Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 123-2025[1]

Regina Police Service and Constable Clinton Duquette

December 11, 2025

Summary: An investigation conducted by the Regina Police Service (RPS) Professional Standards Branch revealed that a police officer repeatedly accessed the personal information of six individuals in its Integrated Electronic Information System (IEIS) without a legitimate need-to-know pre-requisite basis. This snooping occurred over a period of three years, three months and 15 days. The RPS notified the affected individuals and reported the matter to the Office of the Saskatchewan Information and Privacy Commissioner (OIPC).

The Commissioner found that: (1) privacy breaches occurred each time the police officer accessed each of the affected individuals' personal information in IEIS and that these breaches were intentional and wilful; (2) RPS took minimal steps in containing the privacy breach; (3) the RPS letter to the affected individuals was appropriate but it was not conveyed in a timely fashion; (4) the police officer wilfully and knowingly accessed personal information for personal reasons in contravention of *LA FOIP,* the privacy training they had received, the *Confidentiality Protocol* they had signed and the privacy disclaimer in IEIS; and (5) the disciplinary measures adopted by the RPS in this case are wholly inadequate and will not restore public faith in the RPS.

The Commissioner recommended:

(1) That RPS inform the remaining affected individuals of their right of access under section 5 of *LA FOIP* so they may choose to submit a formal access to information request to RPS for a summary of the dates and times the police officer searched their personal information.

(2) That the police officer's access to IEIS be permanently revoked.

[1] The other OIPC file numbers associated with this matter include: 152-2025; 207-2025 and 278-2025.

(3) Should RPS not revoke the police officer's access privileges to IEIS, then it is recommended that RPS conduct focused and targeted audits on the police officer's access to IEIS on a monthly basis for an indefinite period to ensure that: (i) the police officer is no longer accessing the personal information of the six affected individuals; and (ii) going forward, the police officer only accesses the personal information on IEIS on a need-to-know basis.

(4) That RPS install a feature into IEIS that requires RPS members to provide a reason with sufficient particularity when conducting queries. Such a feature will assist RPS in conducting audits to ensure lawful access of personal information in IEIS.

(5) That the RPS conduct random audits of queries by RPS members (sworn and civilian) of information databases that contain personal information. Audits should be conducted from random samples of a pool of RPS employees, rather than just random audits of RPS files.

(6) That RPS ensure its Access and Privacy Unit is sufficiently resourced to perform audits of access to IEIS and any other information databases that contain personal information, including CPIC and the SGI database.

(7) That RPS implement a protocol for conducting audits of an employee's access to personal information in cases where there is evidence that an employee has made an unauthorized access, or in cases where the RPS has reason to suspect the employee may have made unauthorized accesses to personal information.

(8) That RPS commit to a policy of zero tolerance for unauthorized breaches of personal information.

(9) That this matter be conveyed to the Attorney General of Saskatchewan for an opinion with respect to prosecution pursuant to section 56(2) of *LA FOIP*.

TABLE OF CONTENTS

I. BACKGROUND....4

II. DISCUSSION OF THE ISSUES....6
1. Jurisdiction....6

2. Did a privacy breach occur?....6
a. Is personal information involved in this matter?....6
b. Was there authority for the collection, use or disclosure of personal information?....8

3. Did RPS respond appropriately to the privacy breach?....9
a. Containment of the Breach....9
b. Notification of Affected Individuals....10
c. Investigation of the Breach....12
i. Privacy Training....13
ii. Confidentiality Protocol....16
iii. IEIS Privacy Disclaimer....17
iv. Audits....18

d. Prevention of Future Breaches....18
i. Revoking/Terminating Access....19
ii. Audits....20
iii. Recording Reasons for IEIS Queries....20
iv. RPS Audit Program....22
v. Disciplinary Protocol....23

III. FINDINGS....24

IV. RECOMMENDATIONS....25

I. BACKGROUND

[1] An investigation by the Regina Police Service (RPS) Professional Standards Branch into an unrelated matter revealed that a police officer accessed the personal information of six individuals on multiple occasions in the RPS Integrated Electronic Information System (IEIS) from October 2021 to June 2024. This snooping was conducted without a legitimate need-to-know pre-requisite basis. The police officer accessed the personal information of:

- **Affected Individual 1** on 9 separate dates for a total of 25 unauthorized searches from October 7, 2021 to November 29, 2023.
- **Affected Individual 2** on 17 separate dates for a total of 19 unauthorized searches from December 20, 2021 to June 7, 2024.
- **Affected Individual 3** on 2 separate dates for a total of 2 unauthorized searches on May 11, 2022 and June 8, 2022.
- **Affected Individual 4** on 6 separate dates for a total of 6 unauthorized searches from May 23, 2022 to July 13, 2023.
- **Affected Individual 5** on 3 separate dates for a total of 3 unauthorized searches from July 23, 2022 to August 31, 2022.
- **Affected Individual 6** on 7 separate dates for a total of 12 unauthorized searches from March 22, 2023 to June 22, 2024.

