OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report P-2015-002

November 23, 2015

Royal Newfoundland Constabulary

Summary: The Complainant submitted a privacy complaint under the *Access to Information and Protection of Privacy Act, 2015* (the "*ATIPPA, 2015*") in respect of a notice which the Complainant received from the Royal Newfoundland Constabulary (the "RNC"). The notice advised the Complainant that information about the Complainant had been accessed by an RNC employee without a valid business reason. The RNC also submitted a Privacy Breach Incident Report in relation to this matter. Additionally the RNC submitted two other Privacy Breach Incident Reports to this Office related to two other incidents of inappropriate access by employees which occurred this year. The Commissioner initiated an investigation on his own motion into these two events. Given the related issues and the possibility of a systemic problem within the RNC, the Commissioner decided to respond to all three matters collectively. The Commissioner found that the RNC had some administrative, technical and physical safeguards in place to protect personal information from unauthorized access; however, it is clear from these recent incidents that these mechanisms have not been fully absorbed, implemented and understood by RNC staff. The Commissioner found that the RNC must now go further in developing and employing these protections so that they are as strong as reasonably possible and, additionally, so that employees fully appreciate the application and implications of same. The Commissioner made several recommendations to assist the RNC in preventing such situations in the future. The recommendations include taking additional steps to monitor access both in terms of providing and removing access to the information system based on professional roles and implementing an on-going, robust random auditing program. It would also include protocols to ensure that information is securely maintained.

Statutes Cited: *Access to Information and Protection of Privacy Act*, S.N.L. 2002, c. A-1.1, as amended, section 34; *Access to Information and Protection of Privacy Act, 2015*, S.N.L. 2015, c. A-1.2, section 64.

Authorities Cited: Office of the Information and Privacy Commissioner of British Columbia, Investigation Report F10-02.

I BACKGROUND

Incident 1

[1] On May 26, 2015, this Office received a Privacy Breach Incident Report outlining a privacy breach involving an officer of the Royal Newfoundland Constabulary ("RNC") who inappropriately accessed and used Motor Registration Division ("MRD") records to obtain the VIN number and owner's name of a particular motor vehicle. In January, 2015, the officer used and possibly disclosed the information for the purpose of assisting a family member in the purchase of the vehicle. The RNC was made aware of the situation through a complaint made by a member of the public. The officer accessed MRD records for this purpose on four (4) separate occasions. The officer has admitted to these accesses, but denies disclosing the entirety of the information.

Incident 2

[2] On June 30, 2015, this Office received a Privacy Complaint from the Complainant who had been notified by the RNC that a civilian employee of the RNC had inappropriately accessed the Complainant's personal information. This Office was also notified, via a Privacy Breach Incident Report, that this employee had accessed and disclosed the personal information of other individuals who were known or related to the employee. In all cases, the information was accessed for personal reasons from the RNC Integrated Constabulary Automated Network ("ICAN"). The RNC was made aware of this situation through a complaint made by a member of the public. From 2010-2014, the employee accessed the personal information in ICAN on thirty-seven (37) occasions, in relation to twelve (12) individuals including the Complainant and the employee herself, resulting in four hundred and seventy-four (474) separate incidents. The employee has admitted to the RNC that four hundred and thirty-nine (439) of those incidents were without a valid purpose. There was also an indication in the Privacy Breach Incident Report that the employee destroyed personal information, relating to someone other than the Complainant, on one (1) occasion. The employee also admitted to carrying out this act. There is a further indication that the employee disclosed the information she obtained on three (3) separate occasions to a significant other or friend. The employee has indicated that her intentions were not malicious but merely personal curiosity.

Incident 3

[3] On July 9, 2015, this Office received a Privacy Breach Incident Report outlining a privacy breach involving another civilian employee of the RNC inappropriately accessing and disclosing MRD records for the purpose of verifying the status of the registration on a particular vehicle for a family member and for training purposes. The RNC was made aware of this situation through a complaint made by a government employee. From August, 2011 to June, 2015, the RNC employee accessed the MRD records for this purpose on thirty-nine (39) separate occasions; there is no indication of the number of disclosures; however, it appears that any disclosure was limited to the individual to whom the information related. The employee has admitted to these accesses.

[4] Following receipt of the latest Privacy Breach Incident Report, I initiated an investigation on my own motion in respect of the two other breaches so that I could examine all three breaches as a group and investigate the apparent systemic issues.

[5] It is concerning to have received notification of three privacy breaches of a similar nature in such a short period of time. It is of crucial importance to the integrity and effectiveness of the RNC as a law enforcement agency that these activities are eliminated. The RNC relies on citizens, complainants and witnesses to come forward with information, and incidents such as these may undermine the public confidence in the RNC's ability to carry out its role. Furthermore, incidents such as these may have a chilling effect on information provided to the RNC if individuals feel confidentiality and privacy cannot be ensured.

