OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report P-2018-001

February 22, 2018

City of St. John's

Summary: After experiencing an assault while on duty, a parking enforcement officer asked another City employee to access the alleged assailant's personal information stored on the Motor Registration Database. That employee accessed the personal information requested and provided it to the parking enforcement officer. After conducting an own motion investigation, the Commissioner found that the City had not discharged its duty pursuant to section 64(1)(a) of the *Access to Information and Protection of Privacy Act, 2015* to take reasonable steps to safeguard personal information against unauthorized access, use or disclosure. The Commissioner recommended that the City ensure all its employees receive adequate privacy training, renew its Information Sharing Agreement with Service NL, and do more to foster a privacy culture, especially within its Department of Planning, Engineering and Regulatory Services.

Cited Statutes: *Access to Information and Protection of Privacy Act, 2015*, SNL 2015, c A-1.2.

Other Resources: *Information Sharing Agreements: Essential Administrative Safeguards* (http://www.oipc.nl.ca/pdfs/audit_of_information_sharing_agreements.pdf)

I BACKGROUND

[1] On December 8, 2017 the City of St. John's, in compliance with Section 64(4) of the *Access to Information and Protection of Privacy Act, 2015* (the *ATIPPA, 2015*), notified the OIPC of a privacy breach involving the Motor Registration Database (MRD). Three City employees in its Department of Planning, Engineering and Regulatory Services had access to the MRD pursuant to an Information Sharing Agreement (ISA) entered into between the City and Service NL. One of those employees accessed the MRD on December 5, 2017 at the request of a parking enforcement officer, and disclosed personal information to him thereby breaching the *ATIPPA, 2015*. On December 19, 2017 the OIPC notified the City that it had opened an own motion investigation pursuant to section 73(3) of the *ATIPPA, 2015*.

II PUBLIC BODY'S POSITION

[2] The City conducted its own internal investigation and determined that the employee in question accessed the personal information of a City resident on the MRD without a legitimate business purpose to do so. The City appears to have accepted that the employee acted on her own and not as the result of a request from anyone else. Inconsistencies between the statements of the employees interviewed by City human resources staff and other evidence lead me to conclude that the employee acted at the request of the parking enforcement officer who lacked direct access to the MRD. The City acknowledges a lack of privacy training, especially within its Department of Planning, Engineering and Regulatory Services, and indicates that it will prioritize executing a new ISA in the immediate future.

III DISCUSSION

[3] Employees should not have to endure violence or threats of violence in the performance of their duties. Parking enforcement officers unfortunately are frequent targets of citizen ire for simply enforcing parking by-laws.

[4] On December 3, 2017, a resident of the City allegedly went beyond verbal abuse and assaulted a parking enforcement officer who was in the process of ticketing the resident's vehicle. The officer promptly reported the assault to the Royal Newfoundland Constabulary (RNC) and his superiors, but appeared dissatisfied with the timeliness of the responses of both. The parking enforcement officer learned that the assigned investigator would be off shift for a number of days when he called the RNC seeking an update.

[5] The officer's colleagues appeared frustrated that they had heard nothing from management, even though management was advised of the incident on December 3, 2017. Understandably, parking enforcement officers are concerned when an unknown person assaults a fellow officer while issuing a parking ticket. Parking enforcement officers do not have access to the MRD. On the afternoon of December 5, 2017, the officer approached another employee in his Department and asked her to access the resident's personal information by entering a license plate number into the MRD. The employee entered the license plate number into the MRD and obtained the resident's name and address, which she provided to the officer.

[6] The employee who entered the license plate number into the MRD mentioned what she had done to a staff member of the City's legal department, who appropriately reported the breach to the City's ATIPP Coordinator, leading to the breach report to the OIPC.

[7] From reviewing the records generated as a result of the City's investigation, a number of concerns emerged, including that:

- City staff did not view the unauthorized access and disclosure of personal information as significant;
- City staff appeared generally unaware of their legal duties and obligations pursuant to the *ATIPPA, 2015*; and,
- some City staff employed in the Department of Planning, Engineering and Regulatory Services were hostile to the member of the City's legal department who appropriately recognized and reported the breach of privacy.

[8] Section 64(1) of the *ATIPPA, 2015* places obligations on a public body to employ reasonable measures to safeguard personal information in its custody or control:

> *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*.

[9] If its employees receive no or inadequate training with respect to the legal requirements of the *ATIPPA, 2015*, and in particular as to what constitutes unauthorized collection, access, use or disclosure, a public body has not met its obligations under section 64. In the circumstances of this breach, the City's inadequate protection of personal information is aggravated by the fact that City employees' access to the MRD is granted at the discretion of Service NL. Residents provide personal information to public bodies as required in order to obtain services, including the issuance of driver's licenses. In the case of driver's licenses, residents provide their personal information to Service NL for entry into the MRD. Service NL is responsible for safeguarding the privacy of the personal information it collects.

