OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report P-2018-004

July 10, 2018

Town of Wabana

Summary: The Complainant alleged that Town of Wabana (the "Town") staff e-mails were collected from their Town e-mail accounts without authorization by [named Town employee], and improperly used and disclosed by Town Council. The Town argued that as the computers used to access staff e-mails were Town property, there was no improper collection, use or disclosure. The Commissioner could not determine whether the e-mails in question were improperly collected, used or disclosed as they could not be produced for review. However, the Commissioner found the Town's lack of policies and procedures on access constituted a breach of the security provisions of the *Access to Information and Protection of Privacy Act, 2015*.

Statutes Cited: *Access to Information and Protection of Privacy Act, 2015*, S.N.L. 2015, c. A-1.2 sections 61 and 64.

Authorities Relied On: OIPC NL Report A-2016-021; *City of Ottawa v. Ontario*, 2010 ONSC 6835; *R. v. Cole*, [2012] SCC 53.I

File #0055-100-18-001

I BACKGROUND

[1] This Office received a privacy complaint under the *Access to Information and Protection of Privacy Act, 2015* (the "*ATIPPA, 2015*") alleging there had been improper access of Town of Wabana (the "Town") staff e-mails by [named Town employee]. The complainant believes that in January 2018 the named Town employee improperly collected e-mails of other staff members and disclosed them to Town Council.

[2] The Town responded to this complaint, acknowledging access to e-mails occurred but contending the e-mails were the property of the Town and therefore any access was not improper. It went on to indicate that the Town has no policies or procedures in place that address privacy and records management, and no remediation plan in place for responding to breaches of personal information.

[3] Neither the Town nor the Complainant could provide copies of the specific e-mails in question for this Office to review. Given the Town's admission that the named Town employee did access e-mails from co-workers e-mail accounts, the complaint proceeded to formal investigation in accordance with section 74(2) of the *ATIPPA, 2015*.

II PUBLIC BODY'S POSITION

[4] The Town acknowledged that staff emails were accessed by the named Town employee, maintaining that the named Town employee is "privy to all e-mails or any other mail or correspondence that comes to the town" and is "required to share all correspondence with the council."

[5] The Town went on to state that:

> *All e-mail accounts in the office uses [sic] the computer equipment of the Town of Wabana, are paid for by the Town of Wabana, are the property of the Town of Wabana and must be used for town business only…and the clerk has the authority granted to her by the [Municipalities] Act and by local council to proceed in a manner that is in the best interests of the town.*

It acknowledged that the named Town employee had access to all Town computers, and thereby the work e-mails of those assigned to each, but maintained that the "e-mails were set up for town business, hence all correspondence derived from e-mail accounts are the property of the Town of Wabana."

[6] Additionally the Town admitted not having any policies or procedures related to privacy or a breach remediation plan. The Town acknowledged that this complaint shed light on the need for such and expressed its intention to address this deficiency.

III COMPLAINANT'S POSITION

[7] The Complainant maintains that the collection of staff e-mails by the named Town employee was improper, as was the use of and disclosure to the Council. The Complainant alleged that there was no work purpose or function for the e-mails in question to have been accessed and viewed by other staff and Council, but rather they were being used to garner information on Town staff with a view to terminating their employment.

IV DECISION

[8] A public body's custody and control does not extend without limitation to personal information on workplace computers, as discussed in case law and previous reports of this Office. The Superior Court of Justice in Ontario held in *City of Ottawa* v. *Ontario (Information and Privacy Commissioner and John Dunn* that in regard to the personal communications of an employee:

> *[37] It can be confidently predicted that any government employee who works in an office setting will have stored, somewhere in that office, documents that have nothing whatsoever to do with his or her job, but which are purely personal in nature. Such documents can range from the most intimately personal documents (such as medical records) to the most mundane (such as a list of household chores). It cannot be suggested that employees of an institution governed by freedom of information legislation are themselves*

subject to that legislation in respect of any piece of personal material they happen to have in their offices at any given time. That is clearly not contemplated as being within the intent and purpose of the legislation.

[38] The question then is whether information stored electronically should be treated any differently. I do not see any rational basis for making such a distinction.

[39] There is, however, one difference in how the employer might treat electronic records somewhat differently and that relates to the security concerns posed by employees' use of email and the internet while at work. Understandably, employers who allow employees to use their electronic servers for personal matters will typically have policies to ensure that these electronic media are not being used in a manner that is inappropriate or illegal or that compromises the security of the entire system.

[40] In this case, the City of Ottawa had a Responsible Computing Policy which addressed, among other things, the personal use of IT services and assets by its employees. There were understandable restrictions on such use, none of which arise in this case. In order to ensure compliance with the policy, and for network management reasons, the City stipulated that it had the right to access its IT assets and information at any time and that monitoring may be done at any time without notice and without the knowledge of the individual users. Employees were therefore warned that if they had privacy concerns they should refrain from using the City's IT services to store or transmit personal-use information.

