Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINTS MC19-00058 and MC19-00059

Toronto Police Services Board

September 16, 2022

Summary: The Toronto Police Services Board (the police or the TPS) was notified that a TPS employee may have inappropriately accessed the complainants' personal information from a police database. The TPS investigated and found that the TPS employee accessed and disclosed the complainants' personal information to another TPS employee in violation of the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*).

In this report, I find that the TPS employee conducted database searches of the complainants' personal information without authorization, and verbally disclosed their personal information to another TPS employee contrary to the *Act*. I conclude that the TPS does not have reasonable measures in place to protect personal information in its database, as required by section 3(1) of Regulation 823 to the *Act*. I recommend improvements to the TPS verification and auditing protocols. I also recommend improvements to its privacy guidance documents, and privacy training program. In addition, I recommend notifying additional parties whose privacy was breached and who the TPS identified during this investigation.

Statutes Considered: *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O 1990, c. M.56; R.R.O. 1990, Reg. 823.

Orders and Investigation Reports Considered: Order PO-2913; Privacy Complaint Reports PC11-34 and PR16-40

OVERVIEW:

[1] The Office of the Information and Privacy Commissioner of Ontario (the IPC)

received privacy complaints from two individuals (the complainants) concerning the Toronto Police Services Board (the police or TPS).

[2] The complainants were tenants of a main floor suite in a residential building. The basement suite of the same building was occupied by two TPS employees, one of whom is the employee at the centre of this complaint (the Employee).

[3] The complainants state that when they were living in the same building, the Employee told them that she had previously ran database searches on another neighbour. The complainants reported this to their local police service (not the TPS). The TPS states that on November 6, 2018, the complainants contacted the TPS to complain about the Employee's conduct. The TPS then began an investigation of this complaint.

[4] Following this, on April 2, 2019, the TPS sent a letter to three affected parties it had identified at that time, which included the complainants. The letter informed them that a TPS employee (later identified as the Employee) had "conducted several unauthorized database queries on you and your associated vehicles." The letter stated that the Employee verbally provided the complainants' information to another TPS member (the Associated Officer), but that no printed records were created or distributed. The Associated Officer was later identified to the IPC as the other resident of the basement unit. The TPS stated that the Employee made the accesses for personal reasons unrelated to her duties.

[5] In later communications with the IPC, the TPS provided more information regarding the searches the Employee conducted. She ran searches using one of the complainants' names and date of birth, then using the license plate of a vehicle he drove. The Employee did not say how she knew his date of birth. The complainants suspected that this information came from their mutual landlord but TPS was not able to confirm this.

[6] The TPS was able to confirm that the Employee had disclosed to the Associated Officer both the fact that she conducted the database queries, and the information that she obtained resulting from the queries. They state that the Associated Officer assured them that he had not and would not disclose any personal information told to him by the Employee.

[7] The Employee later advised the TPS that she conducted these searches because she was "living at the same residence as the complainants and wanted to know of any criminal activities that would cause her concern."

[8] The TPS would not provide any details of the Employee's discipline, claiming "the nature of the discipline is a matter for the employer and is not public information." The Employee later resigned from the TPS, at which point the TPS terminated the conduct investigation.

ISSUES:

The following issues were identified in this investigation:

1. Is the information at issue "personal information" as defined by section 2(1) of the *Act*?

2. Was the use of personal information in accordance with section 31 of the *Act*?

3. Was the disclosure of personal information in accordance with section 32 of the *Act*?

4. Did the police have reasonable measures in place to prevent unauthorized access to the personal information of individuals, in accordance with section 3(1) of Regulation 823 to the *Act*?

DISCUSSION:

1. Is the information at issue "personal information" as defined by section 2(1) of the Act?

[9] "Personal information" is defined under section 2(1) of the *Act*, in part, as follows:

> "personal information" means recorded information about an identifiable individual, including,
>
> > (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
> >
> > (b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
> >
> > (c) any identifying number, symbol or other particular assigned to the individual,
> >
> > (d) the address, telephone number, fingerprints or blood type of the individual,

[10] The list of examples of personal information under section 2(1) is not exhaustive. Therefore, information that does not fall within the subparagraphs may still qualify as personal information.

