OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report P-2023-002

August 31, 2023

Royal Newfoundland Constabulary

Summary: Two Complainants alleged that an employee of the Royal Newfoundland Constabulary (RNC) had improperly accessed their personal information. An internal audit confirmed that two RNC employees had accessed the two Complainants' personal information and that the access was contrary to RNC policy and operational purposes. The RNC took disciplinary measures against the two employees, which were upheld at arbitration. In response to complaints, our Office undertook a privacy investigation. A prosecution was commenced under section 115 of *ATIPPA, 2015* resulting in a guilty plea by one employee and the acquittal of the other. The Commissioner recommended that the RNC continue efforts to improve its culture of privacy, expand training, and implement upgrades to its system to assist with auditing and monitoring access.

Statutes Cited: *Access to Information and Protection of Privacy Act, 2015*, SNL 2015, c. A-1.2, sections 115;

Royal Newfoundland Constabulary Act, section 60.

Authorities Relied On: NL OIPC Report: *Access Controls: Royal Newfoundland Constabulary;* January 13, 2023

Arbitration Award, RNC and NAPE, January 17, 2022
Royal Newfoundland Constabulary *Policy and Procedure Manual on Confidentiality* (General Order 339, October 27, 2015)

Files 0040-060-18-010 and -011

BACKGROUND

Privacy Complaints

[1] In late 2017, the Royal Newfoundland Constabulary ("RNC") received complaints from two individuals (the "Complainants") alleging that an RNC civilian employee had accessed information about the Complainants in police files for malicious or improper purposes. The RNC conducted an audit of its databases and confirmed that two civilian employees had accessed such files without any apparent operational purpose. Upon being notified of this finding by the RNC, the two Complainants filed privacy complaints with this Office under the *Access to Information and Protection of Privacy Act, 2015* ("*ATIPPA, 2015*") in March 2018.

[2] The RNC response to our complaint investigation confirmed that an audit of the Integrated Constabulary Automated Network database ("ICAN") access logs showed that the personal information of the two Complainants (as well as that of several other individuals who did not file complaints) in the RNC database had been improperly accessed on several different occasions and used by the two civilian employees (referred to here as "AB" and "CD"). The RNC did not confirm that the information had been improperly disclosed to anyone else.

Disciplinary Measures

[3] The RNC advised that, following the audit, it had conducted disciplinary interviews with each of the two employees in January and February 2018. One individual (CD) admitted to improperly accessing information, partly on behalf of the other employee (AB), and was given a one-month unpaid suspension. The other employee, AB, denied all impropriety but the RNC concluded that the employee had in fact improperly accessed the information. The RNC imposed a two-month unpaid suspension. As a further measure, the RNC subjected both employees to more frequent monitoring and audits upon their return to work.

Prosecutions

[4] Our Office interviewed the Complainants and RNC personnel in March 2018 and reviewed the RNC privacy investigation and disciplinary files. In the fall of 2018, the OIPC decided to initiate prosecutions of both individuals under section 115 of *ATIPPA, 2015*:

> *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.*

[5] The individual (CD) who had earlier admitted to the privacy breaches plead guilty in Provincial Court in May 2019 and was given an absolute discharge. The other individual (AB) plead not guilty. The case proceeded to trial, which was initially scheduled for August 2019. After several delays, the trial began but AB was acquitted on February 20, 2020 on the basis that insufficient evidence was provided to the court by the Crown to meet the burden of proof.

[6] Our own privacy investigation had been placed on hold pending the outcome of the prosecutions. That delay was further extended when we were notified that the Crown was considering an appeal of the AB acquittal. The appeal was heard in October 2021, and the acquittal was subsequently upheld. Our privacy complaint investigation was finally resumed in January 2022.

Discipline Arbitration

[7] In the meantime, the union representing civilian RNC employees had filed a grievance on behalf of AB contesting the discipline imposed by the RNC. The arbitration hearing was held in November 2021. The arbitrator's award, dated January 17, 2022 found that the employee had:

> *…accessed personal information of [certain individuals] without a valid business reason, on the three dates alleged by the Employer. The Grievor's access of information was a breach of privacy and a violation of the expectation of employees, the RNC Confidentiality Policy, Routine Orders, Oath of Confidentiality, Oath of Office and the ATIPP Act. The Employer has proven the allegation in the letter of discipline on the balance of probabilities and had just cause for discipline.*

[8] The arbitrator upheld the finding of misconduct and the disciplinary penalty of two months' suspension without pay imposed on AB by the employer.

