Information and Privacy Commissioner,
Ontario, Canada

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

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT PR23-00009

Toronto Metropolitan University

August 26, 2025

Summary: The Toronto Metropolitan University (TMU) reported a privacy breach under the *Freedom of Information and Protection of Privacy Act* to the Office of the Information and Privacy Commissioner of Ontario. TMU discovered the breach when a reporter from The Toronto Star advised TMU it had obtained "internal information" from a TMU safety and security team member.

In this report, I find that in addition to the unauthorized access reported by TMU, there was also an unauthorized disclosure of personal information to The Toronto Star. I also find that TMU did not respond adequately to the breach.

While TMU has taken steps to remedy some of the issues identified in this investigation, given the concerns raised here, I recommend improvements to TMU's privacy guidance documents, practices and privacy training.

Statutes Considered: *Freedom of Information and Protection of Privacy Act*, R.R.O. 1990, c. F.31, as amended, sections 2(1) and 42(1); R.R.O. 1990, Regulation 460, section 4(1).

Investigation Reports Considered: Privacy Complaint Reports MI10-5, MR21-00114, NJ12-7, PC07-71, PC11-34, PC18-00074, PC20-00017, PR16-40 and PR17-23.

BACKGROUND:

[1] On February 15, 2023, the Toronto Metropolitan University (TMU) reported a breach under the *Freedom of Information and Protection of Privacy Act* (the *Act)* to the Office of the Information and Privacy Commissioner of Ontario (the IPC).

[2] TMU reported that, on February 3, 2023, a reporter from The Toronto Star (The Star) contacted TMU with a list of questions about security practices on its campus. The reporter advised TMU that The Star had spoken with "a community safety and security member and had information about TMU's security guards' shift schedules and dispatcher radio logs."

[3] Based on the above, TMU launched an investigation and, through an audit, discovered that a contracted security dispatcher (the contractor) had downloaded 735 records from TMU's cloud-based drive without authorization between August 7, 2022 and February 8, 2023. Consequently, TMU reported a privacy breach to the IPC. The breach report did not indicate the number of affected individuals.

[4] The contractor responsible for the breach was employed by TMU's third-party security services provider. The records were accessed via the contractor's personal mobile devices, using the TMU multi-factor authentication process. TMU reported the privacy breach because the records "contained internal security-related information that may have also contained personal information of students, faculty and staff that may have been disclosed to the Toronto Star."

[5] According to the breach report, the downloaded records included daily radio logs (the logs) of documented security incidents on campus based on calls received by TMU's Campus Safety and Security Office, and they contained the following personal information:

- the names of students, faculty, and staff who had reported and been involved in security incidents, student ID numbers and personal contact information consisting of phone numbers.

[6] To contain the breach, on February 8, 2023, TMU terminated the contractor's access to all its systems and documents, as well as the contractor's ability to work on its premises. TMU stated that the contractor provided their personal phone and laptop (the devices) for inspection to TMU's security services provider, the contractor's employer, and neither device revealed evidence of the downloaded documents. TMU also reported that the contractor's employment was terminated by the security services provider approximately a month after TMU discovered the breach. Further, TMU advised that it received assurances from The Star that "they would not disclose any personal information in their reporting."

[7] On March 8, 2023, The Star published an article regarding safety on TMU's campus, specifying that it had seen internal security schedules after the newspaper was contacted by "a member of TMU's security team [who] provided staff schedules and other internal documents to support their claims."[1] The article stated that TMU requested The

[1] Kennedy, Brendan. "'This Campus Isn't Safe': Following a String of Sexual Assaults inside a Toronto University, the School's Response Is under Fire." *Toronto Star*, 9 May 2023,

Star hand over the "stolen documents" shared by its source, which the newspaper declined to do. The article also stated that The Star had provided TMU with a description of the information contained in the documents.

[8] Regarding notification, TMU advised in its breach report that it did not give notice to any potentially affected parties for various reasons, including TMU's containment and control of the breach, The Star's assurances regarding disclosure, lack of evidence of malicious intent, a risk of harm to the affected individuals because "individuals could 're-live' the incidents that they reported", and a risk of damage to trust in campus security.