[11] To qualify as personal information, the information must be about the individual in a personal capacity and it must be reasonable to expect that an individual may be identified if the information is disclosed.

[12] The TPS states that the Employee accessed the complainants' "names, dates of birth, addresses, address histories, driver's licence numbers, driver license histories, driving prohibitions, registered owner/vehicle information, release conditions for current charges, and list of convictions."

[13] The TPS, in its correspondence to the complainants, confirmed that the Employee disclosed personal information.

[14] I agree and find that the information described above is personal information as defined under section 2(1) of the *Act*.

2. Was the use of the personal information in accordance with section 31 of the Act?

[15] Section 31 of the *Act* states that an institution shall not use personal information in its custody or control unless the circumstances of the use fall within one of the exceptions set out in the *Act*.

[16] There is no evidence that the Employee's use of the complainants' personal information to perform the database searches, or her accesses to the personal information obtained from these searches, were authorized under the *Act*. The TPS has not made any claims that they were authorized, and described the searches as "unauthorized database queries." The TPS notes that the Employee herself stated that she performed these searches for personal reasons, rather than reasons related to her employment.

[17] Accordingly, I find that the Employee's use of the complainants' personal information was not in accordance with section 31 of the *Act*.

3. Was the disclosure of the personal information in accordance with section 32 of the Act?

[18] Section 32 of the *Act* states that an institution shall not disclose personal information in its custody or under its control, except in the circumstances set out in subsections (a) through (l).

[19] During its investigation, the TPS interviewed the other basement tenant, the Associated Officer. He confirmed that the Employee "'verbally' disclosed her unauthorized accesses and the resulting personal information of the complainants gleaned from these queries."

[20] As with the use of the personal information, the TPS has not claimed that the

Employee's disclosures of personal information were authorized under the *Act* and described these as unauthorized disclosures. There is no evidence that the verbal disclosure of personal information by the Employee was authorized under the *Act*.

[21] Based on the information provided to me, I find that the Employee's verbal communication of the complainants' personal information to the Associated Officer was a disclosure of personal information that was not in accordance with section 32 of the *Act*.

4. Were reasonable measures in place to prevent unauthorized access to and disclosure of the personal information, as required by section 3(1) of Regulation 823 under the Act?

[22] Establishing that the Employee both used and disclosed personal information contrary to the *Act* does not end the analysis. The TPS is subject to section 3(1) of Regulation 823 of the *Act*, which outlines the obligations institutions are under to ensure they have reasonable measures in place to prevent unauthorized access to their records. Section 3(1) of Regulation 823 states:

> Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

[23] Different institutions may meet this requirement in different ways, as noted by Investigator Lucy Costa (addressing the equivalent *Freedom of Information and Protection of Privacy* (*FIPPA*) regulation) in PR16-40:

> From the way this section of the regulation is written, it is clear that it does not prescribe a "one-size-fits-all" approach to security. It does not set out a list of measures that every institution must put in place regardless of circumstance. Instead, it requires institutions to have "reasonable" measures and ties those measures to the "nature" of the records to be protected. It follows that the same security measures may not be required of all institutions. Depending on the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them, the required measures may differ among institutions.[1]

[24] While each institution will determine the privacy and security measures necessary to protect the personal information under its custody or control, the IPC's "Privacy Breaches: Guidelines for Public Sector Organizations"[2] (the Privacy Breach Guidelines) provide a useful framework for determining whether the measures the TPS

[1] PR16-40 at paragraph 72.
[2] https://www.ipc.on.ca/wp-content/uploads/2019/09/privacy-breach-protocol-e.pdf

has in place meet its section 3(1) obligations. The guidance provided regarding how to investigate a breach and how to reduce the risk of future privacy breaches are especially helpful in this case. Beyond the need to make sure that any breaches are contained and the relevant parties notified, these guidelines also set out the need to review the policies and practices in place protecting personal information, together with the privacy training provided to staff, so that the institution can determine whether they need to make changes to improve these documents and processes. The guidelines also note the need to take corrective action to prevent similar breaches from occurring in the future.