[2] Over a period of three years, three months and 15 days, the police officer inappropriately accessed the personal information of six citizens of the City of Regina 67 times in the IEIS police database. The affected individuals included a former partner of the police officer, the former partner's sibling, and the former partner's previous partner along with other individuals. RPS submitted that the police officer effected the unauthorized searches for "personal reasons".

[3] On March 5, 2025, the RPS Professional Standards Branch reported this matter to the RPS Access and Privacy Unit. RPS indicated that the notification of affected individuals was postponed until the conclusion of the Professional Standards Branch investigation into the actions of the police officer.

[4] On June 3, 2025, RPS notified four of the six affected individuals of the privacy breach by telephone. RPS was unable to reach the remaining two.

[5] On June 5, 2025, RPS notified the Office of the Saskatchewan Information and Privacy Commissioner (OIPC) of the privacy breach.

[6] RPS sent notification letters dated June 5, 2025, to the four affected individuals it was able to contact by telephone. The RPS letter contained the details of the breach and included a description of the personal information accessed by the police officer. The letter also listed details of the RPS investigation and findings as well as an apology. RPS sent letters to the two outstanding affected individuals asking them to contact RPS.

[7] On June 9, 2025, one of the two individuals contacted RPS and provided updated contact information. RPS was then able to send a letter to the individual on that same day with details of the breach, details of the RPS investigation/findings and an apology.

[8] On June 16, 2025, one of the affected individuals, Complainant 1, requested an OIPC investigation.

[9] On June 23, 2025, the final outstanding affected party contacted RPS and provided updated contact information. The following day, RPS sent a letter to this individual with details of the breach, details of the RPS investigation/findings and an apology.

[10] On August 11, 2025, OIPC notified RPS and Complainant 1 that an investigation was commenced.

[11] On August 21, 2025, another affected individual, Complainant 2, contacted this office and requested an investigation. That same day, OIPC notified Complainant 2 that an investigation had been commenced.

[12] On September 18, 2025, RPS provided its submission to OIPC.

II. DISCUSSION OF THE ISSUES

1. Jurisdiction

[13] RPS qualifies as a "local authority" pursuant to section 2(1)(f)(viii.1) of *The Local Authority Freedom of Information and Protection of Privacy Act*[2] (*LA FOIP*). OIPC has jurisdiction and as outlined in the notice to RPS, is conducting this investigation pursuant to section 32 of *LA FOIP*.

2. Did a privacy breach occur?

[14] A privacy breach occurs when a local authority collects, uses and/or discloses personal information without the authority of *LA FOIP*. The first step in determining if a privacy breach has occurred is to identify if personal information is involved. If so, then the second step is to determine whether the personal information was collected, used and/or disclosed in a way that was not authorized by *LA FOIP*.

a. Is personal information involved in this matter?

[15] Personal information is defined at section 23(1) of *LA FOIP*, though the list is not exhaustive. Personal information is information about an identifiable individual, that is personal in nature.[3]

[16] The police officer accessed the personal profiles of six affected individuals in IEIS on a repeated basis. The files in IEIS consist of internal police files related to RPS investigations and police occurrences. The letters sent by RPS to the affected individuals explained that the police officer accessed and/or viewed the following types of personal information with respect to each affected individual:

[2] *The Local Authority Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. L-27.1, as amended.

[3] See OIPC Investigation Report 253-2024, 033-2025 at paragraph [14].

- full names;
- dates of birth;
- fingerprint serial numbers;
- physical descriptions;
- the role the affected individual played in an investigation, either as a complainant, witness, victim, suspect, reporter; and/or
- whether the affected individual was ever charged in relation to a particular occurrence.

[17] Without a doubt, this type of information qualifies as "personal information" pursuant to the definitions contained in section 23(1)(a), (b), (d), (e) and (k)(i) of *LA FOIP*:

> **23**(1) Subject to subsections (1.1) and (2), **"personal information"** means personal information about an identifiable individual that is recorded in any form, and includes:
>
> (a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;
>
> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
>
> ...
> (d) any identifying number, symbol or other particular assigned to the individual;
>
> (e) the home or business address, home or business telephone number, fingerprints or blood type of the individual;
>
> ...
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual;

b. Was there authority for the collection, use or disclosure of personal information?

