Information and Privacy Commissioner,
Ontario, Canada

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

ORDER MO-4611

Appeal MA22-00321

Toronto District School Board

January 6, 2025

Summary: A school board received a multi-part request under the *Municipal Freedom of Information and Protection of Privacy Act* for a variety of records, including privacy assessments. The board withheld the records at issue, taking the position that disclosure would impact its economic interests (section 11(a)). In this order, the adjudicator finds that one record is not exempt under section 11(a) and orders the board to disclose it. The adjudicator upholds the board's decision to deny access to the two remaining records on the basis that section 11(a) applies and finds that the public interest override (section 16) does not apply.

Statutes Considered: *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. M.56, as amended, sections 11(a) and 16.

Orders Considered: Orders MO-2070, MO-3175, MO-2866, MO-3182, MO-2456, M-381, MO-3990.

OVERVIEW:

[1] This order determines whether the Toronto District School Board (the board) properly withheld information pursuant to the exemption for records that would impact an institution's economic and other interests at section 11(a) of the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*). It also considers whether there is a compelling public interest in the disclosure of any of the records to which the exemption is found to apply.

[2] The board received a multi-part access request pursuant to the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*) as follows:

1. Any requests the TDSB has received about sharing users' information with a domestic or foreign government or government agency or law enforcement agency either directly from the agency itself, or indirectly from a TDSB service provider, like Google or Microsoft;

2. Any notices that the TDSB has received from a TDSB service provider, like Google or Microsoft, that inform the TDSB that users' information has been turned over to the domestic or foreign government or government agency or law enforcement agency;

3. Any documents that indicate how the TDSB responded to the above requests or notices in points 1 or 2;

4. The search for the records for the above items only needs to cover the periods of 2011 to present day;

5. A copy of the TDSB's "Transparency Report" or similar document (if the TDSB creates such a document). A "Transparency Report" is a document that many organizations publish that describe the information requests from a government, an agency of the government or law enforcement agency;

6. All Privacy Impact Assessments (PIAs) for Google services or apps that are used by the TDSB (see Policy P094);

7. All assessments for Google related services that were performed under the Cyber Risk and Security Policy (see Operational Procedure PR725).

Please note that it may be possible that this FOI request may return personal information on students at the TDSB. To be clear, I am not interested in learning about the identities of individual persons. I am attempting to gather information [on] which governments, agencies, law enforcement agencies that the TDSB has been providing personal information to.

[3] The board denied access to records that were responsive to parts 2, 3, 6, and 7 of the request in their entirety, citing sections 11(a) (economic and other interests) and 14(1) (personal privacy) of the *Act*. The board also advised that it was not able to locate records responsive to parts 1 and 5 of the request.[1]

[4] The requester, now the appellant, appealed the board's decision to the Information and Privacy Commissioner of Ontario (IPC).

[1] Part 4 sets out the relevant time period for parts 1 through 3 of the request and is not a request in itself.

[5] During mediation, the appellant expressed his belief that records responsive to part 5 of his request for a "Transparency Report" or similar document should exist. The appellant provided an explanation and example of this type of record.

[6] The mediator shared this information with the board, who indicated that it did not have a transparency report or any other record responsive to part 5 of the appellant's request. The board also confirmed that it was maintaining its decision to deny access to the responsive records pursuant to sections 11(a) and 14(1) of the *Act*.

[7] The appellant subsequently confirmed that he is no longer taking issue with the board's search for records relating to part 5 of his request. The appellant also confirmed that he is not seeking access to the information that the board withheld pursuant to section 14(1) of the *Act*. However, the appellant raised the possible application of the public interest override at section 16 of the *Act*.

[8] As mediation did not resolve the appeal, the file was transferred to the adjudication stage of the appeal process, where the adjudicator may conduct an inquiry under the *Act*.

[9] During the adjudication stage, the board issued a revised decision in which it granted partial access to the email records responsive to parts 2 and 3 of the request, which were previously withheld in their entirety. The board indicated that it was continuing to rely upon section 14(1) to withhold the remaining personal information in the records.