[25] As part of my evaluation of the section 3(1) measures in place, I reviewed the TPS privacy policies and other guidance documents in place, as well as the privacy training provided to staff. I reviewed the policies and procedures that the TPS had in place, and the steps the TPS took to determine the scope of the breach, including its audits of accesses to personal information. I also addressed the TPS's failure to notify additional affected parties. Finally, I reviewed the role communication of disciplinary measures plays in remediating a breach, and the communication that the TPS provided in this instance.

Auditing of Accesses and other Containment Measures:

[26] Containment is one of the necessary steps for an institution to take in response to a privacy breach. This includes determining the personal information involved and ensuring that no personal information has been retained by an unauthorized recipient.[3]

[27] In this case, the keys to containing the breach were ensuring that there were no further disclosures of personal information (by the Employee or the Associated Officer), and determining the extent of the Employee's accesses.

Extent of Disclosures

[28] The Employee acknowledged telling the Associated Officer personal information. This officer later told the TPS that he had not disclosed this personal information to anyone else, and provided assurances that he would not reveal this information in future.

[29] In its correspondence to the one of the complainants, the TPS acknowledged an unauthorized disclosure by the Employee but stated that it was confined to a verbal telling, stating as follows:

> No printed records were ever created, nor distributed by the subject member. The information gleaned was verbally provided to another member of the TPS, with no further release or reiteration.

[3] Privacy Breaches: Guidelines for Public Sector Organizations, https://www.ipc.on.ca/wp-content/uploads/2019/09/privacy-breach-protocol-e.pdf.

However, the complainants questioned how the police could state this with certainty.

[30] In response, the TPS advised that since the Employee made the accesses so she could find out about any criminal activities that would cause her concern, she had no need to print or distribute this information. They also note that the Employee stated that she did not print or distribute any records.

[31] However, the TPS itself expressed some doubt as to the Employee's truthfulness elsewhere in its response, referring to her as "not completely forthright in her responses to the Investigating Detective."

[32] Given this, it would have been better for the TPS to have independently verified that the Employee did not use the database system to print documents containing the complainants' personal information. Knowing this would help determine if the Employee had any printed copies of the records of personal information in her possession, rather than having to rely on her word.

[33] I note that nothing in the information provided to me indicates that the Employee printed or otherwise further disclosed the complainants' personal information and I am generally satisfied that the TPS took adequate measures to ensure that the breach of the complainants' personal information was contained. However, the failure to verify that no documents containing personal information were printed is a gap in that aspect of their response. I recommend that in cases where the TPS has identified an unauthorized access to personal information, the TPS should independently verify whether the personal information has been printed as a step within its breach response.

[34] The next matter to be examined is whether the TPS took adequate steps to determine if the Employee made any other unauthorized accesses.

Audits

[35] Audits play an important role in determining the scope of a breach, as they can uncover whether an employee has made unauthorized accesses to personal information other than those identified by a particular complainant.

[36] During its initial investigation, the TPS was alerted to a possible access to a third individual's personal information. The TPS conducted an audit focussed on this individual and found that the Employee had indeed accessed this third individual's personal information.

[37] When asked by the IPC about whether they would conduct further audits to determine if the Employee had made other unauthorized accesses, the TPS stated that additional audits would require significant resources, due to the number of accesses the Employee conducted within her duties, and the difficulty in separating out any unauthorized accesses from authorized ones. However, the TPS later conducted an additional audit, stating that their reason for doing so was that the complainant's lack of

forthrightness caused concern that she may have made more unauthorized accesses.

[38] The TPS's concerns were borne out as the later audit, which covered a five-year span, showed unauthorized accesses to the personal information of an additional seven individuals.[4]

[39] This complaint came to the TPS because it was notified that the Employee had searched for another neighbour's personal information. Given that context, the TPS conducting additional audits into the Employee's accesses was key to fulfilling their security obligations under section 3(1) of Regulation 823.