[9] After reviewing TMU's breach report, the IPC had concerns about the adequacy of its response to the breach, particularly with respect to containment and notification. The IPC also had concerns about the security measures TMU had in place to protect its records. As a result, this matter moved to the investigation stage of the IPC's complaint process, and I was assigned as the Investigator.

[10] As part of my investigation, I requested and received written representations from TMU, discussed below.

PRELIMINARY ISSUES:

[11] TMU submitted that the information in the logs is "personal information" as defined in section 2(1) of the *Act*. I agree with this characterization.

[12] TMU did not dispute that the contractor used this personal information without authorization contrary to section 41(1) of the *Act* when he downloaded the logs.

ISSUES:

1. Was there a disclosure of personal information, and if so, did it comply with section 42(1) of the *Act*?

2. Did TMU respond adequately to the breach?

DISCUSSION:

ISSUE 1: Was there a disclosure of personal information, and if so, did it comply with section 42(1) of the *Act*?

[13] During this investigation, TMU stated that neither it nor its third-party security services provider found any evidence that the personal information downloaded was

---

http://www.thestar.com/news/investigations/this-campus-isn-t-safe-following-a-string-of-sexual-assaults-inside-a-toronto-university/article_06a2ba2f-56b6-53cc-8601-a09f528af2ab.html.

disclosed to The Star. TMU also advised that the contractor denied downloading and/or disclosing the personal information to The Star or any other third party.

[14] Further, TMU advised that The Star described two records in its possession - a "Systems Daily Service Checklist" and "Shift Schedules" – and based on this description, TMU found that these records did not contain personal information.

[15] Although TMU acknowledged that it would be an unauthorized disclosure under the *Act* if The Star was provided with additional records containing personal information by the contractor, TMU took the position that, "without confirmation from the Toronto Star that any record other than the two described, were provided to them, TMU does not have information that suggests the Toronto Star has personal information belonging to TMU in its custody."

[16] Specifically, TMU concluded that the breach did not involve a disclosure of personal information, for the following reasons:

> Based on our analysis of the two types of records (but not the actual records) we now can confirm that the two records on their own do not contain personal information. Though it is possible that an additional record i.e. the radio logs were provided to the Star, our investigation has not confirmed this disclosure to the Star. Further, as the focus of the Star's article[2] was on the adequate security coverage and deployment of security guards on the university campus, the record of interest would likely have been the Shift Schedule which includes no personal information, and only details of the dates and work assignments of the security guards in their professional capacity.

[17] Respectfully, I disagree with TMU's conclusion as I believe there was, on a balance of probabilities, a disclosure of personal information to The Star.

[18] I take this position because, although the security services provider's investigation did not find that personal information was disclosed to The Star, TMU acknowledged this possibility as it was unable to confirm that the logs were not provided to The Star. Additionally, in April 2024, when TMU asked The Star to confirm whether it had received personal information, The Star neither confirmed nor denied this.

[19] It is important to note that when TMU reported the breach and detailed that the logs had been downloaded, it did not report that any emails were part of this breach. According to an email from The Star to TMU in March 2023, the newspaper had in its possession a copy of an email sent by a student to the general security inbox. I note that in February 2025, TMU stated to the IPC that it "does not have knowledge of the Toronto

[2] Ibid. This article specified that The Star had seen internal security schedules after the newspaper was contacted by "a member of TMU's security team [who] provided staff schedules and other internal documents to support their claims."

Star having any other records or information."

[20] Moreover, as mentioned above, TMU reported to the IPC that on February 3, 2023, The Star contacted TMU advising it "had information about TMU's security guards' shift schedules and dispatcher radio logs" (*emphasis added*). As stated above, there is no dispute that the logs contain personal information within the meaning of section 2(1) of the *Act*.