[10] In light of the board's revised decision and the appellant's previous confirmation that he is not seeking access to information withheld pursuant to section 14(1) of the *Act*, the email records responsive to parts 2 and 3 of the request are no longer at issue in this appeal.

[11] The adjudicator originally assigned to the appeal sought and received representations from the board and the appellant. The appeal was subsequently transferred to me to complete the inquiry and issue a decision. After reviewing the parties' representations, I determined that I did not need to hear from the parties further before issuing this decision.

[12] For the reasons that follow, I uphold the board's decision in part. I find that the section 11(a) exemption applies to two of the responsive records and that the public interest override at section 16 does not apply. I find that there is insufficient evidence for me to conclude that section 11(a) applies to the remaining record and order the board to disclose it to the appellant.

RECORDS:

[13] The records at issue consist of the following:

Record Number	Record Description	Responsive To	Decision	Exemptions Claimed
3	TDSB audit	Parts 6, 7 of request	Withheld in full	Section 11(a)
4	Risk assessment	Part 6 of request	Withheld in full	Section 11(a)
5	Security scan	Part 7 of request	Withheld in full	Section 11(a)

ISSUES:

A. Does the discretionary exemption at section 11(a) apply to the records?

B. Pursuant to section 16, is there a compelling public interest in the disclosure of the records?

DISCUSSION:

Issue A: Does the discretionary exemption at section 11(a) apply to the records?

[14] The purpose of section 11 is to protect certain economic and other interests of institutions. The exemption also recognizes that an institution's own commercially valuable information should be protected to the same extent as that of non-governmental organizations.[2]

[15] The board cited section 11(a) to withhold the TDSB audit, risk assessment, and security scan in their entirety. Section 11(a) reads:

> A head may refuse to disclose a record that contains,
>
> > (a) trade secrets or financial, commercial, scientific or technical information that belongs to an institution and has monetary value or potential monetary value.

[16] For section 11(a) to apply, the institution must show that the information:

1. is a trade secret, or financial, commercial, scientific or technical information,
2. belongs to an institution, and

[2] *Public Government for Private People: The Report of the Commission on Freedom of Information and Individual Privacy 1980*, vol. 2 (the Williams Commission Report) Toronto: Queen's Printer, 1980.

3. has monetary value or potential monetary value.

Part 1: Type of information

[17] The types of information listed in section 11(a) have been discussed in prior orders. In this case, the board submits that the TDSB audit, the risk assessment, and the security scan contain technical information as contemplated by section 11(a) of the *Act*.

[18] Previous IPC orders have defined technical information as follows:

> *Technical information* is information belonging to an organized field of knowledge in the applied sciences or mechanical arts. Examples of these fields include architecture, engineering or electronics. Technical information usually involves information prepared by a professional in the field, and describes the construction, operation or maintenance of a structure, process, equipment or thing.[3]

The board's representations

[19] The board provides descriptions of each of the three records in its representations. Specifically, the board describes the TDSB audit as an external audit of the board's use of Google Workspace for Education, the risk assessment as an internal risk assessment of the board's use of Google services, and the security scan as an external cybersecurity risk assessment of the board's use of Google Workspace.

[20] The board submits that these records provide detailed information about its Information Technology (IT) systems' interrelationship with Google Workspace for Education, and that this information is technical in nature as it clearly belongs to "an organized field of knowledge in the applied sciences or mechanical arts".

[21] The board cites Order MO-2070, in which "detailed information about the programming of the software and hardware required for the functioning of [election equipment] as well as descriptions of the method and process required to install that equipment" was found to qualify as technical information.[4] The board submits that this finding is applicable to the present appeal as the records at issue in this appeal similarly contain detailed sets of technical information about IT systems.

The appellant's representations

[22] The appellant does not directly dispute the board's characterization of the information as technical in nature. However, the appellant argues that any technical information in the records is likely already publicly available and therefore should be

[3] Order PO-2010.
[4] Order MO-2070.

disclosed.

[23] The appellant provides links to various Google resources on privacy and security and submits that these and other resources effectively make the technical information in the records publicly available. The appellant also submits that encryption standards, transmission protocols, and application programmer interfaces (APIs) are open source or public. Similarly, the appellant states that using developer mode in common web browsers will reveal the integration between the board and Google, which the board identifies as technical information.