[40] I am satisfied that the TPS conducted adequate audits to determine the scope of the personal information accessed without authority by the Employee. However, I recommend that the TPS implement a protocol for conducting audits of employees' accesses to personal information in cases where there is evidence that an employee has made unauthorized accesses, or in cases where the TPS has reason to suspect the employee may have made unauthorized accesses to personal information.

Notification

[41] The TPS provided written notification to the complainants by way of letter. However, the audits the TPS conducted during the course of this investigation led to the discovery of other individuals whose personal information was accessed without authorization by the Employee. The TPS state that they did not notify those individuals of the privacy breaches affecting them.

[42] Notification is one of the key elements of addressing a privacy breach. The Privacy Breach Guidelines set out that notification should take place as soon as reasonably possible. Further, the TPS's own guidelines addressing privacy breaches (addressed in more detail below) also speak to the need to notify those affected, as they state that when the TPS has confirmed that a breach involving personal information has occurred, the TPS should provide notification to the affected parties.

[43] While these breaches were discovered at a later date than the accesses involving the complainants, there is no expiration period on the need to notify individuals of breaches to their privacy. Therefore, I recommend that the TPS provide notification to those individuals whose personal information was accessed without authorization under the *Act* by the Employee.

Privacy Policies and Guidelines:

[44] I asked the police to provide me with any policies or other training materials that address unauthorized accesses to personal information. In response, the police

[4] During this investigation, I asked the TPS if they had notified these additional individuals of these unauthorized accesses. They stated that they did not do so. I will address this failure to notify below.

provided me with the following sections of the Information Management Chapter of the TPS Policy and Procedure:

- Chapter 17-02 Information Breaches (the Breach Chapter)
- Chapter 17-03 Requests for Information Made Under the Municipal Freedom of Information and Protection of Privacy Act (the Access Chapter)

[45] Part 1.12 the Access Chapter directs that information in the TPS data system is confidential and generally is not to be disclosed except in specific circumstances. It reads in part as follows:

> Members shall… treat as confidential any data or information obtained from, or entered into a computerized information system … and shall not impart or allow any member or non-member access to such data or information, except:
>
> (i) when required in the performance of their duties; or
>
> (ii) when otherwise directed by the Chief of Police.

[46] The portion of the Access Chapter addressing confidential information further states that a member shall not disclose information they acquired in the course of being a [TPS] member or copy any [TPS] record, other than as required in the performance of their duties, as authorized by their supervisor, or as required by law. The policy also states that members shall not release or provide access to TPS documents unless it is in accordance with the law or authorized by the Chief of Police.

[47] The Breach Chapter sets out the steps to take when the TPS learns of a breach of any information under the care and control of the TPS. It describes the potential consequences of such breaches to employees in its Rationale section as follows:

> Any unauthorized release of information exposes the Service to civil and legal consequences as well as jeopardizes the public's trust and confidence in the Service. Members who make an unauthorized release of Service information may be subject to internal discipline and/or civil and legal consequences.

[48] The Breach Chapter also defines what a breach is:

> Breach means the unauthorized collection, use, alteration, modification, disclosure, or destruction of Toronto Police Service information. This includes privacy breaches, which relate specifically to personal information.

[49] The *Act* prohibits not just unauthorized disclosures, but also unauthorized

accesses to personal information; policies must clearly communicate that both are prohibited. While a breach, as defined in the Breach Chapter, includes unauthorized use of personal information, the consequences set out only address an "unauthorized release" of personal information. It is not clear from that the Breach Chapter that those who make improper accesses to personal information face the same consequences.

[50] In contrast, the Access Chapter does state that members may only access database information if necessary for their duties or if authorized to do so by the Chief of Police. However, that constraint is found in a chapter whose purpose is to provide a process for responding to access requests made under the *Act*.

[51] In my view, it is unlikely that employees seeking guidance on their privacy obligations would reach for a chapter addressing how to respond to access requests. Guidance needs to be clear and comprehensive, but it also needs to be findable. Placing this guidance in the Access Chapter but not in the Breach Chapter does not satisfy the TPS's obligation to provide guidance to employees on their privacy obligations.