Resumption of Investigation

[9] The external legal proceedings having finally been completed, our Office in January 2022 notified the RNC that we would resume the privacy complaint investigation. Given the passage of time we advised the RNC that we needed to complete an update on the issues to be addressed (see Issues one through eight, below). We received submissions on those issues from the RNC, which will be incorporated into the assessment to follow.

[10] Concurrently with the events described above, our Office had launched a separate access control audit of the RNC. The purpose of this audit was:

> *… to examine the access controls in place in specific RNC systems. As electronic access controls will not prevent an authorized user from unauthorized access, use or disclosure of the information, other safeguards are required to ensure users understand why they have access, what they are allowed to do with this access and any consequence of non-compliance. As such, the audit also examines associated policies, procedures and training.*

[11] The audit was completed and our Office issued a Report entitled Access Controls in January 2023. As many of the findings and conclusions bear directly upon the issues dealt with in this privacy complaint investigation, the audit report will be cited from time to time in the present Report.

ISSUES

[12] The following issues are to be addressed in this Report.

1. Whether RNC privacy policies and specific policies on operational access to information are reasonably adequate.
2. Whether privacy training is adequate. Whether Oaths of Confidentiality should be rewritten to emphasize personal information.
3. Whether privacy awareness activities and resources are adequate.
4. Whether operational access to databases (ICAN, MVR, CPIC) are sufficiently restricted to individuals who need such access.

5. Whether current access audit capability is sufficient – in particular, whether audits can detect not only whether there is improper access, but also whether employees can add information to the databases without oversight.
6. Whether there were gaps in the evidence – was there a possible legitimate operational reason for access that was not recorded, such as a verbal request?
7. Is there an issue with weak culture of privacy in the RNC workplace? Can we recommend improvements?
8. The RNC investigation process, the internal audit in response to the complaint, and the disciplinary investigation, were completed before the OIPC became involved. Is that how it should be?

DECISION

[13] After thorough review of the evidence, we accept and rely on the findings of the RNC investigation that the two employees in question accessed information of the Complainants from the ICAN database on several occasions without a valid operational purpose. These actions breached the privacy of the Complainants and others, contrary to *ATIPPA, 2015*, and violated RNC policies and procedures.

[14] Our conclusion is reinforced by the January 17, 2022 findings and conclusions of the grievance arbitrator referenced previously. The arbitrator's findings were reached after a three-day hearing of the evidence of witnesses, a review of voluminous documentary evidence and review of the submissions of both the employer and the union.

[15] We have concluded that the personal privacy of the Complainants was breached notwithstanding that AB was acquitted on the section 115 offence charges for reasons specific to that case. Our present review is now focused primarily on the privacy practices of the RNC as an organization and compliance with *ATIPPA, 2015*. What follows are our findings about its policies, practices, and procedures.

RNC Policies and Procedures

[16] *Order 339 (Confidentiality, 2015)* is a comprehensive policy statement governing the treatment of all types of information held by the organization, including personal information of third parties. It states, in part:

> *The RNC has both a legal and ethical responsibility for the information generated within the fulfillment of its mandate as a police service, and, the RNC is committed to protecting the privacy of personal information and the confidentiality of the law enforcement information in its custody and control. It is the responsibility and obligation of RNC employees, to ensure that information to which they have access is kept private and confidential.*

[17] This Order reflects requirements established in the *Royal Newfoundland Constabulary Act*. Section 60 recognizes the importance of confidentiality, stating in part:

> *60.(1) A police officer, an employee of the constabulary, an investigator, the commissioner, adjudicators and all persons acting under this Act shall preserve secrecy in respect of all information obtained in the course of their duties and shall not communicate that information to another person…."*

[18] As confirmed by our *Access Controls* audit report, we are satisfied that this comprehensive and highly-detailed policy, and other accompanying policies, rules and procedures, are sufficient to provide a sound basis for the organizational control of access, use, disclosure and protection of personal information in RNC custody. Furthermore, the RNC has taken steps to revise and update its confidentiality, information management and other related policies to bring them even more concretely into accordance with *ATIPPA, 2015*.

Oaths of Confidentiality

[19] Every RNC employee must swear an oath of confidentiality upon commencement of employment and again periodically thereafter. We are satisfied that the existing language is adequate for the purpose. While the oath itself may not specifically refer to *ATIPPA, 2015* or to the personal information of citizens, the oath is embedded in the above-referenced Confidentiality policy, which does.

Training and Awareness Activities

[20] As our *Access Controls* audit report states, staff must be trained on policies and procedures in order to understand both how they apply in their role and the consequences of non-compliance. This is particularly important for the protection of privacy. Further, one-time privacy training efforts are not enough. The RNC has committed to continuing formal privacy training, at least every two years, as well as to frequent ongoing messaging and reminders about privacy issues. We are satisfied that this is a reasonable approach.