[24] The appellant also submits that any technical information in the records is likely outdated, based on the board's assurances to parents regarding its IT and security practices. Relatedly, the appellant submits that any risks that the information in the records may reveal should have already been remedied, as the records are over one year old (at the time of his representations).

[25] Finally, the appellant argues that Order MO-2070 is distinguishable from the present appeal. The appellant argues that this appeal involves numerous parties and relationships including the board, Google, and the students. By contrast, the appellant argues that Order MO-2070 only involves two parties, namely the institution and the affected party.

Analysis and findings

[26] I have reviewed the TDSB audit, the risk assessment, and the security scan and accept that they contain technical information as defined above. I find that the TDSB audit and the security scan consist of external assessments of the board's use of Google Workspace for Education and Google Workspace respectively, including descriptions of existing settings, as well as findings and recommendations. The risk assessment contains discussion about the board's use of Google services, along with some conclusions and recommendations.

[27] I agree with the board that Order MO-2070 is relevant to this appeal. Specifically, I find that the records at issue in this appeal similarly contain information about software and IT systems that "[belong] to an organized field of knowledge that falls within the category of mechanical arts; specifically the field of information technology".[5] I do not agree with the appellant that Order MO-2070 and its findings about the type of information at issue is any less applicable because of the number or nature of the parties that the appellant identifies in this appeal.

[28] I also agree with and adopt the reasoning from Order MO-3175, in which information about the operation and maintenance of specific elements of an institution's IT system was found to meet the definition of "technical information" as contemplated in

[5] Order MO-2070.

section 11(a).[6] Based on the evidence before me, I find that the information at issue in this appeal was similarly prepared by professionals and describes the operation and maintenance of various aspects of the board's IT system and other products and services.

[29] The appellant submits that any technical information in the records is likely already public and or outdated. I note that this is not the test under this section. Additionally, I have reviewed the Google resources that the appellant links in his representations and do not agree that they effectively make the information in the records public. While there may be some overlap in the topics discussed in the Google resources and those that appear in the records at issue, I find that the TDSB audit, risk assessment, and security scan contain technical information that is more specific to the board and its systems.

[30] Accordingly, I find that the records contain "technical information" as contemplated by section 11(a) and part one of the test has been met.

Part 2: Belongs to

[31] The second part of the test for exemption under section 11(a) requires the institution to demonstrate that the information belongs to the institution.

[32] For information to "belong to" an institution, the institution must have some proprietary interest in it, either in a traditional intellectual property sense – such as copyright, trademark, patent or industrial design – or in the sense that the law would recognize a substantial interest in protecting the information from misappropriation by another party.

[33] Examples of information belonging to an institution include trade secrets, business-to-business mailing lists,[7] customer or supplier lists, price lists, or other types of confidential business information. In each of these examples, there is an inherent monetary value in the information to the organization resulting from the expenditure of money or the application of skill and effort to develop the information. Additionally, if the information is consistently treated in a confidential manner and its value to the institution comes from its not being generally known, a valid interest in protecting the confidential business information from misappropriation by others will be recognized.[8]

The board's representations

[34] The board submits that it has a proprietary interest in the TDSB audit, the risk assessment, and the security scan because its staff applied skill and effort in preparing the risk assessment and assisting in the preparation of the TDSB audit and the security

---

[6] Order MO-3175.
[7] Order P-636.
[8] Order PO-1763, upheld on judicial review in *Ontario Lottery and Gaming Corporation v. Ontario (Information and Privacy Commissioner)*, [2001] O.J. No. 2552 (Div. Ct.); see also Orders PO-1805, PO-2226 and PO-2632.

scan. In addition, the board submits that it expended money in paying the external parties that prepared the TDSB audit and the security scan.

[35] The board cites Order MO-2866 in support of the proposition that information in audits prepared by an external party for an institution can be considered to "belong to" the institution.[9] The board acknowledges that the information in Order MO-2866 was found to consist of financial and commercial rather than technical information, but submits that the type of information at issue does not change the analysis for ownership.