[52] In follow up correspondence to the TPS I asked for any additional policies in place to prevent unauthorized accesses. The police did not direct me to any additional guidance documents, instead stating:

> [We], along with every other organization meeting the definition of 'institution' under *MFIPPA*, do not have such policies that can completely prevent misuse. There is no training or prospect of punishment that will completely prevent unauthorized accesses. The weakest link in any organization's security protocols is always the employee, as there are certain individuals that will tempt fate no matter the consequences.

[53] I acknowledge the TPS's point that airtight protection against unauthorized accesses to or disclosures of personal information may not be possible, and indeed, perfection is not the standard the TPS is being held to. Rather, section 3(1) of Regulation 823 requires that reasonable measures to prevent unauthorized accesses be in place. The privacy documentation that the TPS provided – limited to the Breach Chapter and the Access Chapter of its Policy and Procedures – do not demonstrate that this standard has been met. The Breach Chapter does not describe the consequences that could result from an unauthorized access to personal information, and the privacy constraints regarding employees accessing the police database are only found in the Access Chapter, which an employee may not know to consult.

[54] I recommend that the TPS enhance or revise its existing guidance documents to more clearly communicate that staff are not permitted to use or access personal information in police databases, and to communicate this in a form or place where employees may be able to easily locate this guidance. These guidance documents should communicate that doing so is a breach of the *Act*, and set out the possible consequences to the employee for doing so.

Training:

[55] In addition to having adequate privacy guidance documents in place, institutions should also provide its employees with privacy training, to ensure that employees are adequately and effectively advised of their privacy obligations. In response to my request for information on their privacy training regime, the police provided the following information:

> Privacy training regarding obligations to safeguard information is ongoing and occurs throughout a member's career. The topic of confidentiality/privacy is covered during onboarding training for officers, as well as when there is training as result of a promotional processes, Professional Standards courses, or in specific units (e.g. Communications Operators). All members of the Service have privacy awareness training on an ongoing basis through the use of screensavers (with privacy specific education and guidelines) or on special occasions such as Privacy Day when there is an opportunity to write an article about privacy issues. Any time members of Access & Privacy liaise with members while responding to *MFIPPA* requests there is a level of education about privacy obligations and the *Act*.

[56] The police state that they have had privacy awareness training in place since June 2018, but state that they are "unable to respond" to the question of whether and when the Employee had received privacy training.

[57] Tracking employee participation is key to ensuring that all employees receive relevant and up-to-date privacy training. It is concerning that the TPS could not provide confirmation that the Employee had received privacy training, or state when that occurred. However, they did note they now have a system in place to record employees' privacy training and that if an employee misses a training session, it will be rescheduled.

[58] When asked for copies of the training materials used by the police, they declined to provide these, stating that they were employment-related information pursuant to section 52(3) of the *Act*, and therefore excluded from the auspices of the *Act*.

[59] Instead of providing privacy training materials, the police contended that the Employee was fully advised of her obligations under the *Act*, stating as follows:

> [The] employee was made fully aware of the importance of privacy, confidentiality, authorized access and not to use our resources for personal gain. No other training is needed in regards to the prevention of unauthorized accesses as this is a simple concept to comprehend and is agreed to by all of our members through the aforementioned 'user agreement'.

[60] The user agreement the police refer to is a privacy warning flag, which appears on all TPS computers and other devices prior to users being able to sign in to those devices. It reads as follows:

- Accessing TPS I&IT resources will be deemed a valid consent to the terms of TPS Standards of Conduct and Procedures.
- Each member is expected to use TPS I&IT resources to perform their assigned duties and not for personal gain, entertainment or malicious purposes.
- All transactions are subject to monitoring/audit and may be recorded in order to ensure compliance. Therefore, members can expect a reduced expectation of personal privacy while using all TPS-IT resources, at all times.
- Violation of these terms of acceptable use will be assessed on a case- by-case basis and may expose a member to disciplinary action, up to and including dismissal.
- Members are encouraged to familiarize themselves with the Acceptable Use Agreement (located in the 'Governance' section of the TPS intranet), and seek clarification from a supervisor or Unit Commander when required.