[21] Additionally, in my view, the case for The Star having likely received personal information is further supported by the following factors:

a. The Star had a copy of an email from a student to the general security inbox. In correspondence exchanged between The Star and TMU, the newspaper stated: "We have obtained a copy of an email sent by a student to the general security inbox." The Star's correspondence also quoted a statement from the student's email which expresses the student's concern about safety on campus. In this email, the student expresses their views and opinions. While TMU did not identify this record in its breach report to the IPC, I find that it contains personal information relating to an identified individual. This record is part of the same email chain discussing records obtained "from a member of TMU's Community Safety and Security team," and it contains the personal views or opinions of an identifiable individual, which is considered "personal information" under paragraph (e) of the definition of that term in section 2(1) of the *Act*. This is conclusive evidence that The Star had a record containing personal information in its possession.

b. TMU's determination that checklist and schedule records described by The Star were a part of the records downloaded by the contractor.

c. Importantly, there is no conclusive evidence before me from TMU indicating that The Star did **not** receive the logs from the contractor (or otherwise). TMU's audits do not appear to track this information and in my view, it is more likely that the contractor disclosed all the information they downloaded to The Star without picking and choosing specific documents.

[22] For these reasons, I find that, on a balance of probabilities, personal information was disclosed to The Star.

[23] With respect to this disclosure, section 42(1) of the *Act* sets out the circumstances in which personal information may be disclosed. Section 42(1) of the *Act* imposes a general prohibition on the disclosure of personal information but states that personal information may be disclosed in several enumerated exceptional circumstances. Section 42(1) states, in part:

> An institution shall not disclose personal information in its custody or under its control except,

> (a) in accordance with Part II;
>
> (b) where the person to whom the information relates has identified that information in particular and consented to its disclosure;
>
> (c) for the purpose for which it was obtained or compiled or for a consistent purpose;
>
> (d) where disclosure is made to an officer, employee, consultant or agent of the institution who needs the record in the performance of their duties and where disclosure is necessary and proper in the discharge of the institution's functions;
>
> [...]

[24] As stated in Privacy Complaint Report PC07-71[3], "in order for a given disclosure of personal information to be permissible under the Act, the institution in question must demonstrate that the disclosure was in accordance with at least one of the section 42(1) exceptions." In this matter, TMU has not indicated that any of the circumstances in section 42(1) would apply if the personal information was disclosed. I also note that TMU acknowledged that a disclosure of personal information in this circumstance to The Star would not be authorized under the *Act.*

[25] Accordingly, I find that the disclosure of personal information to The Star was contrary to section 42(1) of the *Act*.

Issue 2: Did TMU respond adequately to the breach?

[26] In this matter, the breach involved the unauthorized use and disclosure of personal information.

[27] To determine whether TMU has responded adequately to the breach, the IPC's guidance document, *Privacy Breaches: Guidelines for Public Sector Organizations* (the Breach Guidelines)[4] is informative. The Breach Guidelines recommend steps that institutions should take to contain a breach, investigate it, reduce the risk of a similar breach from reoccurring and notify affected individuals.

[28] The Breach Guidelines also set out the need to review the policies and practices in place to protect personal information, together with privacy training provided to staff (or contractors), so an institution can determine whether it needs to improve its documents and processes and take corrective action.

---

[3] See PC07-71 - Information and Privacy Commissioner of Ontario.

[4] *Privacy Breaches: Guidelines for Public Sector Organizations*, Information and Privacy Commissioner of Ontario, Toronto, Ontario, 2019.

[29] As part of my investigation, I reviewed TMU's:

- *Privacy and Access to Information Policy, including Appendix B: Privacy Breach Protocol*;
- *Privacy Incident Management Web Page*[5];
- *Information Protection Policy*;
- *Acceptable Use of Information Technology Policy*;
- Standard operating procedure, Security Procedure for Moving Files into Secure Drive;
- *Confidentiality Agreement*;
- *Final Executed [security services provider] Master Services Agreement*; and
- Staff/contractor privacy training.

Containment

[30] To contain a breach, institutions should identify the nature and scope of the breach, determine what personal information is involved, and take containment measures. Such measures include ensuring that no personal information has been retained by an unauthorized recipient and that the breach does not allow unauthorized access to any other personal information.[6]

[31] After identifying the contractor as the individual who used and disclosed the records without authorization on February 6, 2023, TMU terminated their access to all its systems and data, including the cloud-based drive in which the logs were stored, on February 8, 2023.