[18] *LA FOIP* does not define the terms "collection, "use," or "disclosure". This office has found the following definitions helpful:[4]

- "Collection" can mean the bringing together, assembling, accumulating, or obtaining personal information from any source by any means.
- "Use" indicates the internal use of personal information by a local authority and may include the sharing of the personal information in such a way that it remains under the control of the local authority.
- "Disclosure" is the sharing of personal information with a separate entity, not a division or branch of the local authority that has possession or control of that information.

[19] The unauthorized access of the affected individual's personal information stored in IEIS constitutes a "use" of the personal information. A local authority must only use personal information in accordance with section 27 of *LA FOIP*, on a "need to know" basis. Section 27 of *LA FOIP* provides:

> **27** No local authority shall use personal information under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, except:
>
> (a) for the purpose for which the information was obtained or compiled, or for a use that is consistent with that purpose; or
>
> (b) for a purpose for which the information may be disclosed to the local authority pursuant to subsection 28(2).

[20] The "need-to-know" principle provides that information should only be available to those in an organization who need to know it for purposes related to their immediate duties.[5] In its submission to this office, RPS advised that the police officer accessed the personal information of the six affected individuals without their consent "and used the information for personal gain". RPS explained that the police officer was aware these searches were

[4] See OIPC Investigation Report 279-2024 at paragraphs [25] to [27].

[5] See OIPC Investigation Report 032-2024, 097-2024 at paragraph [16].

privacy breaches and that they were wrong but continued to access the affected individuals' personal information. As such, the police officer's accesses to the personal information was not authorized by section 27 of *LA FOIP*. There is a finding that privacy breach occurred each time the police officer accessed each of the affected individuals' personal information in IEIS and that these breaches were intentional and wilful.

3. Did RPS respond appropriately to the privacy breach?

[21] The determination of a local authority's response to a privacy breach involves several considerations. Whether the local authority responds appropriately to a privacy breach is informed by sections 6-7 of OIPC *Rules of Procedure*. The following considerations include:

a. Was the breach contained;

b. Were the affected individuals notified;

c. Was the breach investigated; and

d. Were appropriate steps taken to prevent future breaches.

a. Containment of the Breach

[22] Local authorities should take immediate steps to contain a breach immediately upon learning of the breach. The steps adopted will depend entirely upon the nature of the breach, but may include:[6]

- Stopping the unauthorized practice.
- Recovering the records.
- Shutting down the system that was breached.
- Revoking access to personal information.
- Correcting weaknesses in physical security.

[6] *Supra,* footnote 2 at paragraph [22].

[23] OIPC applies a standard of reasonableness in the assessment of breach containment. The local authority must demonstrate that it has reduced the magnitude of the breach and the resulting risk to affected individuals. This measure reassures the public and, most of all, the affected individuals.[7]

[24] A privacy breach is a very serious matter and can have dire consequences to any organization. A privacy breach always results in a loss of faith and trust on the part of the public, and a loss of faith and trust on the part of the individuals the institution serves. This privacy breach is extremely serious because the primary goal of a police force is to ensure public safety.[8] The misuse of a police information system for the personal reasons of a staff member seriously undermines not just the trust of the affected individuals but the public as a whole. This privacy breach is highly concerning.

[25] In its submission, RPS indicated that it did not revoke the police officer's access to IEIS because the police officer was allowed to continue to work as a police officer and required access to IEIS. RPS noted that the police officer confirmed they had not made copies or removed personal information from the IEIS database. RPS reviewed its audit logs and confirmed that no print commands were ever issued when the police officer accessed the affected individuals' personal information.

[26] There is a finding that RPS took minimal steps in containing the privacy breach.

b. Notification of Affected Individuals

[27] Best practice for local authorities involves informing affected individuals as soon as possible that their personal information has been breached. This is an obvious and crucial

[7] See OIPC Investigation Report 197-2022, 215-2022 at paragraph [19].

[8] The RPS vision statement is "Working together to keep Regina safe". RPS elaborates on this statement by stating that its primary goal is to ensure public safety: https://www.reginapolice.ca/our-mission/.

step that invokes the principles of fairness. Affected individuals must be informed of the possible risks so they can take any remedial steps deemed necessary for self-protection.

[28] The information that a local authority should include in a notice to affected individuals should include:

- A description of the breach (a general description of what happened).
- A detailed description of the personal information involved (e.g., name, credit card numbers, medical records, financial information, etc.).
- A description of possible types of harm that may result from the privacy breach.
- Steps taken and planned to mitigate the harm and to prevent future breaches.
- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g., how to contact credit reporting agencies).
- Contact information of an individual within your organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to OIPC (provide contact information).
- Recognition of the impacts of the breach on affected individuals and an apology.

