Information and Privacy
Commissioner/Ontario
Commissaire à l'information
et à la protection de la vie privée/Ontario

ORDER MO-1822

Appeal MA-030150-1

Limestone District School Board

Tribunal Service Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Sevices de tribunal administratif
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9188
TTY: 416-325-7539
http://www.ipc.on.ca

NATURE OF THE APPEAL:

This appeal concerns a decision of the Limestone District School Board (the Board) made pursuant to the provisions of the *Municipal Freedom of Information and Protection of Privacy Act* (the *Act*). The requester (now the appellant) had sought access to records containing generic data in the following categories, for students attending a Board school who had completed and received a final mark for the most recent three semesters: number of absences by category, school, common course code, credit value, gender, course description, and final mark for each course. He also requested the two most recent year-end statistical reports delivered to the Information and Privacy Commissioner/Ontario (IPC).

The appellant subsequently amended his request to also include the name, model, version and brief description of the database server currently used by the Board for student record management and how it is networked, and the name, version and brief description of the software used to input data and generate reports from the database. He also amended the scope of his request to data for the most recent semester.

The Board provided copies of the year-end statistical reports delivered to the IPC and denied access to the detailed computer information pursuant to sections 13 and 14 of the *Act*. Regarding the generic data requested, the Board claimed that this information was not currently available but could be made available through the creation of computer programs and extensive work to collect and compile these records.

The Board provided the appellant with two fee estimate options regarding the requested data. The appellant chose to work with the first estimate. The appellant appealed this estimate and the decision relating to the detailed computer information.

During the mediation stage, the issue of the fee was resolved. The appellant was, subsequently, provided with information responsive to his request for generic data for the most recent school semester. However, the Board continued to deny access to the detailed computer information (the names of two servers, the names of four software applications and the version number for a database application), pursuant to sections 13 and 14 of the *Act*. This issue was moved to adjudication.

I first sent a Notice of Inquiry to the Board seeking representations. The Board created a record containing the detailed computer information. The Board's position is that all of the information contained in this document is exempt under sections 13 and 14. The Board acknowledges that the appellant did have a discussion with Board staff during the mediation stage in order to help him narrow another request he had with the Board for information contained in its computer systems. The Board states that as a result of that discussion the appellant became aware of the two software applications that the Board uses for its databases. However, the Board maintains that it has not formally provided the appellant with any "written records". Accordingly, the Board maintains that all of the information contained in the record is at issue. Under the circumstances, I will conduct my inquiry on the basis that none of the information contained in the record has been disclosed under the *Act*, and all of it is at issue.

The Board also submitted representations on the application of sections 13 and 14 and agreed to share them in their entirety with the appellant. I then sought representations from the appellant and included with a Notice of Inquiry a copy of the Board's representations. The appellant submitted representations in response. I shared the appellant's representations with the Board and sought and received reply representations from it.

RECORDS:

There is one record at issue, a one-page document describing the Board's computer systems.

DISCUSSION:

As indicated above, the Board has claimed the application of both sections 13 and 14 to the information at issue. I will first deal with section 14.

PERSONAL INFORMATION

The exemption under section 14 applies only to information that qualifies as "personal information", as defined under section 2(1) of the *Act*. "Personal information" is defined, in part, to mean recorded information about an identifiable individual, including any identifying number assigned to the individual [paragraph (c)], the individual's address [paragraph (d)] and the individual's name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual [paragraph (h)].

To qualify as personal information, it must be reasonable to expect that an individual may be identified from the information [Order PO-1880, upheld on judicial review in *Ontario (Attorney General) v. Pascoe*, [2002] O.J. No. 4300 (C.A.)].

The Board submits:

> While a list of hardware/software does not, per se, include direct personal information, it provides the capacity to gain access to extensive personal information about all [of the Board's] students. It is analogous to a safe in which valuable information is stored - the combination or key to that safe is not in itself "personal information" but rather the means to access it.

The Board states that its "computer systems" contain "extensive personal information" about its students, including "name, school, address, parent/guardian, academic progress [and] attendance…"

The Board also includes a report of its Manager of Information Technology Services, which states, in part:

> Detailed information about software applications utilized and hardware installed is commonly used by hackers to break into computer systems. If a hacker knows what applications are in use and the hardware utilized, it will provide considerable information about security vulnerabilities. Hackers target the known vulnerabilities in specific hardware or software systems.
>
> Making detailed information […] about our systems available publicly greatly increases the risk that our information technology systems will be compromised. These systems are used to access, manipulate, and store very confidential information […] about both students and staff.

In response, the appellant states that the Board's safe analogy is "exaggerated". In support of this view, he states:

> The passwords used by various users to access the database are more analogous to the combination or key to the safe. The model number of the safe is more analogous to the version number [of the software].
>
> Having the model number would allow someone to look up a description of the safe and see how safe it is – the description would not tell you how to crack the safe.

In reply, the Board states:

> Knowing the specific software and version number used will not only tell you how "safe" or secure the system is but it will also tell you how to "crack" it.
>
> Security information about software isn't made available in the form of generic "this system can be compromised" message – it is provided in the form of "this system can be compromised because of xxx". For example, a security bulletin release for Microsoft SQL Server 2000 (a database server) is titled "SQL Query Method Enables Cached Administrator Connection to be Reused" (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/Bulletin/MS01-032.asp). To continue with the "safe" analogy, a similar security release for a floor safe may be "Thin floor of safe makes safe vulnerable from below".

This situation is unusual. On the one hand, the information at issue does not on its face contain information about an identifiable individual. On the other hand, there does not appear to be any dispute that the information in the Board's database contains the personal information of students of the Board (such as, student name, school, address, parent/guardian, academic progress and

attendance record). As a result, anyone who gains access to the information in the database would have access to the personal information of the Board's students.