[32] I find it concerning that TMU provided inconsistent information regarding its own investigation into the containment of the breach. It appears that TMU had not identified the full scope of the breach by July 2023 because in submissions to the IPC at that time, TMU twice stated that the contractor provided their personal phone and laptop devices for inspection and neither device revealed evidence of the downloaded documents. In response to this investigation, in February 2024, TMU clarified that it had received assurances from its security services provider on February 15, 2023, that the information downloaded to the contractor's personal devices had been permanently deleted "in the presence of [the security services provider's] employee(s)". In retrospect, TMU confirmed that the contractor did not retain personal information on their personal devices based

---

[5] https://www.torontomu.ca/gcbs/what-we-do/access-privacy1/privacy-incident-management/

[6] *Privacy Breaches: Guidelines for Public Sector Organizations*, Information and Privacy Commissioner of Ontario, Toronto, Ontario, 2019.

on the assurances it received about the permanent deletion of this information.

[33] TMU also noted that after discovering the breach, TMU twice requested that The Star return the records it had been provided with, noting its concerns "about certain documents containing personal and confidential information that was stolen from the university and may have been given to [The Star]." TMU stated to The Star that disclosure of this information would be a privacy breach.

[34] In my view, the following actions demonstrate the steps taken by TMU to contain this element of the breach:

- terminating the contractor's access to TMU systems, data, and physical location;
- receiving assurances from its security services provider that the personal information downloaded by the contractor was deleted from their devices;
- requesting the return of records from The Star; and
- receiving assurances from The Star that "they would not disclose any personal information in their reporting."

As such, I am satisfied with TMU's steps to contain the breach.

Notification

[35] Initially, TMU decided not to notify individuals affected by the breach. However, after discussions with the IPC, TMU revised its position and advised that it would notify those for whom it had contact information.

[36] In February 2024, almost a year after the breach, TMU determined that 174 records containing personal information were downloaded from its systems without authorization, affecting 880 individuals.

[37] By early May 2024, TMU had notified by telephone a total of 655 affected individuals. The remainder of the affected individuals could not be contacted due to invalid numbers or unanswered calls after two attempts.

[38] The Breach Guidelines state:

> You should notify those affected as soon as reasonably possible if you determine that the breach poses a real risk of significant harm to the individual, taking into consideration the sensitivity of the information and whether it is likely to be misused.

[39] I am concerned about the time it took TMU to revise its position on notification because this meant that TMU notified affected individuals a year after the privacy breach occurred.

[40] Additionally, I am concerned that TMU was not fully transparent about the extent of the breach. In its telephone notification script, TMU noted the inappropriate downloading of personal information by the contractor twice, yet it did not specify that this information was stored on the contractor's personal devices. The script stated: "the guard has deleted the information from their devices and is no longer working for the university." This wording omits notifying affected parties that the personal information was downloaded to the contractor's "personal" devices, which I believe minimizes the nature of the breach.

[41] TMU further failed to notify the affected individuals of the unauthorized disclosure to The Star. When I questioned TMU about this, TMU's position was that the notification script was and is appropriate for two reasons: 1. The Star's reliance on its journalistic principles around respecting confidentiality and privacy, and 2. TMU's investigation which determined that two records accessed by The Star did not contain personal information. TMU stated that "Anything further would be speculative and contrary to the information TMU is aware of."

[42] The Breach Guidelines state that notification to affected parties should include details about the extent of the breach, which in this case involved personal information that was downloaded to the contractor's personal mobile devices without authorization, as well as its unauthorized disclosure to The Star. Further, while I understand that TMU maintains the position that there was no unauthorized disclosure of personal information, in my view, TMU could have been more transparent about the likely disclosure of personal information by the contractor to The Star. In my view, this information should have been included in the notification given to the affected individuals.

[43] In conclusion, I find that TMU did not respond adequately to the breach with respect to notification because:

a. it took over a year to notify all affected individuals, far beyond the IPC's Breach Guidelines to notify "as soon as reasonably possible";

b. the notice did not advise affected individuals of the downloading of their personal information to the contractor's *personal* devices; and

c. the notice did not notify affected individuals of the likely unauthorized disclosure of their personal information to The Star.