[36] The board submits that in Order MO-2866, the IPC found that since the information contained in the audits was treated confidentially by the institution and the third party, the information derives value by "not being generally known". The board argues that this is entirely analogous to the present case, as the board has kept the risk assessment confidential, and both the board and the external parties have consistently treated the information in the TDSB audit and the security scan in a confidential manner.

The appellant's representations

[37] The appellant's representations heavily reference the board's Freedom of Information and Protection of Privacy Policy (Policy P094), and specifically its definitions of "privacy" and "privacy impact assessment". The appellant submits that the policy defines privacy as "the right or interest of an individual to control the collection, use, and disclosure of their personal information" and clearly states that privacy is a fundamental right for citizens of Ontario. The appellant further states that the policy identifies a privacy impact assessment (PIA) as "a risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology, program, process or other activity may have on an individual's privacy".

[38] Based on these two definitions, the appellant makes a series of statements which I attempt to summarize here. First, the appellant states that the above definitions support the conclusion that an individual's personal information belongs to the individual, not the board. Second, the appellant submits that an essential part of any IT system is the data that it processes, which in this case belongs to the individual (here, the student), and not the board. Third, the appellant submits that an IT system is not only composed of hardware and software, but also the data (here, personal information) that it processes. Therefore, the appellant concludes that the IT system should be seen as a partnership between the board and its students, the latter of whom owns the data.

[39] Based on the above explanation, the appellant submits that because any PIA or risk assessment is done for the benefit of the partnership, these records and any information about privacy risk do not belong solely to the board. The appellant submits that while the board may have paid for internal and external audits of the IT system, this is not determinative as the system itself would not exist without student data. The

[9] Order MO-2866.

appellant argues that the purpose of the PIAs and risk assessments is not to test the hardware and software, but to evaluate the risk to students' personal information. The appellant submits that students have a real stake in the IT systems as it is their information that provides these systems with their value.

Analysis and findings

[40] As previously indicated, the test for deciding whether information "belongs to" an institution requires an examination of whether the institution has some proprietary interest in the information. Based on my review of the records, I conclude that the TDSB audit and the security scan belong to the board in the manner contemplated by section 11(a). Given my finding in part three about the monetary value of the risk assessment, I do not find it necessary for me to confirm whether the risk assessment belongs to the board for the purposes of this section.

[41] The board does not appear to argue that it has a proprietary interest in the records in a traditional intellectual property sense, such as copyright, trademark, patent, or industrial design. Therefore, in order to satisfy part two of the section 11(a) test, the board's proprietary interest must be in the sense that the law would recognize a substantial interest in protecting the information from misappropriation by another party.

[42] I accept the board's submission that it expended money in paying the external parties who prepared the TDSB audit and the security scan. In acknowledging that the board "may have physically paid for internal and external audits of the IT system", the appellant does not appear to dispute this, although he does not find it determinative.

[43] The board also submits that board employees applied skill and effort in assisting in the preparation of the TDSB audit and the security scan. While the board does not elaborate on the nature or extent of the skill and effort that was applied, or on the level of assistance provided, I have reviewed the records and accept that there was likely some application of skill and effort in preparing them.

[44] The board submits that in Order MO-2866, the IPC found that since the information was treated confidentially by the institution and the third party, the information derives value by "not being generally known". The board argues that this is analogous to the present case. The board submits that because it and the third parties similarly treated the information at issue in this appeal confidentially, the same finding should apply here.

[45] In summarizing Order MO-2866, the board appears to combine two distinct statements that the adjudicator makes. While the adjudicator concluded that the institution had a valid interest in protecting the information from misappropriation, this was based on her findings 1) that the information was consistently treated in a confidential manner and 2) that the information derives value to the institution from not being generally known. My interpretation of Order MO-2866 and previous IPC decisions is that these are considered separate statements, insofar as a finding of the former does

not necessitate a finding of the latter, as the board seems to suggest.

[46] I accept that the board and the third parties have treated the information in the TDSB audit and the security scan confidentially. However, for the reasons indicated above, I do not accept that this necessarily also means that the value of the information in the records to the institution comes from its not being generally known.