[29] As noted in the factual recitation of this Investigation Report, the RPS Professional Standards Branch reported this matter to the RPS Access and Privacy Unit on March 5, 2025. It was not until June of 2025 that RPS contacted the affected individuals by telephone and sent them letters that included the following:

- Details of the breach including a description of the personal information involved.
- A notification that the police officer had been disciplined and that, as part of the discipline, they were required to take additional privacy training and will be subject to random audits for a period of two years.

- An apology.
- Contact information of the RPS Manager of Access and Privacy.
- Contact information for OIPC.

[30] There will be a finding that the RPS letter to the affected individuals was appropriate but it was not conveyed in a timely fashion. The fact it took RPS three months to notify the affected individuals is concerning. We understand that RPS required time to investigate the matter to have sufficient details with which to inform the affected individuals. Still, notification of affected individuals in a privacy breach should be given immediate priority given that a snooper may use the personal information for questionable purposes. It is obvious that individuals whose personal information has been breached are extremely vulnerable especially when the breach involves facts of this nature.

[31] We note that one of the affected individuals requested follow up information from RPS including the dates and times the police officer searched their personal information. RPS provided the individual with a table that squarely addressed the request. There will be a recommendation that RPS inform the remaining affected individuals of their right of access under section 5 of *LA FOIP* so they may choose to submit a formal access to information request to RPS and obtain a summary of the dates and times the police officer searched their personal information.

c. Investigation of the Breach

[32] Once the local authority has contained the privacy breach and sent appropriate notification to the affected individuals, an investigation should be conducted. The investigation must address the incident on a systemic basis and include a root cause analysis and conclusion. The institution must consider its duty to protect personal information as set out at section 23.1 of *LA FOIP*. Specifically, section 23.1 of *LA FOIP* requires that local authorities establish policies and procedures to maintain administrative, technical and physical safeguards:

> **23.1** Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> (ii) loss of the personal information in its possession or under its control; or
>
> (iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[33] In determining the root cause of a privacy breach, the local authority must identify shortcomings in existing safeguards and formulate safeguards that could prevent future privacy breaches. Safeguards can be administrative (e.g., policies, procedures, confidentiality statements on contracts), technical (e.g., access controls on electronic storage) or physical safeguards (e.g., locked cabinets or bins, locked doors, security cameras).[9]

[34] Commendably, RPS had several administrative safeguards in place to prevent this type of unauthorized access. This police officer bypassed every single safeguard to snoop upon the six affected individuals over a period of just over three years.

i. Privacy Training

[35] RPS indicated in its submission to this office that the police officer received focussed privacy training in 2017, 2018 and 2019. RPS provided the training materials used in each of the training sessions. Below are summaries of the more salient concepts that were

[9] *Supra,* footnote 2 at paragraph [41].

emphasized over the years. We note this training provides an excellent background for police officers in the privacy laws of this province:

2017 Privacy Training:

- A privacy breach occurs when personal information is used for reasons that are not consistent with the purposes for which it was collected;

- A privacy breach occurs when personal information is disclosed without authorization, when it is lost or destroyed, when it is accessed by an employee of the RPS without a need-to-know basis, and when it is shared with an unauthorized agency;

- Section 56 of *LA FOIP* (2017) was discussed:

  > **s. 56** Every person who knowingly collects, uses or discloses personal information in contravention of the Act or regulations is guilty of an offence and liable on summary conviction to a fine of not more than $1,000, to imprisonment for not more than one year or to both.

- Internal police investigations for breach will result in internal discipline up to and including dismissal, similar to any other policy or legislation breach where it is proven that the breach was wilful or committed knowingly.

2018 Privacy Training:

Breach and Breach Response

- A privacy breach is the unauthorized access to, loss or modification of personal information;

- A privacy breach can be accidental or intentional;

- In the event of a privacy breach the proper response is to contain the breach, evaluate and report. If personal information is lost or if there is an accidental breach of personal privacy, a report must be made immediately to the immediate supervisor;

Access and Use

- Access and use personal information for RPS business purposes only;

- Access does not equal the right to use personal information for non-authorized purposes.

In the Event of Non-Compliance

- Collecting, using or disclosing personal information for non-police business is a wilful violation of LA FOIP and has the following consequences: (1) Penalties – fine of up to $50,000 and/or 1 year in jail; (2) Discipline by RPS which can range from a warning to dismissal.

- Non-compliance could lead to far reaching and highly damaging consequences for the RPS. Any loss of integrity of the RPS perceived by the public will lessen the effectiveness of the Service.