[44] Going forward, I recommend TMU take steps to ensure that when a breach occurs, those affected by the breach are notified in accordance with the IPC's Breach Guidelines.

[45] Despite my recommendation above, and my finding that an unauthorized disclosure occurred, I will not be recommending that TMU provide further notification to the affected individuals about the disclosure. In my view, while the notice ought to have included more detail for the benefit of affected individuals, I find no useful purpose in directing that further notice be provided now given the passage of time. Further, as TMU

is named in this publicly available report, these individuals may now become aware of the incident and its circumstances.

Information Practices

[46] Section 4(1) of Ontario Regulation 460, made pursuant to the *Act*, requires that TMU "ensure that reasonable measures to prevent unauthorized access to the records [it has] are defined, documented and put in place, taking into account the nature of the records to be protected."

[47] This requirement "applies throughout the life cycle of a given record, from the point at which it is collected or otherwise obtained, through all of its uses, and up to and including its eventual disposal."[7]

[48] The Breach Guidelines provide guidance to institutions to assess whether they have satisfied the requirements in section 4(1). The Breach Guidelines inform TMU to review the policies and practices it has in place to protect personal information and its staff (or contractor) training to determine whether it needs to make changes to improve its documents and processes.

[49] In this matter, TMU determined that the contractor downloaded (used) the logs without authorization by accessing TMU's cloud-based drive via their personal devices, using the TMU multi-factor authentication process.

[50] Accordingly, I must determine whether TMU had information practices in place with respect to security measures (such as auditing, monitoring and logging), confidentiality agreements, and privacy training and awareness.

Auditing and Monitoring

[51] Once TMU was contacted by The Star reporter, it launched its audit to review internal systems for unauthorized activity. TMU found that the contractor viewed and downloaded hundreds of records, both while on and off shift, over an extended period without TMU detecting this activity (between August 7, 2022 and February 8, 2023).

[52] In my view, it is important that institutions have the ability to detect large or recurrent downloads of information, particularly if this capability is available to staff/contractors with access to personal information. It is also important to monitor with timely and regular auditing those with ready access to personal information.

[53] At the time of the incident, TMU was conducting audits "as necessary." However, in the wake of this incident, TMU has advised that it will monitor risk by conducting quarterly audits to check for suspicious activity, including downloading activity. It has also advised that it will conduct more system-wide audits of access and activity in archived

[7] See IPC Privacy Complaint Report MI10-5.

files.

[54] TMU has further noted that, in addition to these more "regular audits," staff will be reminded of its backend logging systems, which enable TMU to monitor activity and investigate incidents according to its policies, and that infractions may result in discipline.

[55] I am satisfied that the changes implemented by TMU to its auditing practices from "as necessary" to quarterly, together with the addition of reminders to staff, are reasonable responses to the breach and a marked improvement in helping detect unauthorized accesses in the future.

Access Management

[56] In response to the privacy breach, TMU has drafted a *Standard Operating Procedure* to document and explain the access controls for TMU's Security Management Team and has added "a more formal reporting process and form". TMU has also indicated that adherence to its privacy and other policies is more closely monitored by both its Security Management Team and its security services provider's Account Manager. TMU did not provide details to explain how this adherence is closely monitored or what "other" policies it was referring to.

[57] Further, TMU has stated that it has drafted an updated *Privacy and Access to Information Policy* which includes a *Privacy Breach Protocol*. This is currently being reviewed by stakeholders for feedback as part of TMU's policy review process. TMU noted that it expects to complete this review and stakeholder consultation process in 2025 and have the revised policy in place later in the year.

[58] Having reviewed information on TMU's website where its *Privacy and Access to Information Policy* is found, I note an inconsistency. Although the policy clearly sets out that it applies to "any other individual with access to Personal Information in the University's custody or control," the introductory page featuring the document says that the privacy policy is for "staff and faculty" and "all employees of TMU." During this investigation TMU emphasized that the contractor was not an employee of TMU. In light of this, I suggest that TMU update its website to specify that this policy also applies to contractors.