[47] Having said that, I have reviewed the records and find that in addition to being treated confidentially, the information in the TDSB audit and the security scan derives value to the board from not being generally known. I am satisfied that the information in both records is sufficiently detailed and specific to the board's IT systems that the law would recognize a substantial interest in protecting the information from misappropriation by another party.

[48] I have also considered the appellant's representations on this issue. I am not convinced that the appellant's characterization of the IT system as a "partnership" is relevant to a determination of whether the information in the records belongs to the board. I understand the appellant believes that because any PIA or risk assessment is done for the benefit of the "partnership", the records do not belong solely to the board. However, the appellant's analysis does not speak to the question of ownership as it is contemplated by this part of the section 11(a) test. For instance, the appellant does not rebut or provide alternatives to the board's representations regarding its expenditure of money or application of skill and effort to develop the information in the records.

[49] Therefore, while I have reviewed the appellant's proposed definition of an IT system and its constitutive elements, I find that this does not aid in my determination of whether information "belongs to" an institution under this part of the test. The appellant's more general argument, which is that students have an interest in the information at issue, is more appropriately discussed in the section on public interest under "Issue B".

[50] Accordingly, I find that the TDSB audit and the security scan belong to the board as contemplated by section 11(a). I do not find it necessary to determine whether the risk assessment belongs to the board given my conclusions in part three.

Part 3: Monetary value

[51] To have "monetary value", the information itself must have an intrinsic value. The purpose of this section is to permit an institution to refuse to disclose a record where disclosure would deprive the institution of the monetary value of the information.[10]

[52] The mere fact that the institution spent money to create the record does not mean it has monetary value for the purposes of this section.[11] Nor does the fact, on its own,

[10] Orders M-654 and PO-2226.
[11] Orders P-1281 and PO-2166.

that the institution has kept the information confidential.[12]

The board's representations

[53] The board argues that the TDSB audit, the risk assessment, and the security scan have intrinsic value beyond the fact that the board spent money commissioning the records and kept them confidential.

[54] The board states that in a sense, the value of the information is "negative", as the monetary value of the information lies in withholding it. The board submits that the information is not general information about IT systems in broad use, but particularized information about the board's IT systems. Given the level of detail in the records, the board argues that disclosure would be extremely costly and potentially dangerous.

[55] The board states that in Order MO-2866, the IPC found that the information at issue had monetary value because disclosing it would have a "direct cost" to the institution by giving bidders on the project an unfair advantage and possibly causing a delay in the project, which would require the institution to pay for other options in the interim.[13] Although the board also cites Order PO-2765, I do not consider it because its findings are made in connection with a different exemption. I note that the relevant test under that exemption is whether there is a "reasonable expectation of harm", whereas part three of the section 11(a) test requires the institution to demonstrate that the information has monetary value.

The appellant's representations

[56] The appellant submits that a value that is "negative", as the board describes, is one that has not been realized and that we cannot draw conclusions based on hypothetical events. The appellant also submits that the majority of the cost that would arise from a hypothetical breach would be associated with the students' data, which is not a cost that the board would bear.

[57] The appellant alleges that the board has publicly stated that it does not pay for Google services, including Google Workspace for Education. The appellant submits that the board is not entitled to claim that something is free and proceed to argue that it has monetary value. The appellant also submits that Google does not offer free services out of charity, but because there is inherent and significant value in the students' personal information. In the appellant's view, this supports his claim that personal information is a vital component of the board's IT systems.

[58] The appellant cites Privacy Complaint MC17-52, which involved a complaint against the board's use of Google's G Suite for Education services. Specifically, the appellant cites the board's statement that "it views Google as both a service provider and an agent of

[12] Order PO-2724.
[13] Order MO-2866.

the board".[14] On this basis, the appellant argues that the IT system contains contributions that are made by Google and therefore does not solely belong to the board.

Analysis and findings

[59] Based on my review of the records, I accept that the information in the TDSB audit and the security scan has monetary value. As previously indicated, I accept that the board expended money in paying the external parties that prepared the information, and that both the board and the third parties treated it confidentially. As this is not determinative, I also accept that the information in the TDSB audit and security scan is detailed and particularized to the extent that disclosure could result in a direct cost to the board.

