresses intended for the BCC field into the TO or CC fields.

[30] Moreover, because the BCC field is the least commonly used, some e-mail programs hide it by default. In other words, the sender must either change their e-mail settings to show the BCC field for every new e-mail, or must take extra steps to show the BCC field for the current e-mail. This detail may trip up inexperienced users, if they are not aware that BCC is an option.

What recommendations are appropriate?

[31] With this background, I turn now to the question of what recommendations are appropriate to address the kind of privacy breach that occurred in the present case.

[32] When the complaint was filed, the job competition in question was not yet concluded, so the possibility of prejudice was a live issue. The competition has since concluded. The Complainant does not allege, and I do not find, that there was any actual prejudice to the Complainant in the job competition itself. Nevertheless, the public disclosure of the e-mail address – and therefore the fact that the Complainant was an applicant – did cause the Complainant some distress.

[33] This sort of privacy breach can, in the human resources context, have serious consequences. It reveals who has applied for a job, which may be personally or professionally embarrassing for a candidate. It may put a candidate in an awkward position with respect to their current employer, their co-workers, their family, or the other candidates. It may give a candidate an advantage or disadvantage over the other candidates. It exposes contact information that a candidate may have wanted to keep confidential, and that may be misused by someone else.

[34] I have no evidence before me that there was a pattern of mistakes by this employee or any other HR employee. For purposes of this decision, I must assume the mistake happened just this once.

[35] On the individual level, HR's response to the privacy breach was appropriate. HR acknowledged the error and has apologized three times. The Complainant does not seek, nor would it be appropriate for me to recommend, any repercussions for the HR employee who made the mistake. We have all made mistakes with e-mail. We learn from the mistake and we carry on; and so it should be for the HR employee in this case.

[36] On the institutional level, HR's response has been less convincing. The deputy minister's letter to me of March 18, 2022, attaches nine policies or

procedures, including the entire staffing manual. These documents together run to hundreds of pages, none of which addresses directly the issue of e-mail hygiene. HR has not attempted to link these documents to the actual issue in the case.

[37] The letter also refers to general ATIPP training, but that training that does not address e-mail hygiene.

[38] The letter does make certain commitments about privacy protection, which I have quoted in the Facts section above. All of those commitments are stated in the future tense (“will continue”, “will review and update”, “will develop”).

[39] I acknowledge that there is no policy, or procedure, or training, which will prevent every mistake. What we can do is to look for changes to “the practices of the public body” that effectively and provably reduce the risk of the same mistake being repeated. After careful consideration, I have concluded that the four commitments made in the deputy minister’s letter would accomplish that objective – provided, of course, that HR actually follows through on them.

Conclusion

[40] The Department of Human Resources breached the Complainant’s privacy when an HR employee included the Complainant’s email address in the “CC” field of an email sent to the short-listed applicants in a job competition.

[41] The privacy breach was the result of a mistake by an HR employee. I do not have evidence before me of a broader problem. However, the consequences of a privacy breach in the HR context can be serious. The deputy minister of HR has made a series of commitments that, if kept, constitute a satisfactory response to the privacy breach in this case.

Recommendations

[42] I **recommend** that the Department of Human Resources follow through on the four commitments made in the March 18, 2022, letter from the deputy minister. For greater certainty, those commitments are quoted in paragraph 11 of this decision.

[43] I recommend that the deputy minister write a reporting letter to me no later than three months from the date of this decision, with details of how the four commitments have been kept.

Graham Steele

ᑲᑦᑦᑲ / Commissioner / Kamisina / Commissaire