[10] As discussed extensively in our audit of Service NL, *Information Sharing Agreements: Essential Administrative Safeguards*, it must ensure that all third parties granted access to the MRD employ privacy safeguards that, at a minimum, comply with an ISA's terms and legal duties pursuant to the *ATIPPA, 2015*.

[11] At the time of this breach, the ISA entered into with the City had expired (but still followed in principle). That ISA referenced standards for the City's adherence, including ensuring compliance with an earlier version of the *ATIPPA, 2015*. Given that the ISA was in place for five years, the lack of privacy training for City staff is cause for concern. Public bodies should

not receive access to the MRD without a clear commitment to privacy training and providing confirmation of that training to Service NL. By auditing compliance with an ISA, Service NL can identify lapses in the efforts of third parties to safeguard personal information stored in the MRD. Failure to address those lapses to the satisfaction of Service NL can and should result in the revocation of a third party's access to the MRD.

[12] In this case, the City advised that employees in its Department of Planning, Engineering and Regulatory Services received some *informal* privacy training on execution of the ISA in 2012. Given that the City also collects personal information, its obligations pursuant to the *ATIPPA* (which underwent a significant revision since 2012), its obligations pursuant to the ISA and normal staff turnover, this is a disappointing example of a public body failing to meet its obligations pursuant to section 64 of the *ATIPPA, 2015*. In regards to the City's access to the MRD, one must also question whether Service NL should have continued the City's access to the MRD in the face of the City's dereliction of its duties.

[13] To be fair, the now-expired ISA lacked specific requirements for privacy training and recording the delivery of that training. As discussed in the Report, *Information Sharing Agreements: Essential Administrative Safeguards*, all renewed ISAs will be more robust and will address the deficiencies in previous versions of Service NL's standard ISA template.

[14] Appropriately, the City has policies and procedures in place to promote employee safety. One of those policies, *Workplace Violence Prevention*, sets out safe work practices for parking enforcement officers. The policy requires officers to report incidents of workplace violence to management. Management is required to notify all parking enforcement officers, in a timely manner, of any incidents that affect their safety.

[15] It is beyond the purview of this Report to determine the City's compliance with its *Workplace Violence Prevention* policy in regards to the events of December 3, 2017. Parking enforcement officers must address with management any dissatisfaction with decisions about whether and when management notifies them of incidents of violence or the level of detail provided. Parking enforcement officers cannot take matters into their own hands by indirectly accessing personal information contrary to the *ATIPPA, 2015*. There may be

incidents that require management to access personal information from the MRD and disclose that information to parking enforcement officers in compliance with its *Workplace Violence Prevention* policy.

IV CONCLUSION

[16] The City failed to discharge its duty to implement reasonable measures to safeguard personal information against unauthorized access, use or disclosure. The City also did not recognize the hostility expressed towards the staff member who recognized and reported the breach. A public body's privacy culture must instill privacy values in all staff and address negative responses to its privacy champions.

[17] There are many positives:

- The City promptly reported the breach and notified the affected individual;
- City staff fully cooperated with our investigation and promptly responded to requests for records and other information;
- The City arranged with the OIPC's Advocacy and Compliance branch for sixty-nine of its staff members to receive privacy training in March of 2018. Staff in the Department of Planning, Engineering and Regulatory Services are included in this group;
- Members of the City's legal and ATIPP staff participated in an education session in November of 2017. That training provided an overview of the entirety of the *ATIPPA, 2015*. Staff from the OIPC and the provincial Access to Information and Protection of Privacy Office delivered the training;
- The City's Senior Executive Committee recognizes the need to ensure the adequacy of its efforts to safeguard personal information, including the identification of its personal information holdings and databases and the staff with access to same; and,

- The City is also actively working towards execution of a new ISA with Service NL. Compliance with that ISA will result in the City being required to confirm regularly with Service NL that it has adequate privacy training and other safeguards in place.

V RECOMMENDATIONS

[18] As noted above, the City has acknowledged relevant shortcomings and commendably committed to necessary remedial measures. Under the authority of section 76(2) of the *ATIPPA, 2015*, I recommend that the City take steps:

- to ensure that all staff with access to personal information receive formal privacy training within 90 days of the date of this Report and to provide the OIPC with confirmation of same;
- to develop policies addressing privacy training for new hires and for annual training for all staff with access to personal information;
- to review and update its related forms and other documents, including its Oath of Confidentiality;
- to address the hostility displayed by members of its Department of Planning, Engineering and Regulatory Services and to work towards establishing a positive privacy culture in that Department; and

[19] Under the authority of section 76(1) of the *ATIPPA, 2015*, I recommend that the City renew its ISA with Service NL within 30 days of the date of this Report and in the absence of that renewal that the City stop using or disclosing personal information stored in the MRD.

[20] As set out in section 78(1)(b), the head of the City must give written notice of his or her decision with respect to these recommendations to the Commissioner within 10 business days of receiving this Report.

[21] Dated at St. John's, in the Province of Newfoundland and Labrador, this 22nd day of February 2018.

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