[6] I decided to provide a written Report because collectively these breaches suggest a common misunderstanding within the RNC of what is meant by privacy and the application and implications of the *Access to Information and Protection of Privacy Act, 2015*("*ATIPPA, 2015*"). It is my intention that this Report serve to assist the RNC in clarifying any such confusion.

II ROYAL NEWFOUNDLAND CONSTABULARY SUBMISSION

[7] The RNC provided separate submissions for the Complaint file and the own motion investigation file. The submissions included, but were not limited to, the initial complaints that lead to the discovery of the

incidents, the RNC's internal investigations documents; auditing information; privacy-related policies, procedures and other documentation, and human resource documentation for the employees involved.

[8] The human resources documentation indicates that all employees, both civilian and law enforcement, sign either an Oath of Office or Oath of Secrecy. These documents state:

> [Oath of Office]: […] *I will not, directly or indirectly, without due authority disclose to any person any information or matter that may come to me in the performance of my duties or by reason of my employment with the Royal Newfoundland Constabulary, SO HELP ME GOD.*
>
> [Oath of Secrecy]: […] *I will not, directly or indirectly, without due authority disclose to any person any information or matter that may be obtained by me in the course of my duties as a Special Constable and a member of the Royal Newfoundland Constabulary, SO HELP ME GOD.*

[9] To remind staff of these assurances, the RNC also provided staff with copies of Routine Orders 2013-002, 2015-002, and 2015-006, issued January 17, 2013, January 20, 2015 and April 10, 2015 respectively. The 2015-006 Order states:

> *All staff are reminded that all RNC records and information is strictly for official duties related to law enforcement. Release of any RNC information without authorization for non-law enforcement purposes is strictly prohibited.*
>
> *Commencing your employment with the Royal Newfoundland Constabulary you swore to the following Office of Oath/Confidentiality:*
>
> *"I will not, directly or indirectly, without due authority, disclose to any person any information that may come to me in the performance of my duties."*
>
> *Individuals will be held accountable for breaches of confidentiality or privacy regarding RNC records or information. A breach includes unauthorized access too, use or disclosure in any manner (including written, electronic or verbal) of RNC records or information.*

[10] The 2015-002 Order states:

> *All staff are reminded that all RNC records and information is strictly for official duties related to law enforcement. Release of any RNC information for personal reasons or non-law enforcement related reasons is strictly prohibited.*
>
> *Commencing your employment with the Royal Newfoundland Constabulary you swore to the following Office of Oath/Confidentiality:*
>
> *"I will not, directly or indirectly, without due authority, disclose to any person any information that may come to me in the performance of my duties."*

> *Individuals will be held accountable for breaches of confidentiality or privacy regarding RNC records or information. A breach includes unauthorized access too, use or disclosure in any manner (including written, electronic or verbal) of RNC records or information.*

[11] These Orders were signed by the Chief of Police and were circulated to all employees. Employees were also reminded of their Oaths in Routine Order 2013-002, albeit in relation to the use of social media.

[12] Included in the RNC online Policy Manual, which all employees are obligated to familiarize themselves with, is a chapter entitled, *Information Management and Technology* which the RNC provided to this Office. This chapter contains the following guidelines:

> […] *4.2 Access to RNC's information and technology resources is for the purpose of conducting RNC business.*
>
> *4.3 Access by employees to RNC information for personal reasons or non-law enforcement related reasons is prohibited and any improper access by an employee will cause an employee to be subject to discipline up to and including dismissal.*
>
> *a. Information is only accessible to officers and RNC civilian employees for the purposes of law enforcement and related programs and activities.*
> *b. Random audits of officers and civilian RNC employees access to RNC information will be conducted to ensure there has been no improper access to RNC information for personal or non-law enforcement related reasons by officers or civilian employees.* […]
>
> *4.6 The following conditions are unacceptable and will result in discipline up to and including dismissal.*
> *a. Users must not:*[…]
>
> *(3) use the Employer's equipment for personal purposes;* […]
>
> *9.1 The Access to Information and Protection of Privacy Act requires that:*[…]
>
> *b. access to personal and confidential information is limited to those that need to use it to do their job;* […]
>
> *10.3 Motor Registration Division (MRD):* […]
>
> *e. Front line personnel have access to the license and registration information on MRD to assist with identification of drivers and vehicles. The information is used for police purposes only and shall not be shared with other agencies.*[…]
>
> *10.4 Integrated Constabulary Automated Network (ICAN):* […]

> *c. All sworn employees of the RNC will be permitted to access ICAN. The extent of privileges will vary from employee to employee. An employee's privileges will be determined by the employee's supervisor in consultation with the ISD.*
>
> *d. all personnel will receive ICAN training to support the level of privileges that their position requires within the organization. All training will be coordinated through the RNC Training Section.* […]

[13] The RNC also provided the slide deck of a presentation on access and privacy which was given to at least two of the employees.