By clicking OK, you accept the above agreement.

[61] Warning flags, such as the one captured above, can be a useful tool to inform employees of their privacy obligations on a regular basis. I note that the above warning does not include any reference to the *Act*, or employees' obligations to ensure the privacy of personal information in the data system. The flag could be improved to more directly communicate these obligations to them.

[62] Regardless of the wording of this particular example, privacy warning flags are not a substitute for adequate training and privacy policies. They are only one facet of how an institution can ensure the security of the information in its custody or control.

[63] The police describe unauthorized accesses as a "simple concept". I disagree with this assessment. Without adequate training in their privacy obligations, employees may not be aware of what accesses they are permitted to make and for what purposes.

[64] The response by the police has laid the responsibility for the accesses at the feet of the Employee, noting that not all accesses can be prevented as there will be cases where employees "tempt fate." This may well be true, but without more information about the specifics of the training provided to the Employee, I cannot know whether she knew she was acting inappropriately, or if she was aware of the possible consequences of her actions. While the police may state that the Employee "was made fully aware of the importance of privacy, confidentiality, authorized access and not to use our resources for personal gain," they have not demonstrated that this is indeed

the case.

[65] The police point to interviews in which the Employee admitted to conducting unauthorized inquiries as proof that she was aware she was acting inappropriately. This, however, does not negate the possibility that had her training been more up to the task, she may not have made these inquiries. Put another way, I can only be satisfied that this incident is attributable solely to employee wilfulness by reviewing the training that the TPS provided her with. I do not have that information before me in this case.

[66] More importantly, I do not know what training other employees are being provided with regarding their privacy obligations. Part of my role as investigator is to determine whether an institution has adequate measures in place to prevent unauthorized access to records, and without being provided with more information regarding privacy training, I cannot be satisfied that the current measures are adequate.

[67] I also want to address the TPS claim that the training materials themselves are excluded from the *Act*, because they are employment-related materials pursuant to section 52(3) of the *Act.* Section 52(3) reads in part as follows:

> [This] Act does not apply to records collected, prepared, maintained or used by or on behalf of an institution in relation to any of the following:
>
> …
>
> 3. Meetings, consultations, discussions or communications about labour relations or employment-related matters in which the institution has an interest.

[68] The IPC has previously addressed whether training guidance is excluded from the *Act* pursuant to section 52(3). IPC Order PO-2913 dealt with the equivalent provincial provision under *FIPPA* to determine whether training materials prepared for use at the Ontario Provincial Police Academy were excluded from that Act's application. The adjudicator determined that there was a distinction between records relating to an employee's personnel record and generic training materials, stating as follows:

> …the records at issue in the current appeal are OPP-wide procedures used to establish consistency in, and adequacy of training. As well, they are tools for ensuring that the OPP as an organization meets its statutory mandate as a police agency, as noted by the Ministry. In addition, although not determinative of the issue, I would suggest that the establishment of training standards is one facet of holding the police accountable to the public with respect to the overall performance and behaviour of its officers…

[69] The adjudicator in that case found that the training materials were generic in nature, and therefore not excluded from the application of *FIPPA*. I adopt this reasoning. Having the training materials provided for review would permit me to better evaluate whether employees are receiving adequate privacy training. Without that information, I am left with only the TPS's bare assurances that it is providing the necessary privacy guidance. Section 52(3) of the *Act*, does not prevent the TPS from showing – rather than just telling – that it is meeting its privacy obligations.

[70] Having not been provided with the training materials used, I am not satisfied that the TPS has satisfied its privacy obligations under Section 3(1) of Regulation 823. I recommend that the police review its current privacy training program and revise it as necessary to ensure that it provides adequate and specific privacy protection against unauthorized accesses to personal information within its databases. The TPS should also provide me with a complete copy of its training program, including its training tracking procedures, in order to demonstrate its compliance with section 3(1) of Regulation 823.