[59] After receiving a draft copy of this report with the recommendations, TMU advised that it approved and published an updated *Privacy and Access to Information Policy* in February 2025. It also highlighted that the version of this policy, which is currently posted on its website, references contractors as part of the "University Community" in the *Definitions* section of the policy, and that "University Community" includes "all students, faculty, and staff, including contractors and visitors."

[60] I have reviewed the above documents and am generally satisfied that they provide sufficient guidance. However, I take issue with two of the documents. One of these is TMU's *Privacy Incident Management Protocol*, which describes a privacy breach as "an

unauthorized disclosure of personal information." This definition is inaccurate as it does not take into consideration other elements set out in the *Act* such as unauthorized collection, theft or loss or unauthorized use. To remedy this, I will recommend that TMU update this document by providing an accurate definition. I discuss the second document, TMU's *Acceptable Use of Information Technology Policy*, which is part of the *Protocol*, immediately below.

Personal Devices

[61] I find TMU's *Acceptable Use of Information Technology Policy* to be deficient because it does not provide any specifics on protecting personal information on personal devices held by contractors. While this policy makes it clear that "The use of personally-owned equipment that involves the use of IT Resources is covered by this Policy," it does not set out specific guidelines or rules regarding the use of personal devices. Having reasonable measures in place to prevent unauthorized access to records whilst considering the nature of the records to be protected includes records stored on any device, including a personal mobile device such as a phone and/or a laptop.

[62] During my investigation, I invited TMU to provide submissions on the use of personal devices by contracted security services personnel since TMU advised that security guards use their personal devices to access logs and "this information was stored on the contractor's personal mobile device[s]."

[63] I also asked TMU to provide me with relevant polices and procedures regarding the use of such devices, inquiring whether TMU would consider creating these if they did not exist. TMU responded as follows:

> Contractors are obligated to abide by the terms of their confidentiality agreements with [TMU] and to follow the privacy and security guidelines provided to them as part of their [TMU] onboarding, including online privacy training modules and reminders to safeguard personal information as part of their duties.
>
> Following the breach, [TMU] reviewed and assessed its current practices and did not identify a policy gap as the cause of this issue, but rather a need to enhance data management and document security controls. The remediation […] involved changing and modifying the settings and access to documents, making access more restrictive […] which included an internal Procedure for Moving Files into a Secure Drive. […] Contractors can no longer access any files outside of the files needed for their specific shifts and do not have the ability to download any documents to any devices after the completion of their shifts.

[64] Based on the above, I note that through technical safeguards, TMU has removed contractors' ability to download any records to any devices after the completion of their

shift. However, it appears they can still download records to their personal devices **during** their shifts. It is also unclear for what purpose they would have this ability. TMU did not provide an explanation, nor a policy that clearly sets out in what circumstance (if any) it would be appropriate to download personal information. For this reason, I also have concerns that TMU has not clearly addressed this in its policy, nor communicated it to contractors.

[65] In Privacy Complaint Report NJ12-7,[8] the IPC stated that "Allowing the use of personal devices over which the agency has no control presents serious privacy and security risks." The report also suggested that in such circumstances, an institution or organization should conduct a review of other potential vulnerabilities elsewhere in the organization. For example, it should determine whether other employees were storing personal information on their mobile devices, to what extent personal devices were being used throughout the organization, and whether the personal information was secure.

[66] During this investigation, TMU's position was that this privacy breach was the result of one bad actor who disregarded the confidentiality requirements of the terms of their contract. I disagree with this characterization. In my view, allowing contracted security staff to access and use personal information on their *personal* devices without a clear policy is an organizational gap in the protection of that information.

[67] As such, I recommend that TMU create, implement and communicate to all contractors/security staff a policy/procedure setting out the specific circumstances in which they can access and use records containing personal information on their personal devices during their shifts.

Confidentiality Agreements

[68] TMU's *Employee Confidentiality Agreement* (the Agreement) for contractors employed by its third-party security services provider sets out consequences for contravening legal obligations or TMU's established polices and procedures. The Agreement requires contractors to sign in order to acknowledge that they have read it and will abide by it. It states in part:

> I understand that discipline or sanctions, up to and including dismissal, may result if I access, collect, use, disclose, or dispose of personal information that contravenes legal obligations or the University's established policies and procedures. I understand that the obligations of this Agreement will survive the termination of my employment or volunteer activities at Toronto Metropolitan University and that failure to keep confidential the personal information of individuals is grounds for appropriate disciplinary and/or legal action.