III DISCUSSION

[14] The breaches occurred both before and after the coming into force of the *ATIPPA, 2015*. Consequently, the relevant sections of both the *ATIPPA, 2015* and its previous version must be examined.

[15] The relevant section of the *Access to Information and Protection of Privacy Act*, S.N.L. 2002, c. A-1.1, as amended, is as follows:

> *36. The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.*

[16] The relevant, comparable section of the *ATIPPA, 2015,* is as follows:

> *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.*

[17] While the wording is more expansive in the current *ATIPPA, 2015* the intention is the same in relation to the protection of personal information. A public body must act reasonably to protect personal information from theft, loss and unauthorized collection, access, use or disclosure. Furthermore, a statutory obligation is imposed on a public body to ensure that personal information in its custody and control is securely maintained and disposed of by the public body.

[18] There are a few things which are clear at the outset. First, each employee accessed personal information outside of the scope of their employment duties; each employee admitted to this. Their reasons for accessing the information were purely personal. However, based on the roles of these individuals (Constable, Communications Technician and a Clerk Typist with Patrol Operational Support Services) and the general responsibilities of the RNC, these individuals require a broad range of access to Motor Registration Division records or the ICAN database.

[19] Second, the RNC has developed certain safeguards including auditing protocols, privacy policies and access and privacy training to assist in the protection of information and prevent unauthorized access. Audits did not capture the incidents in question and it is difficult to say whether an audit would have captured any of the incidents being discussed herein. However, the lack of auditing procedures is certainly a hindrance to capturing and preventing unauthorized accesses and therefore, indicative of an effective security measure.

[20] Finally, none of the mechanisms currently employed by the RNC in respect of the protection of personal information have been fully absorbed, implemented and understood by RNC staff. Therefore, the RNC must now go further in developing and employing these protections so that they are as strong as possible and, additionally, so that employees fully appreciate the application and implications of same.

[21] To achieve this result, the RNC must address all the elements of privacy safeguard: technical, administrative and physical.

Technical Safeguards

[22] There is no evidence before me to suggest that the role-based access model employed by the RNC to provide and remove employee access to personal information is inadequate. However, as I have discussed in the past, role-based access should be based on the need-to-know principle, so that employees have access to the least amount of that personal information necessary to perform their job functions.

[23] Consequently, it is incumbent on the RNC to review the access levels that it has provided to every employee and every role to determine if, in fact, the level of access is based on the "need to know" principle.

[24] This is consistent with the statements set out in the RNC Policy and Procedure manual outlined above. In so far as MRD records are concerned, only those employees who need access to this information in order to perform police duties, or assist in performing these duties as part of their employment responsibilities should have access. In respect of ICAN, employees should have access to the information only as required to perform the tasks which are necessary in their role.

[25] Once the level of access issue is addressed, the RNC must then turn its attention to its auditing capabilities. The documents provided by the RNC indicate that the RNC and Service NL share responsibility for auditing MRD records; however, currently, there is no mechanism in place for auditing RNC use of MRD records. A proposal for how such an audit could be conducted has been drafted but not yet implemented. It is proposed that on a monthly basis Service NL would provide the RNC with a print-out of access or inquiries for the previous month. It is then the responsibility of the RNC to review this document and determine if the accesses relate to an authorized purpose.

[26] The RNC is responsible for auditing ICAN access; however, there are no set policies, procedures or practices in place for these audits. Currently audits are conducted on an as-needed basis (i.e. where there is a complaint) or at the direction of the directors of each particular division.

[27] In respect of MRD auditing, the proposed system appears to be a reasonable security arrangement to detect and deter inappropriate access. The system should ensure that random audits are run such that each employee is captured at least once annually. Employees should also be notified after an audit is performed on their usage and advised of the results. In respect of ICAN auditing, the system must be strengthened. Audits must be run on a regular basis, as well as on an as-needed basis. Additionally, as with the MRD audits, each employee should be audited at least once annually and notified after an audit is performed of the results.

Administrative Safeguards

[28] There is a prevailing attitude at the RNC that accessing, disclosing, using or destroying personal information outside of employment duties is acceptable so long as the act is in respect of a friend or family member, with or without their consent. The unspoken belief is that it is not a breach of the individual's privacy as there is no harm intended; in fact, in most cases the employee is of the opinion that they are assisting the individual. At least two of the employees involved in these incidents indicated that this was a

common practice. Employees seem to become more entrenched in this belief when the information is not disclosed to anyone, or at least to anyone other than the person whom the information is about or someone related to that individual.