[41] It was the City's policy with respect to management of its IT services that led the Arbitrator to find that the personal emails of Mr. O'Connor were actually in the custody of the City. The Arbitrator held that the policy meant the City: (1) had physical possession and the right to possession of the emails; and (2) the City had the authority to regulate the use and disposal of the records on its system. In my view, those factors are not determinative of control given the purpose for which the City retained the right to monitor its system, as contrasted to the underlying purpose of freedom of information legislation.

[42] Employers from time to time may also need to access a filing cabinet containing an employee's personal files. That does not make the personal files of the employee subject to disclosure to the general public on the basis that the employer has some measure of control over them. The nature of electronically stored files makes the need for monitoring more pressing and the actual monitoring more frequent, <u>but it does not change the nature of the documents</u>, nor the nature of the City's conduct in relation to them. It does not, in my view, constitute custody by the City, within the meaning of the Act. [emphasis added]

[9] While the Town maintains that its ownership of the computers permits it to access staff e-mails, the Supreme Court of Canada (the "SCC") noted in *R. v. Cole*, [2012] SCC 53 that "ownership of property is a relevant consideration, but is not determinative," and employees maintain a "reasonable expectation of privacy" in the information contained on work computers.

[10] Obviously, the context of this matter is different in that we are not dealing with incursions on privacy in the context of criminal litigation. At the end of the day, the *ATIPPA, 2015* simply restricts the collection, use and disclosure of 'personal information' to circumstances authorized by the *Act*, regardless of the presence (or absence) of reasonable expectations of privacy.

[11] The relevant section of the *ATIPPA, 2015* is section 61(c), which states:

> *61. No personal information may be collected by or for a public body unless*
>
> *c) that information relates directly to and is necessary for an operating program or activity of the public body.*

[12] Therefore, it is necessary for this Office to examine the content of the emails in question to assess whether it constitutes personal information, and if so, whether access of this information by the named Town employee was authorized by section 61(c).

[13] As noted above, neither the Complainant nor the Town could provide copies of the e-mails in question for this Office to review. Although the e-mails were tabled at a private meeting of Council, we were informed that no copies were retained from that meeting. As we could not review them, we could not assess if they, in fact, contained personal information or determine whether their collection, use or disclosure constituted a breach of privacy pursuant to the *Act*.

[14] Any public bodies that permit the use of their computers for personal purposes require clear policies and direction to employees delineating the circumstances in which public bodies may access employee's personal information on those computers. These policies should set out how the collection of this personal information relates directly to and is

necessary for an operating program or activity of the public body. A public body cannot claim unfettered ownership of information on these work computers, but instead must maintain policies and procedures defining when access is allowed. The absence of any such policies or procedures on the part of the Town is contrary to section 64:

> *64. (1) The head of a public body shall take steps that are reasonable in the circumstances to ensure that*
>
> *(a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;*
>
> *(b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and*
>
> *(c) records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.*

[15] By way of example, the *Government of Newfoundland and Labrador Email Guidelines* prohibit the use of e-mail for purposes such as promoting hatred or distributing obscene material. Clearly, if there is reason to believe that an employee is using government's e-mail network in contravention of the law or this policy, the government may access and collect such personal e-mails pursuant to section 61(c) of the *ATIPPA, 2015*.

V CONCLUSIONS

[16] We could not determine whether a breach of privacy, as defined by the *ATIPPA, 2015*, occurred via the improper collection of staff e-mails by the named Town employee. We are satisfied that a breach of the *ATIPPA, 2015* security provisions did occur as the Town had not created proper policies and procedures setting out when access to personal information located on workplace computers may occur in the context of its operating programs and activities.

VI RECOMMENDATIONS

[17] Under the authority of section 76(2) of the *ATIPPA, 2015*, I recommend that the Town:

(a) Draft and put into effect safeguards regarding its duties under section 64 of the *ATIPPA, 2015*, including the circumstances in which the Town may collect the personal information of Town staff, whether on its computer network or otherwise;

(b) Ensure it is not collecting, using or disclosing personal information in contravention of the *ATIPPA, 2015*;

(c) Provide all staff and Council training and education related to the *ATIPPA, 2015* the duties it imposes on staff and Council; and

(d) Draft and put into effect a breach mediation plan protocol (as described in the Department of Justice and Public Safety's Privacy Breach Protocol).

[18] As set out in section 78(1)(b) of the *ATIPPA, 2015*, the head of the Town 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.

[19] Dated at St. John's, in the Province of Newfoundland and Labrador, this 10th day of July 2018.

Donovan Molloy, Q.C.
Information and Privacy Commissioner
Newfoundland and Labrador