[69] TMU confirmed that all contractors sign a confidentiality agreement annually and

[8] See IPC Special Investigation Report NJ12-7.

that the contractor signed the Agreement in June 2022.

Training

[70] TMU stated that contractors are only required to complete privacy training when hired. It advised that this is pre-requisite training, which is tracked through an internal training system. TMU confirmed that the contractor completed onboard training, which included mandatory *Access to Information and Protection of Privacy* eTraining consisting of 2 online interactive modules: Module 1 on *Access to Information* and Module 2 on *Privacy Protection.* TMU stated that all contractors must complete the modules and pass the quizzes with an 80% score for each module. The contractor completed this mandatory training in June 2022.

[71] IPC guidance states that to achieve the goals set out in privacy policies and procedures, institutions must provide employees and contractors with corresponding training. As highlighted in Privacy Complaint PC18-00074,[9] the obligations under section 4(1) of Regulation 460 extend to providing adequate privacy training to ensure the protection of personal information.

[72] Training is a key tool to avert unauthorized accesses. Through training and education, an institution should communicate to employees (and contractors) that accesses to and uses of personal information for non-work reasons are a breach of the *Act* and could result in serious consequences.

[73] TMU submitted that it already had in place measures, including contractors' obligations to follow the privacy and security guidelines provided to them as part of their onboarding (including online privacy training modules) and reminders to safeguard personal information as part of their duties.

[74] Since the incident, TMU advised that it implemented the following additional training measures:

- TMU's Security Department has provided more privacy and procedural training to on-duty supervisors and contractors during team meetings and daily briefings;
- Contractors are now trained to balance the need for documentation with privacy best practices and the need to maintain safety and security on campus;
- TMU's Privacy Office has undertaken more proactive training regarding best practices for accessing and managing personal information at TMU in addition to the mandatory e-learning; and

[9] See PC18-00074 | Information and Privacy Commissioner of Ontario.

- Contractors are reminded of their privacy obligations during the aforementioned daily briefings and other team meetings.

[75] While reminders of privacy obligations are a good measure to implement post-breach, in my view, this is not enough. TMU does not provide regular training to its contractors. Regular and scheduled privacy training is a highly effective method to help reduce unauthorized accesses, as emphasized in Privacy Complaint Report NJ12-7, which states:

> Even if an organization does have strong privacy policies and protocols, […] those policies and protocols are of little assistance in ensuring the privacy and security of personal information if staff have not been adequately trained. It is equally important to conduct regular training courses to ensure that privacy awareness remains embedded within an organization.

[76] As such, I recommend that TMU review its current training program to ensure that, at a minimum, it provides privacy training to its security contractors on an annual basis. I also recommend that TMU use this breach as a case study within its training material.

Remediation

[77] In response to this incident, TMU has taken various corrective measures regarding its security procedures and practices to reduce the risk of a future similar breach, including by:

- reducing the amount of personal information collected and recorded in radio logs by using non-identifying codes for different call types and limiting the information collected (for example, information that is not material to the dispatch such as student or other ID numbers will no longer be documented);

- reconfiguring access controls to documents so that when contractors are working shifts at TMU, they only have access to the required documents to execute their duties;

- limiting access to all shift logs and historical\archival files by only allowing contractors to access logs specific to their shift and only for the duration of that shift;

- requiring contractors to specifically seek prior approval from TMU Security's management team if historical shift data is required, including an explanation of any exceptional situation requiring access;

- reviewing and updating access controls daily after shift changes;

- where technically possible, using features to remove "download" and "make a copy" permissions; and

- reminding contractors of their privacy obligations at bi-weekly team meetings.