[29] This prevailing attitude represents the thin edge of the wedge. Tolerating this behavior, suggests to employees that the RNC's access to information and protection of privacy policies and procedures are flexible and there will be no worry or hesitation based on repercussions. It is clear that additional training is required to lead a culture change toward a better understanding of what is meant by privacy, the obligations and responsibilities of the *ATIPPA, 2015* and the need to protect personal information from unauthorized access, no matter the intention of the accessing individual.

[30] The submission provided by the RNC includes a privacy training presentation given to employees in the Patrol and Criminal Investigations Divisions and Operational Support Area (Communications). This presentation, while thorough, clearly implies to employees that the interpretations of this Office in relation to the *ATIPPA, 2015* are of no consequence and do not need to be followed. I find this disconcerting and I would much prefer that representatives of the RNC initiate a dialogue with my Office in the event of a disagreement with the interpretation of the statute that my Office oversees. To do otherwise would be a disservice to the RNC and its employees in the event of future investigations.

[31] The training provided by the RNC must be updated to reflect the *ATIPPA, 2015*, and additionally, given that employee misconduct seems to be featured in each these breaches, the training should be careful to reference and educate employees on section 115 of the *ATIPPA, 2015* which states:

> *115. (1) A person who wilfully collects, uses or discloses personal information in contravention of this Act or the regulations is guilty of an offence and liable, on summary conviction, to a fine of not more than $10,000 or to imprisonment for a term not exceeding 6 months, or to both.*
>
> *(2) A person who wilfully*
>
> *(a) attempts to gain or gains access to personal information in contravention of this Act or the regulations;*
> *(b) makes a false statement to, or misleads or attempts to mislead the commissioner or another person performing duties or exercising powers under this Act;*
> *(c) obstructs the commissioner or another person performing duties or exercising powers under this Act;*
> *(d) destroys a record or erases information in a record that is subject to this Act, or directs another person to do so, with the intent to evade a request for access to records; or*

> *(e) alters, falsifies or conceals a record that is subject to this Act, or directs another person to do so, with the intent to evade a request for access to records,*
>
> *is guilty of an offence and liable, on summary conviction, to a fine of not more than $10,000 or to imprisonment for a term not exceeding 6 months, or to both.*

[32] Consequently, while privacy training and oaths of confidentiality are conducted by the RNC, additional training is required. The training must cover the definition of "personal information", auditing, unauthorized access and disclosure, proper use of personal information, the "need to know" principle and privacy versus confidentiality.

Physical Safeguards

[33] The destruction of personal information is not to be taken lightly. It is to be done properly, securely and by authorized persons. The RNC does not appear to have sufficient preventative measures in place to protect personal information from being removed from its premises. Nor does it appear to have any policies which discuss the removal of information from its premises and the proper methods of destroying personal information. Each of these safeguards must be developed and implemented by the RNC

1V RECOMMENDATIONS

[34] Pursuant to sections 76(2) and 77 of the *ATIPPA, 2015*, I recommend that:

(a) the role-based access model currently in place at the RNC should immediately be reviewed and roles should be defined as specifically and granularly as practicable. The amount of personal information available to each employee should also be reviewed so that each role only has access to the minimum amount of personal information necessary to perform their functions;

(b) the role-based access model should be regularly checked and updated so that changes in roles are accurately reflected;

(c) all staff should complete privacy training each year that includes a comprehensive privacy tutorial with specific modules on privacy issues related to electronic information systems and the other topics I have outlined above. Completion of this training should be tracked in each employee's personnel file and linked to an annual renewal of user privileges;

(d) oaths of confidentiality or oaths of office should also be revisited and amended as necessary when employees change roles. These undertakings should reflect the "need to know" principle;

(e) a Privacy Impact Assessment of the ICAN database and the RNC use of MRD records should be completed within 6 months of receipt of this Report;

(f) the auditing system for MRD usage by RNC employees must be implemented as discussed above. This includes policies, procedures and protocols for this system. I will follow-up on the establishment of this auditing system in 6 months;

(g) the auditing system for ICAN usage needs to be formalized. Proper policies, procedures and protocols must be developed including policies mandating regularly occurring audits on all divisions. I will follow-up on the establishment of this auditing system in 6 months; and

(h) policies, procedures and protocols must be developed in respect of the proper handling of personal information to ensure that it is only destroyed with authorization in a secure manner. Policies, procedures and protocols must also be developed to ensure that personal information cannot be removed from RNC premises without authorization and only for limited purposes. I will follow-up on the establishment of these policies, procedures and protocols in 6 months.

[35] As set out in section 78(1)(b) of the *ATIPPA, 2015* the head of the RNC must give written notice of his decision with respect to the above recommendations to the Commissioner and the Complainant within 10 business days of receiving this Report.

Dated at St. John's, in the Province of Newfoundland and Labrador, this 23 day of November, 2015.

E. P. Ring
Information and Privacy Commissioner
Newfoundland and Labrador