2019 Privacy Training:

Privacy Breaches

- The various forms of privacy breaches include: over-collection of information; unauthorized use or disclosure; inaccuracy;

- If there is a breach, contain/stop it and notify your supervisor and Access/Privacy Officer of the RPS immediately;

- There may be a penalty that can range from criminal charges to a $50,000 fine or imprisonment;

Reminders

- Protect personal information;

- Don't discuss personal information with others who do not have the "need to know" basis;

- Your opinion about someone else in a police report becomes their personal information;

- Access personal information for business reasons only;

- Lock your computer when not in use.

[36] This police officer received excellent and ongoing privacy training that advised of the "need to know" principle and the serious consequences of non-compliance. Still the police officer knowingly and wilfully chose to use the IEIS database for their own personal purposes, repeatedly, over a period of just over three years.

[37] This office provided notice to the police officer and offered an opportunity to provide a submission. The police officer refused and was content for the RPS to speak on their behalf. The privacy officer at RPS provided a reason for the unauthorized privacy breaches over the course of the three years. We will not go into detail but it was obvious that the personal reason was not in any way connected to the police officer's employment and the 67 unauthorized privacy breaches did not spring from a need-to-know.

ii. Confidentiality Protocol

[38] This police officer also signed a "Confidentiality Protocol" on December 21, 2021. The Confidentiality Protocol that was signed provided as follows:

> **Confidentiality Protocol**
>
> The confidentiality of personal information is a key concern of the Regina Police Service (RPS) and accordingly the RPS has policies, procedures and practices in place to protect the confidentiality of the personal information of the public and its employees. I understand that in order to emphasize the importance of the protection of confidentiality, the RPS requires employees to sign a confidentiality pledge. Therefore, based on the above, I the undersigned agree as follows:
>
> (a) That I will only collect personal information on a need-to-know basis for the purpose of performing services on behalf of the RPS;
>
> (b) That I will only access, use or disclose personal information in the custody or control of the RPS for the purpose for which it was collected, or for a use that is consistent with that purpose; with the consent of the individual; or for another purpose when access, use or disclosure is authorized by *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP).
>
> (c) That I will keep all personal information in my possession in the strictest of confidence and take appropriate steps to protect the integrity, accuracy and privacy of personal information.
>
> (d) That upon no longer requiring the personal information for the purposes of providing services on behalf of the RPS, I will return or destroy all copies of the personal information in my possession in accordance with RPS policies and procedures.

> (e) That I will only collect, access, use or disclose RPS employee personal information on a need-to-know basis for work purposes, unless I have the informed consent of the employee.
>
> (f) For LA FOIP requests, that I will keep the applicant's identity confidential and only disclose this information on a need-to-know basis to clarify or complete the request.
>
> (g) That I will comply with LA FOIP and all RPS policies, procedures and practices applicable to the management, handling and security of personal information.
>
> I acknowledge that I have read this Confidentiality Protocol and understand that a breach of it may be in contravention of LA FOIP, other applicable laws and/or RPS policies and as such I may be subject to discipline up to and including dismissal.
>
> [Emphasis added]

[39] In spite of signing and acknowledging the Confidentiality Protocol, this police officer continued to access the IEIS database in an unauthorized fashion and repeatedly, over a three year period.

iii. IEIS Privacy Disclaimer

[40] When a user signs into the IEIS electronic database, a "privacy disclaimer" immediately appears:

> Users must not access, use or disclose RPS information for any reason other than approved business or lawful purposes in accordance with RPS policy and The Local Authority Freedom of Information and Protection of Privacy Act (LA FOIP). Access for personal use is prohibited.
>
> [Emphasis added]

[41] Despite being informed that they were to only access personal information on a need-to-know basis in connection with a work purpose, this police officer ignored the privacy disclaimer in IEIS and accessed the personal information of the six affected individuals. In its submission, RPS conceded the police officer "was aware that [their] actions were wrong,

but continued to access information on the individuals…. Accessing their information habitually over an extended period."

[42] There will be a finding that the police officer wilfully and knowingly accessed personal information for personal reasons in contravention of *LA FOIP*, the privacy training they had received, the Confidentiality Protocol they had signed, and the privacy disclaimer in IEIS. Wilful violation was the root cause of the privacy breach.

iv. Audits

[43] In May 2023, RPS implemented an audit program designed especially for the IEIS database. The program randomly audits 30 occurrence files on a monthly basis. The 30 files are from the previous month. Two random files publicized in media releases are also audited. The purpose of the audit program is to ensure RPS staff are accessing IEIS for business reasons only. Since the program commenced in May of 2023, the first audits could only examine compliance back to April of 2023. Understandably, this matter was not discovered by means of the audit program. Rather, the RPS detected the snooping when the internal Professional Standards Branch conducted an investigation with respect to this police officer on an unrelated matter.