[78] At the start of this investigation, I asked TMU to detail the disciplinary consequences imposed on the contractor. While TMU advised that the contractor was terminated by the security services provider for refusing to continue participating in their investigation, it is not clear to me that the contractor's termination was a result of being found responsible for the privacy breach. As noted in IPC Privacy Complaint Report PC11-34, the imposition of discipline is critical to appropriately addressing a privacy breach incident and taking steps to prevent a re-occurrence. This was further elaborated on in IPC Privacy Complaint Report PC18-00074, which highlighted that discipline serves a twofold purpose: it helps assure victims of a privacy breach that their personal information will not be treated the same way in future, and it deters other employees (or contractors) from committing similar violations.

[79] I noted to TMU that the Ministry of the Solicitor General's guidelines[10] state that **anyone** can file a complaint against a security guard for failing to comply with the *Private Security and Investigative Services Act* or its regulations. I also asked TMU to detail what steps, if any, it took to file a complaint about the contractor. In response, TMU stated:

> Toronto Metropolitan University (the "University") did not file a complaint with the Ministry of the Solicitor General as the University's contractual relationship is with [the security services provider] and the University has no formal relationship, contract, employment or otherwise with the guard in question. We knew the Contractor was employed by [the security services provider] and we felt our responsibility was to immediately inform [the security services provider] and take actions under our contract with [the security services provider] to have the individual removed from their assignment and any further shifts at the University as per Section 2.03 the Services Agreement between the University and [the security services provider]. […]
>
> Thus, it was the University's understanding that any complaints, follow-ups, interviews, investigations, and regulatory / licensing reports regarding the Contractor were [the security services provider's] responsibility.

[80] After providing a draft copy of this report with the recommendations, TMU advised that it has taken steps to report the contractor to the Ministry of the Solicitor General.

[81] Despite TMU's position on its contractual relationships with its security services provider and the contractor, I point out that TMU's Agreement sets out a contractor's legal obligations vis-à-vis the protection of personal information, in accordance with legislation and TMU policies and procedures. This Agreement also sets out consequences for breaches of such obligations. It does not, however, specify who has responsibility

[10] See Section 19 of SO 2005, c 34 | Private Security and Investigative Services Act, 2005 | CanLII and section 1 and 2 of O Reg 363/07 | Code of Conduct | CanLII.

over issuing discipline or sanctions. I find it contradictory that TMU believes that it "has no formal relationship, contract, employment or otherwise with the guard in question," but requires contractors to sign this Agreement.

[82] Further, while I understand that TMU's contractual relationship is with the security services provider and TMU felt that its responsibility was to immediately inform its security services provider, there was nothing precluding TMU from reporting this contractor to the Ministry of the Solicitor General since "anyone" can file a complaint. In fact, I find that this type of action would likely be more in keeping with TMU's Agreement. As such, I recommend that TMU review this Agreement and in the future, consider reporting any licensed security contractor to the Ministry of the Solicitor General when/if TMU determines that such a contractor has committed a privacy breach.

CONCLUSION:

Based on the results of my investigation, I conclude that:

1. There was an unauthorized disclosure of personal information to The Star contrary to section 42(1) of the *Act*; and

2. While TMU responded adequately to the breach in certain respects, it failed in others. Consequently, I make the recommendations set out below to enable TMU to take corrective action to prevent similar breaches in the future.

RECOMMENDATIONS:

1. I recommend that TMU conduct a review of its policies, procedures and training to address the issues raised in this report, namely:

    a. Take steps to ensure that when a breach occurs, those affected by the breach are notified in accordance with the IPC's Breach Guidelines;

    b. Set out clear expectations regarding the use of personal devices for work purposes by contractors. Alternatively, TMU may wish to consider whether issuing mobile devices to its contractors and/or security staff that TMU manages and controls would better mitigate any future privacy and security risks;

    c. Provide privacy training to contactors at regular intervals, including using this breach as a case study within TMU's training materials; and

    d. Clearly define the responsibility for contractor discipline or sanctions, including the consideration that TMU add to its checklist of remediation actions the reporting of any licensed security contractor to the Ministry of

the Solicitor General when determining they are responsible for a privacy breach.

2. Within six months of receiving this Report, TMU should provide the IPC with proof of compliance with the above recommendations.

Original Signed by: August 26, 2025

Alexandra Madolciu
Investigator