Communication of Disciplinary Information:

[71] In the letter that notified the complainants of the breach, the TPS noted that the Employee "received counselling to mitigate any similar breach of this nature occurring in the future." This letter was sent some months prior to the Employee's resignation, presumably while the conduct investigation was ongoing.

[72] In the earlier stages of this file, the TPS indicated that disciplinary measures had been taken, but provided no further details. Given that, I asked the TPS for specifics of the disciplinary measures the TPS imposed on the Employee, prior to her resignation.

[73] The TPS confirmed that the conduct investigation of the Employee terminated at the time of her resignation, but would not provide any further details regarding discipline. The TPS stated that they would not do so because they did not believe that it would have any deterrent effect on other employees, and would not appease the complainants, stating that "the affected party is never completely satisfied with the penalties imposed." They also stated that section 52(3) of the *Act* applies such that "records created during the course of this investigation; and those resulting from any disciplinary penalty imposed on the [Employee], would fall outside the auspices of the *MFIPPA*."

[74] For those whose privacy has been breached, reassurance that a breach has been adequately remediated may be important. This was addressed by the IPC in Privacy Complaint Report PC11-34, which also involved private information gleaned from a police database. The investigator in that case stated as follows:

> In my opinion, in circumstances such as these, institutions should disclose detailed information about the privacy breach and the disciplinary action

> taken to the victim of the breach. While this office will not comment on the adequacy of the disciplinary action, if any, the disclosure of this information to an affected individual may serve two purposes. First, it may act as a deterrent to other staff who are entrusted with the privacy of the personal information of members of the public.
>
> In addition, it may reassure the affected individual(s), and other members of the public who have entrusted their personal information with that institution, that the institution will take the necessary steps to ensure that this type of conduct is not repeated. This is particularly important in the context of a privacy breach such as this one which involves highly sensitive personal information. Moreover, this approach accounts for the fact that the citizens of Ontario do not have the option of dealing with another police force, if they find that their personal information has not been appropriately protected.

[75] I am mindful of the particular circumstances of this case, in which the conduct investigation terminated early because of the Employee's resignation. I also note that in their notification letter, sent before the conduct investigation terminated, the TPS did confirm that the Employee had been provided counselling. Given this, I am satisfied that in this particular situation, the TPS has met its obligation to disclose information about the breach, including the disciplinary actions taken. As this is the case, there is no need for me to further address the TPS's position regarding the application of section 52(3) of the *Act*.

CONCLUSION:

1. The information at issue is personal information as defined under section 2(1) of the *Act*.

2. The Employee's uses of the complainants' personal information were not in accordance with section 31 of the *Act*.

3. The Employee's verbal communication of the complainants' personal information to the associated officer was a disclosure of personal information that was not in accordance with section 32 of the *Act*.

4. The TPS does not have reasonable measures in place to prevent unauthorized accesses to and disclosures of personal information of individuals in accordance with section 3(1) of Regulation 823 to the *Act*.

RECOMMENDATIONS:

I recommend that the TPS:

1. As part of its breach response, verify whether personal information has been printed in cases where the TPS has identified an unauthorized access to personal information.

2. Implement a protocol for conducting audits of employees' accesses to personal information in cases where an employee has been shown to have made unauthorized accesses, or in cases where the TPS has reason to suspect the employee may have made unauthorized accesses to personal information.

3. Provide notification to those individuals whose personal information was accessed without authorization under the *Act* by the Employee.

4. Enhance or revise its existing guidance documents, to more clearly communicate that staff are not permitted to use or access personal information in police databases, and to communicate this in a form or place where employees may be able to easily locate this guidance. These guidance documents should communicate that doing so is a breach of the *Act*, and set out the possible consequences to the employee for doing so.

5. Review its current privacy training program and revise it as necessary to ensure that it provides adequate and specific privacy protection against unauthorized accesses to personal information within its databases.

Within six months of receiving this Report, the TPS should provide this office with proof of compliance with the above recommendations, including a complete copy of the TPS privacy training program.

Original Signed by: September 16, 2022

Jennifer Olijnyk
Investigator