[60] Previously, I found that that the TDSB and the security scan consist of external assessments of the board's use of various Google services, and that the records include descriptions of settings, as well as specific findings and recommendations. I accept that the disclosure of this information, which is relevant to the board's operations, could deprive the board of its monetary value.

[61] I do not reach the same conclusion regarding the risk assessment. Having reviewed both the board's representations and the record, there is not enough evidence for me to conclude that the information in the risk assessment has monetary value. In contrast with the TDSB audit and the security scan, I find that the information in the risk assessment consists largely of general statements, some of which are taken from or reference information in the public domain. Additionally, the risk assessment appears to contain information that dates back almost a decade, or longer. While it is possible for some information to retain its monetary value with the passage of time[15], I am not convinced that TDSB has provided sufficient evidence to demonstrate that the information in the risk assessment continues to have monetary value or potential monetary value.

[62] Turning to the appellant's representations, I do not agree that it is improper to draw conclusions based on hypothetical events. A discussion about the monetary value or potential monetary value of information may require some degree of speculation as to what might occur in the event of a hypothetical disclosure. I am also not convinced that the appellant's submissions on how or whether Google is being compensated affects my conclusions about whether the information in the specific records at issue has monetary value to the board.

[63] Accordingly, I find that the information in the TDSB audit and the security scan has monetary value as contemplated by section 11(a), and that the risk assessment does not. As a result, I find that the discretionary exemption at section 11(a) applies to the TDSB audit and the security scan, but not to the risk assessment, which I order disclosed.

---

[14] Privacy Complaint MC17-52.
[15] Order MO-3182.

Exercise of discretion

[64] The section 11(a) exemption is discretionary, and permits an institution to disclose information, despite the fact that it could withhold it. Having found that the TDSB audit and the security scan are exempt from disclosure under section 11(a), I must next determine if the board properly exercised its discretion in withholding the information. An institution must exercise its discretion. On appeal, the IPC may determine whether an institution has failed to do so.

[65] In its representations, the board references its historical practice of withholding PIAs and risk assessments. Additionally, the board indicated that it considered and weighed the applicable factors, including whether the appellant's request was one that would warrant disclosure, and concluded that the balance strongly favoured an exercise of discretion to withhold the records pursuant to section 11(a). The appellant's representations emphasize the compelling need for students and their legal guardians to have access to information about how their personal information is being used, as this is an important matter of safety and security.

[66] I have reviewed the parties' representations and find that the board properly exercised its discretion in withholding the TDSB audit and the security scan under section 11(a). I find that the board did not exercise its discretion to withhold the records in bad faith or for any improper purpose, and that there is no evidence that it failed to take relevant factors into account or considered irrelevant factors. Accordingly, I uphold the board's exercise of discretion in denying access to the TDSB audit and the security scan that I found to be exempt under section 11(a) of the *Act*.

Issue B: Is there a compelling public interest in disclosure of the records that clearly outweighs the purpose of the section 11(a) exemption?

[67] Section 16 of the *Act*, the "public interest override", provides for the disclosure of records that would otherwise be exempt under another section of the *Act*.

[68] Given my finding that the risk assessment is not exempt under section 11(a), it is not necessary to consider whether the public interest override applies to that record. However, I will now consider whether the public interest override applies to the TDSB audit and the security scan.

[69] Section 16 states:

> An exemption from disclosure of a record under sections 7, 9, 9.1, 10, **11**, 13 and 14 does not apply if a compelling public interest in the disclosure of the record clearly outweighs the purpose of the exemption.

[70] For section 16 to apply, two requirements must be met. First, there must be a compelling public interest in the disclosure of the records. Second, this interest must clearly outweigh the purpose of the exemption.

The board's representations

[71] The board submits that there is no compelling public interest in disclosing the records at issue. The board further submits that even if there were a compelling public interest, it would not clearly outweigh the purpose of the section 11(a) exemption. The board also submits that the onus of establishing that the public interest override applies rests on the appellant.