As stated above, in order for information to qualify as personal information it must be "reasonable" to expect that an individual may be identified from the information. I find that the Board has not met this onus.

The Board's evidence suggests that the information at issue provides the "capacity" to gain access to extensive personal information. The Board then compares the information at issue to a safe, with the key or combination to the safe not personal information but the means to access it. The Board also suggests that knowing the specific software and version number will not only tell you how "safe" or secure the system is but how to "crack" it.

In my view, the Board's safe analogy is speculative at best. I am not convinced that by revealing this information it would be reasonable to expect that an individual may be identified as a result of its disclosure.

In addition, the evidence of the Board's Manager of Information Technology Services amounts to generalized assertions regarding the use of this kind of information by hackers to break into computer systems. The Board has provided no evidence of frequency of "hacking" into similar database systems. The Board has made no comment on the extent to which its computer systems are susceptible to hacking if this information was to be released. The Board has provided no evidence from internal or external technical experts regarding the specific vulnerabilities of its database software and computer hardware should this information be disclosed.

Accordingly, I am not prepared to find that the information at issue qualifies as personal information under section 2(1) of the *Act*. Having reached this finding I cannot consider the application of section 14 personal privacy exemption.

I will now consider the application of section 13 to the information at issue.

THREAT TO SAFETY OR HEALTH

Section 13 states:

> A head may refuse to disclose a record whose disclosure could reasonably be expected to seriously threaten the safety or health of an individual.

For this exemption to apply, the Board must demonstrate that disclosure of the record "could reasonably be expected to" lead to the specified result. To meet this test, the Board must provide evidence to establish a reasonable basis for believing that endangerment could result from disclosure. In other words, the Board must demonstrate that the reasons for resisting disclosure are not frivolous or exaggerated [see *Ontario (Information and Privacy Commissioner, Inquiry Officer) v. Ontario (Minister of Labour, Office of the Worker Advisor)* (1999), 46 O.R. (3d) 395 (C.A.)].

An individual's subjective fear, while relevant, may not be sufficient to establish the application of the exemption [Order PO-2003].

The term "individual" is not necessarily confined to a particular identified individual, and may include any member of an identifiable group or organization [Order PO-1817-R].

The Board's submissions are similar to those it has provided above in connection with section 14. The Board argues that access to its hardware/software configurations compromises the security of its computer systems, relying upon the evidence of its Manager of Information Technology Services set out above. The Board states that if an individual had the capacity to hack into its computer systems that individual would have access to extensive personal information about its students, including name, school, address, parent/guardian, academic progress and attendance. The Board suggests that there are a number of students who are at risk if people who are estranged from them identify their location. While acknowledging that an individual request for information about its computer systems is likely to be for legitimate, non-threatening purposes, it has the right to determine the level of risk posed by individual appellants. Finally, the Board argues that disclosure of this information would set a precedent. The Board argues that the practice within Canada is to keep information about information technology systems confidential. The Board cites the Canadian banking system, the Canadian university and college environment and commercial organizations and businesses as examples in support of this statement.

The appellant submits that the Board's rationale against disclosure is exaggerated. He argues that if the Board's computer system can be compromised by the disclosure of software version numbers then the other layers of security, including passwords at each layer of access, would be redundant. In response to the Board's assertion that it is the practice within Canada to keep information regarding information technology systems confidential, the appellant provides three examples where public institutions have released over the internet the version numbers for their data management applications. I note that of the three examples one is an American public school board, another is an Ontario Catholic school board and the third concerns the computer system for an airport terminal in an Ontario city. Taking issue with the evidence of the Board's Manager of Information Technology Services, the appellant states that he was able to find version references for a number of the Board's other applications and software that he presumes can be used to access sensitive and personal information.

In reply, the Board comments on two of the appellant's assertions. Firstly, the Board disputes the appellant's contention that providing the database version numbers does not pose a security risk because they are protected by multiple layers of passwords. The Board suggests that the appellant's position is similar to saying that a house is protected from burglars because it has a very strong front door and lock, ignoring the vulnerabilities elsewhere. The Board submits that vulnerabilities can be exploited to get around built-in password protections. Therefore, new software versions are released to address these vulnerabilities as they arise. Secondly, the Board addresses the appellant's suggestion that it is breaking its own policy regarding the non-disclosure of information technology systems information by making available the version

numbers for a number of other applications and software. The Board distinguishes these systems form the information at issue since they are not used to store sensitive or personal information.

The Board also believes it has the right to determine the level of risk posed by individuals seeking information. It would appear that the Board determined in this case that it did not feel comfortable releasing the information at issue to the appellant for security reasons. I also note that the Board is of the view that it is the practice throughout Canada to keep information about information technology systems confidential. The appellant has commented on the Board's representations and the Board was given an opportunity to reply.

To be successful under section 13, the Board must demonstrate that disclosure of the record "could reasonably be expected to" seriously threaten the safety or health of an individual. The Board must provide a reasonable basis for believing that endangerment could result from disclosure.

In my view, the Board has offered vague and generalized statements about the impact that disclosure of the information at issue would have on the security of its computer systems and, in turn, its students. I acknowledge that the Board is concerned that this information could be used by people with bad intentions to identify and harm students who may be vulnerable. However, I find the Board's arguments remote and hypothetical. They lack sufficient detail to establish a reasonable basis for believing that disclosure of the information in this record could reasonably be expected to seriously threaten the safety or health of an individual. Accordingly, I find that section 13 does not apply.

ORDER:

I order the Board to disclose the entire contents of the record to the appellant by **September 30, 2004** but not before **September 25, 2004**.

Original Signed by: August 27, 2004
Bernard Morrow
Adjudicator