[44] When the police officer's snooping came to light, the RPS Professional Standards Branch completed an audit of accesses by the police officer of the Canadian Police Information Centre (CPIC). RPS also indicated it "checked" the Saskatchewan Government Insurance's (SGI) database and confirmed there was no unauthorized access. RPS reported to this office that no inappropriate or unauthorized access on the part of this police officer occurred as the result of these two external audits.

d. Prevention of Future Breaches

[45] A police organization should ensure that its internal culture commits to the vigorous protection of the personal information of those they serve. Both the public interest and the law demand such a commitment from a police force. On March 12, 2025, the RPS

announced that Robert Eric Semenchuck, was charged with one count of "breach of trust by a public officer",[10] and one count of "unauthorized use of a computer",[11] as a result of an investigation by RPS.[12] Semenchuck held the position of Sergeant with the Regina Police Service during the material time and he resigned in April of this year. He pled guilty to the two charges in the Provincial Court of Saskatchewan on November 21, 2025 and will be sentenced on January 23, 2026. The facts as read out in court revealed that Semenchuck used police databases to pursue personal and intimate relations with dozens of Regina women over a period that spanned almost 15 years. This matter stands as an unfortunate backdrop for the confirmed breach of the privacy laws by another member of the RPS although the RPS was not clear with this office on the motives of the officer in this case.

[46] RPS must prioritize implementing measures to ensure it stamps out any possibility of normalized snooping amongst its employees. Prevention is key in assisting a restoration of lost public trust.

[47] Possible prevention measures include adding/enhancing safeguards already in place, providing additional training, and the regular monitoring/auditing of systems and system users.[13] We specifically address some obvious methods of prevention below.

i. Revoking/Terminating Access

[48] As we have noted above, the police officer in this Investigation Report continues to be employed as an active police officer and they continue to enjoy access privileges to the internal IEIS database. RPS explained that the police officer was "going through some personal issues during the time period which led [them] to making poor decisions." Making

[10] Contrary to section 122 of the *Criminal Code,* RSC 1985, c. C-46, as amended.

[11] Contrary to section 342.1(1)(a) of the *Criminal Code.*

[12] See RPS "News" webpage, *Police Member Charged: Breach of Trust & Unauthorized Use of Computer*. March 12, 2025. The matter was brought forward by a member of the public.

[13] *Supra,* footnote 2 at paragraph [50].

poor decisions for three years, three months and 15 days and deliberately bypassing every safeguard in place should lead to a conclusion that future access could be risky and highly questionable. There will be a recommendation that the police officer's access to IEIS be permanently revoked.

ii. Audits

[49] As part of the internal discipline program prescribed for this police officer, the RPS intends to randomly audit the police officer's accesses to IEIS for a period of 2 years. Two years of random audits is simply insufficient in light of the admitted facts of this case. First, proactive random audits stand as a technical safeguard undertaken by organizations in detecting and deterring privacy breaches.[14] Once a local authority has detected and confirmed unauthorized snooping, and once the decision has been made to allow the snooper to continue in the employment of the local authority, then focused and targeted audits on the snooper should be ongoing and indefinite. Should the RPS not revoke the police officer's access privileges to IEIS, there will be a recommendation that RPS conduct focused and targeted audits of this police officer's access to IEIS on a monthly basis and for an indefinite period to ensure that: (i) the police officer is no longer accessing the personal information of the six affected individuals; and (ii) the police officer is only accessing personal information on a need-to-know basis.

iii. Recording Reasons for IEIS Queries

[50] RPS informed that IEIS is not designed to require or record the reason for access when a query is entered. Surprisingly, RPS warranted that IEIS tracks "every key stroke, every file opened and person accessed." If this is the case, a reason for access is only a logical follow-up.

[51] In 2010, the Office of the Alberta Information and Privacy Commissioner (AB OIPC) investigated whether the Edmonton Police Service (EPS) had reasonable safeguards in

[14] See OIPC Investigation Report 088-2022 at paragraph [48].

place for its internal information system at the time.[15] The AB OIPC found that without a reason for access, it was impossible for EPS to demonstrate that a query into EPROS was for an authorized purposes:

> [para 90] However, this case has placed into high relief the inadequacies in the system that existed at the time the queries were done, both in terms of the understanding of the EPS members as to the appropriate limitations on use of the names of individuals to run police database queries, as well as in terms of the failure of the system in not requiring the reasons for queries to be recorded.
>
> ...
> [para 92] As well, the absence of any requirement to indicate reasons or any ability to do so on the computerized information system has made it impossible for the EPS to conclusively demonstrate an authorized purpose for a large proportion of the queries that have been questioned, both in this case and in relation to other persons. While this office has thus far allowed some leeway by permitting testimony of members as to their general but invariable practices to substitute for demonstrated reasons, what has been revealed in this case makes it clear that the absence of reasons was a severe shortcoming that required a remedy.
>
> [Emphasis added]

[52] EPS implemented a mandatory requirement in its internal information system, EPROS, that required querants to record their reasons with sufficient particularity (such as recording occurrence numbers).[16] AB OIPC explained that the requirement for entering a reason could serve to dissuade inappropriate queries as well as serve as direct evidence in the event of a later audit of the reasons for queries as opposed to conjecture.[17]

[53] There will be a recommendation that RPS install a feature that requires RPS members to provide a reason with sufficient particularity when conducting queries. Such a feature will assist RPS in conducting audits to ensure lawful access of personal information in IEIS.

---

[15] See AB OIPC ORDER F2006-033, Edmonton Police Service (October 13, 2010) at [para 90] and [para 92].

[16] *Ibid,* at [para 96].

[17] See AB OIPC Order F2012-28, Edmonton Police Service, (November 30, 2012) at [para 63].

iv. RPS Audit Program

[54] As described earlier in this Investigation Report, since May of 2023 RPS has been conducting monthly random audits of 30 occurrence files from the previous month as well as two random files from the RPS media release page.

[55] Other police forces across Canada randomly audit their members with access to internal databases containing personal information. The Royal Newfoundland Constabulary (RNC), conducts audits of random samples of search history of every staff member to verify each staff member has accessed files on its systems for legitimate purposes. The Newfoundland and Labrador Office of the Information and Privacy Commissioner (NFLD OIPC) described the RNC audit program in the following way:[18]

> The RNC have a dedicated position to oversee the audit program and all staff with access to these systems are subject to at least one audit each calendar year. On a random basis, the audit manager selects samples from an employee's search history and verifies that the employee's search and corresponding file access was for a legitimate RNC business purpose. If supporting documentation cannot be found, the audit manager provides a standardized audit form to the employee's direct supervisor, who follows-up with the employee. Details are added to the form based on this follow-up and the form is then signed, with a copy retained by the supervisor and a copy returned to the audit manager. Even if no issues are found, the employee is notified that the audit occurred and reminded of pertinent policies.

[56] This office is satisfied that the RPS conducted adequate audits to determine the scope of the unauthorized access to personal information accessed by this police officer. We recognize that conducting audits requires time and labour. Nonetheless, there will surely be a loss of public faith in the RPS in the event of future privacy breaches of this nature. There will be a recommendation that RPS conduct random audits of queries by RPS members (sworn and civilian) of information databases that contain personal information. Audits should be conducted from random samples of RPS employees, rather than random audits of RPS files. There will also be a recommendation that RPS ensure the Access and Privacy Unit is sufficiently resourced to perform audits of access requests to IEIS and any

[18] See NFLD OIPC, *Access Controls: Royal Newfoundland Constabulary.* January 13, 2023.

other information databases that contain personal information, including CPIC and the SGI database. Finally, there will be a recommendation that RPS implement a protocol for conducting audits of an employee's access to personal information in cases where there is evidence that an employee has made an unauthorized access, or in cases where the RPS has reason to suspect the employee may have made unauthorized accesses to personal information.[19]

v. Disciplinary Protocol

[57] The RPS reported on the results of the internal disciplinary process with respect to this police officer in connection with this matter. It was revealed that the police officer was subjected to a remedial penalty that involved one day without pay, the re-taking of a one-hour privacy training course and the re-signing of the RPS Confidentiality Protocol. As noted, this police officer will be subject to random audits of the IEIS database for a period of two years.

[58] With respect, given the scope and breadth of the privacy breach in this case, the three-year timespan of the breach and the concession that the privacy breach was wilful and undertaken with full knowledge of the violation of *LA FOIP* – the disciplinary measures adopted by the RPS in this case are wholly inadequate and cannot restore public faith in the RPS.

[59] RPS must commit to a culture that reflects zero tolerance for inappropriate access of personal information. The RPS should consider severe consequences when violations are deliberate as in this case.[20] The public deserves to know that the RPS guards their privacy and protects their safety – the two concepts go hand in hand.

---

[19] See Ontario IPC, Privacy Complaint Report MC19-00058 and MC19-00059, (September 16, 2022) at paragraphs [35] to [40].