[72] The board cites Order MO-2456, which involved a request for audit reports relating to the institution's computer system. Specifically, the board refers to the adjudicator's finding that the disclosure of information relating to "technical aspects of the system in place to secure the [institution's] computers…would not shed further light on the operations of the [institution]".[16] The board submits that the same decision found that even if a compelling public interest in disclosure did exist, it does not clearly outweigh the institution's security interest. I note, however, that section 11(a) was not the relevant exemption in that decision and therefore any findings about whether or not the public interest outweighs the purpose of the exemption may not be relevant to this case.

[73] Nevertheless, the board submits that its interest is paramount, describing the economic damage that could result from disclosure as "catastrophic".

The appellant's representations

[74] The appellant submits that student safety is paramount and can only be achieved if all parties are informed. The appellant states that where it is clear that student information is being used, students and their legal guardians should have access to any relevant information about the security of their personal information. The appellant submits that it would be unjust to prevent students and their guardians from being informed about the security of their personal information. As such, the appellant argues that PIAs and risk assessments should be made public to this community of stakeholders.

[75] The appellant also submits that students and their guardians need to be able to hold the board accountable when it comes to protecting their personal information. The appellant states that it is important to know when an educational institution is not adequately protecting its students' information, and to be able to take action before a privacy breach occurs. The appellant reiterates that given the age of the records, any privacy risks that are identified within should already have been resolved. The appellant argues that if these privacy risks haven't been resolved, this information needs to be made public so that the board can be held accountable. The appellant submits that making this information public would be consistent with the board's statements about how student safety is a priority, as well as a partnership between parents and the board.

[76] The appellant indicates that he has considered the argument that bad actors may be able to take advantage of any privacy or security information that is made public.

---

[16] Order MO-2456.

Ultimately, the appellant concludes that the positive implications of disclosure would outweigh the negative ones. The appellant submits that because bad actors already know how to exploit the vulnerabilities in Google's system, they would not gain anything from disclosure. However, disclosure would allow the public to be informed and to hold the board accountable. The appellant submits that this is important given the number of major privacy breaches that have been reported by institutions that collect personal information, often without proper consent and with minimal oversight.

[77] The appellant submits that if the board had voluntarily disclosed this information, then this request and appeal would likely not have been required. However, the appellant states that this is currently the only way to get information about the safety and security of students' personal information. The appellant also comments that Canadian society at large is moving toward enabling citizens to better understand how their personal information is being used, including by supporting greater disclosure.

[78] The appellant subsequently provided additional comments regarding this appeal. First, the appellant cites Privacy Complaint PI21-00001, in which there was a reference to another educational institution's disclosure of a Privacy & Information Security Assessment Report. The appellant states that this is proof that educational institutions are releasing PIAs to the public and submits that the board should be following this as a best practice.

[79] Second, the appellant notes that the board reported a cyber incident earlier this year. The appellant submits that if the information at issue was released when it was first requested, the cyber incident may have been avoided. The appellant reiterates that bad actors already know how to access the IT system, and therefore it is imperative that students and guardians have the relevant information about the security of their personal information.

Analysis and findings

[80] The *Act* is silent as to who bears the burden of proof in respect of section 16. This onus cannot be absolute in the case of an appellant who has not had the benefit of reviewing the requested records before making submissions in support of their contention that section 16 applies. To find otherwise would be to impose an onus which could seldom if ever be met by an appellant. Accordingly, the IPC will review the records with a view to determining whether there could be a compelling public interest in disclosure that clearly outweighs the purpose of the exemption.[17]

[81] In considering whether there is a "public interest" in disclosure of the record, the first question to ask is whether there is a relationship between the record and the *Act*'s central purpose of shedding light on the operations of government.[18] In previous orders, the IPC has stated that in order to find a compelling public interest in disclosure, the

[17] Order P-244.
[18] Orders P-984 and PO-2607.

information in the record must serve the purpose of informing or enlightening the citizenry about the activities of their government or its agencies, adding in some way to the information the public has to make effective use of the means of expressing public opinion or to make political choices.[19]

[82] The IPC has defined the word "compelling" as "rousing strong interest or attention".[20]

[83] The IPC must also consider any public interest in **not** disclosing the record.[21] A public interest in the non-disclosure of the record may bring the public interest in disclosure below the threshold of "compelling."[22]

[84] The board cites Order MO-2456, in which the adjudicator found that the disclosure of information relating to "technical aspects of the system in place to secure the [institution's] computers…would not shed further light on the operations of the [institution]". On its face, this seems to be directly relevant to the present appeal. However, I have reviewed Order MO-2456 and find that there are some important distinctions between that decision and the present case.