Restrictions on Operational Access and Auditing

[21] Our *Access Controls* audit report deals at length with this issue. We recognize that in organizations like the RNC it is necessary for a great many employees to have full access to the information databases, such as ICAN, Motor Vehicle Registry (MVR) and the national Canadian Police Information Centre (CPIC) in order to do their work. Without repeating the findings of our audit report at length, we note that the RNC has agreed that it will implement periodic reviews of users' access, to determine suitability of access based on need and on changing job requirements.

[22] In particular, the RNC agrees that it needs to upgrade the user access audit process, for example to add automated functions that can detect abnormal use patterns. Auditing user access at present is a manual and very labour-intensive process. While more robust audit processes are by no means a complete answer to inappropriate employee access, more frequent audits are a greater deterrent to snooping. This upgrading process has already begun.

[23] We are also satisfied that RNC employees cannot anonymously add information to files on citizens, as every addition to the files carries a user stamp.

Gaps in the Process

[24] Initially we had concerns that the records of the disciplinary hearings and court proceedings exposed potential gaps in oversight. For example, it was not clear whether it is possible for another employee to use an unattended computer to access a database. We are

satisfied that while it may be technically possible, the likelihood of that scenario being a significant problem is remote.

[25] However, it is still the case that RNC employees may receive requests for information searches not only in writing, such as via email, but also by telephone or in face to face conversations with officers. These requests need to be logged in some way, in order for the RNC to be able to later confirm that there was a genuine operational justification for accessing a file. That would eliminate the possibility that a snooping employee could assert that the questionable access had been legitimately done in response to a verbal request. That one additional, system-wide measure could be a strong deterrent against improper access.

Culture of Privacy

[26] Historically there have been criticisms that there was not a sufficiently strong culture of privacy in the RNC organization. The RNC is certainly not unique in this regard – the same criticisms have been (and sometimes still are) levelled at regional health authorities, municipalities and other public bodies.

[27] Establishing and maintaining a culture of privacy within an organization, and reaching a widespread, strong understanding of what privacy is, why it is needed and how it is to be achieved, is not easy. Appropriate policies and procedures, oversight and training are all essential. However, the most important requisite for change may be a strong understanding of privacy principles, and commitment to them, from senior management.

[28] The RNC believes, and we agree, that the RNC culture of privacy has improved with time. However, more work needs to be done. We would strongly encourage senior RNC management to actively take responsibility for leading the entire organization in that direction.

RNC Investigation Process

[29] As may be seen from the chronology of events, the RNC had not only completed the audit in response to the 2017 privacy complaint, but had also completed the disciplinary investigation, before the OIPC became involved in early 2018. In discussing the conduct of the investigation the RNC agreed that it needs to ensure that staff involved in conducting such

privacy-related investigations (such as human resources personnel) have received appropriate privacy training.

The Prosecution and its Outcomes

[30] As noted above, it was the decision of our Office to proceed with the prosecution of the two individuals involved. Initiating a prosecution is a serious matter, and that decision was only taken after providing the Crown with the documentary case files, and receiving in response an opinion that there was a reasonable likelihood of conviction. Thereafter the conduct of the prosecution rested not with the RNC or with our Office, but exclusively with the Crown.

[31] One of the individuals charged entered a guilty plea to the charges. The other was acquitted at trial. While we do not intend to comment further on the outcome of that trial, or to suggest that the court decision was wrong, we must note that the grievance arbitrator, who heard all of the evidence and the extensive submissions of both the employer and the union, upheld the finding of misconduct and the discipline imposed by the employer.

RECOMMENDATIONS

[32] Under the authority of section 76(2) of *ATIPPA, 2015*, I recommend that the Royal Newfoundland Constabulary:

1. continue to work to improve and strengthen the culture of privacy within the organization;
2. continue the process of updating and strengthening its privacy-related policies and procedures;
3. continue, and where possible strengthen, ongoing privacy training and privacy awareness measures;
4. continue to upgrade the user access audit process to provide more effective oversight and control;
5. implement a requirement that all access to all databases be supported by a logged operational request or authorization;

6. ensure that all staff involved in conducting such privacy-related investigations have received appropriate privacy training.

[33] As set out in section 78(1) of *ATIPPA, 2015*, the head of the Royal Newfoundland Constabulary 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.

[34] Dated at St. John's, in the Province of Newfoundland and Labrador, this 31st day of August, 2023.

Michael Harvey
Information and Privacy Commissioner
Newfoundland and Labrador