[20] Two employees of the Moose Jaw Police Service were terminated for snooping into internal police information systems (See OIPC Investigation Report 265-2018, 266-2018). Two civilian employees of the RNC faced a one-month unpaid suspension and a two-month unpaid suspension for snooping in RNC's databases (See NFLD OIPC Report P-2023-002). In *Mamak v. Ottawa Police Service*, 2011 ONCPC 4, a police officer faced the penalty of resignation within seven days

[60] There will be a recommendation that RPS commit to a policy of zero tolerance for unauthorized breaches of personal information.

[61] In conclusion, because of the public interest aspect of this privacy breach, we feel it necessary to name the individual at the heart of this privacy breach. This office administers the privacy laws of this province and our main duty is to the people of Saskatchewan. The privacy violation in this case continued for a considerable period of time, the police officer wilfully overrode the privacy safeguards put in place by the employer, in spite of considerable privacy training. The scope and breadth of the privacy breach is concerning. The police officer is Constable Clinton Duquette.[21]

[62] There are several factors that must be considered when recommending a prosecution of a matter of this nature. Those factors include: (1) overall strength of the case; (2) public interest in a prosecution; (3) harm to the community as a result of the privacy breach; (4) number of complainants from the community; and (5) available litigation resources.

[63] We find that every factor listed above can be adequately addressed by the factual matrix of this case. There will be a recommendation that this matter be conveyed to the Attorney General of Saskatchewan for an opinion with respect to prosecution pursuant to section 56(2) of *LA FOIP*.

III. FINDINGS

[64] OIPC has jurisdiction and this investigation is conducted pursuant to section 32 of *LA FOIP*.

---

or summary dismissal for the improper use of CPIC. This was categorized as "wilful acts of disobedience". The appellate panel upheld the conviction and penalty imposed.

[21] See *Stebner v Information and Privacy Commissioner Saskatchewan*, 2019 SKQB 91 on the inherent right of this office to publish the name of an individual who has been found to wilfully violate the privacy laws in Saskatchewan through a privacy breach (at paragraph 172). In this case, Justice Danyliuk dismissed an application for injunctive relief (paragraphs 166 to 167), and dismissed an application for a publication ban at paragraphs (171 to 176).

[65] Privacy breaches occurred each time the police officer accessed each of the affected individuals' personal information in IEIS and these breaches were intentional and wilful.

[66] RPS took minimal steps in containing the privacy breach.

[67] The RPS letter to the affected individuals was appropriate but it was not conveyed in a timely fashion.

[68] The police officer wilfully and knowingly accessed personal information for personal reasons in contravention of *LA FOIP*, the privacy training they had received, the *Confidentiality Protocol* they had signed, and the privacy disclaimer in IEIS.

[69] The disciplinary measures adopted by RPS in this case are wholly inadequate and will not restore public faith in the RPS.

IV. RECOMMENDATIONS

[70] My recommendations are as follows:

> (1) That RPS inform the remaining affected individuals of their right of access under section 5 of *LA FOIP* so they may choose to submit a formal access to information request to RPS for a summary of the dates and times the police officer searched their personal information.
>
> (2) That the police officer's access to IEIS be permanently revoked.
>
> (3) Should RPS not revoke the police officer's access privileges to IEIS, then it is recommended that RPS conduct focused and targeted audits on the police officer's access to IEIS on a monthly basis for an indefinite period to ensure that: (i) the police officer is no longer accessing the personal information of the six affected individuals; and (ii) going forward, the police officer only accesses the personal information on IEIS on a need-to-know basis.
>
> (4) That RPS install a feature into IEIS that requires RPS members to provide a reason with sufficient particularity when conducting queries. Such a feature will assist RPS in conducting audits to ensure lawful access of personal information in IEIS.

(5) That the RPS conduct random audits of queries by RPS members (sworn and civilian) of information databases that contain personal information. Audits should be conducted from random samples of a pool of RPS employees, rather than just random audits of RPS files.

(6) That RPS ensure its Access and Privacy Unit is sufficiently resourced to perform audits of access to IEIS and any other information databases that contain personal information, including CPIC and the SGI database.

(7) That RPS implement a protocol for conducting audits of an employee's access to personal information in cases where there is evidence that an employee has made an unauthorized access, or in cases where the RPS has reason to suspect the employee may have made unauthorized accesses to personal information.

(8) That RPS commit to a policy of zero tolerance for unauthorized breaches of personal information.

(9) That this matter be conveyed to the Attorney General of Saskatchewan for an opinion with respect to prosecution pursuant to section 56(2) of *LA FOIP*.

Dated at Regina, in the Province of Saskatchewan, this 11th day of December, 2025.

Grace Hession David
Saskatchewan Information and Privacy Commissioner