[85] First, I have already discussed the fact that the information in Order MO-2456 was withheld under a different exemption. As a result, whether or not the public interest is found to outweigh the purpose of the exemption in that case is not necessarily relevant here. Second, the institution in Order MO-2456 did not withhold the records in full. In her discussion of the public interest override, the adjudicator explicitly took into consideration the portions of the reports that the institution was prepared to release to the appellant. Previous IPC decisions have similarly found that a significant factor to be considered when deciding whether the public interest override applies is the degree of public disclosure that has already taken place.[23]

[86] The appellant emphasizes that there is a compelling public interest in subjecting the board's use of Google services to increased public scrutiny. Given the increasing prevalence of technological solutions within schools and the importance of privacy, which is recognized by both parties, I am willing to accept that there may be a public interest in information about the board's IT systems, and particularly any risks to the board's students, staff, and community members. In my view, any recent incidents increase the likelihood that a public interest may be found.

[87] However, I am not convinced that the public interest in this case is "compelling". First, while I do not doubt that the disclosure of the TDSB audit and the security scan rouses the appellant's strong interest or attention, I do not have enough evidence to

---

[19] Orders P-984 and PO-2556.
[20] Order P-984.
[21] *Ontario Hydro v. Mitchinson,* [1996] O.J. No. 4636 (Div. Ct.).
[22] Orders PO-2072-F, PO-2098-R and PO-3197.
[23] Order M-381, MO-3990.

conclude that this interest or attention is shared by other members of the public, particularly given the technical nature of the records. Second, while the appellant concludes that the positive implications of disclosure would outweigh the negative ones, I am required to consider any public interest in non-disclosure. In my view, the possibility that technical information in the records could be exploited gives rise to some public interest in non-disclosure. I find that both of these factors lower the public interest to below the threshold of "compelling".

[88] Even if I were to accept that there was a compelling public interest in the disclosure of the records at issue, I am not convinced that this interest clearly outweighs the purpose of the section 11(a) exemption. I previously found that the TDSB audit and the security scan contain information which, if disclosed, could result in a direct cost to the board and deprive the information of its monetary value. I find that the appellant has not advanced sufficient evidence to demonstrate that any compelling public interest in disclosure of the specific information in the TDSB audit and the security scan would outweigh the purpose of the section 11(a) exemption to protect the board's economic interests.

[89] Accordingly, I find that the appellant has not established a compelling public interest in disclosure that would outweigh the purpose of the section 11(a) exemption. Therefore, I uphold the board's decision to deny access to the TDSB audit and the security scan.

ADDITIONAL ISSUES

[90] In its representations, the board states that records 6 and 7[24] may contain third party information as defined in section 10(1) of the *Act*. The board submits that it did not notify the affected parties because it denied access to the records. However, if the IPC decides that section 11(a) does not apply, the board submits that any affected parties should be notified and advised of their right to raise section 10(1).

[91] As I have upheld the board's decision with regard to the TDSB audit and the security scan, I do not find it necessary to consider the question of notification in relation to those records.

ORDER:

1. I order the board to disclose the risk assessment (record 4) to the appellant by **February 5, 2025**.

[24] I note that there are no records 6 and 7 in this appeal. I assume the board is referring to the records responsive to parts 6 and 7 of the request.

2. I uphold the board's decision to deny access to the TDSB audit and the security scan pursuant to section 11(a) of the *Act*.

3. In order to verify compliance with order provision 1, I reserve the right to require the board to provide me with a copy of the record disclosed to the appellant.

Original Signed by: January 6, 2025

Anda Wang
Adjudicator