February 27, 2009 **P-2009-001**

NEWFOUNDLAND AND LABRADOR

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

REPORT P-2009-001

Eastern School District

Summary: On 3 November 2008 Eastern School District ("ESD") notified this Office that a break-in had occurred at a teacher's home and the teacher's laptop computer containing the personal information of 79 students had been stolen. The information consisted of student names, addresses, phone numbers and grades. The teacher had taken the information from the school on an encrypted USB drive and it was subsequently "backed up" on the laptop's hard drive, without ESD's knowledge. The teacher failed to realize the necessity of working directly from the encrypted USB drive in order to keep the information secure. The Commissioner found that section 36 of the *Access to Information and Protection of Privacy Act* (the "*ATIPPA*") had been breached, as ESD had not taken proper administrative measures to protect the personal information in its custody or control. ESD has now distributed a brochure to all users of encrypted USB drives, clarifying the use and the role of these USB drives in protecting personal information. The Commissioner made no recommendations, as he found that this action satisfied section 36 of the *ATIPPA* in this case.

Statutes Cited: *Access to Information and Protection of Privacy Act*, S.N.L. 2002 c. A-1.1, as am., ss. 36 and 39.

Authorities Cited: Newfoundland and Labrador OIPC Report P-2008-002.

Other Resources: *Key Steps When Responding to a Privacy Breach*, ATIPP Office, Department of Justice, Government of Newfoundland and Labrador http://www.justice.gov.nl.ca/just/civil/atipp/ .

I BACKGROUND

[1] On 3 November 2008 this Office was contacted by officials from Eastern School District ("ESD") who notified us that a break-in had occurred at a teacher's home and a laptop computer belonging to the teacher containing the personal information of 79 students had been stolen. The information consisted of student names, addresses, phone numbers and grades. The teacher had taken the information from the school on an encrypted USB drive and it was subsequently "backed up" (saved) on the laptop's hard drive, without ESD's knowledge. ESD asked this Office to carry out an investigation with respect to whether there had been a privacy breach (a breach of any of the sections of Part IV of the *ATIPPA*).

[2] The information was taken home by the teacher for the purpose of entering student grades into the computer system. Briefly, the process of entering grades is completed as follows. WinSchool (the database used by ESD to store all student information) has a utility that enables export to a particular teacher of small subsets of information (i.e. a class list containing student names, addresses, and phone numbers), along with pre-determined entry fields for grades. This process is referred to as "writing teacher's classes" and produces a standard data set, with no option to delete specific fields (i.e. addresses and phone numbers, which ESD acknowledges are not necessary for grade entry). eClass is companion software to WinSchool, and allows teachers to open this subset of data using eClass and enter grades and coded comments for each student. The teacher only sees his or her own classes/courses and students. Once this information is entered into eClass by a teacher, WinSchool imports the information from eClass back to the main WinSchool database from which report cards are printed. Installing eClass on a computer does not mean that personal information is saved to that computer. Until the process of "writing teacher's classes" is completed, eClass contains no student information. This process can only be initiated by a school administrator or the administrative assistant.

[3] In this case, the process of "writing teacher's classes" was completed, saved to an encrypted USB drive and the USB drive was taken home so the teacher could complete the grade entering process at home. Unfortunately, the teacher backed up the information on the hard drive of the laptop. Having done so, if eClass was now opened on the stolen laptop, it would contain a table

of student names, addresses, phone numbers and grades that is easily readable. As eClass does not have password protection capability, the program is easily opened with the click of a mouse, much like Microsoft Word.

II DISCUSSION

Response to Breach and Security Measures in Place

[4] According to the Department of Justice ATIPP Office document entitled "Key Steps When Responding to a Privacy Breach," it is clear that ESD correctly identified and applied the appropriate framework within which to approach this situation. The steps, as outlined in this document are as follows:

- Contain the breach
- Evaluate the risks
- Notification
- Prevention.

[5] Containing the breach is not possible as the computer has not been recovered. It is unknown whether this information has been accessed. ESD advises that while the computer was password protected, there were no additional security measures installed on the computer. As noted, this was a personal laptop belonging to a teacher; it was not the property of ESD.

[6] The second step in responding to a privacy breach is to evaluate the risks, including: the type of personal information involved; the cause and extent of the breach; the individuals affected by the breach; and foreseeable harm resulting from the breach. This is necessary in order to determine what other steps are immediately required and what precautions should be taken in order to minimize, as much as possible, the chance of another breach occurring. As noted in previous privacy reports, names, addresses and phone numbers could be used for illicit purposes in the hands of the wrong person. ESD, in its Privacy Breach Reporting Form (which is designed

to evaluate the risks), also acknowledged the possibility of identity theft. Fortunately, a relatively small number of people were affected.

[7] The third step in responding to a privacy breach is notification and this is directly related to the evaluation of the risks. This evaluation assists in determining whether notification is necessary, and if so, how it should be done and what information it should contain. The more sensitive the information, the importance of notification increases and the manner in which it is done becomes more important. Once those individuals whose personal information is involved in the breach are aware of the breach and what information was potentially or actually exposed, they, along with the public body, can take appropriate steps to mitigate any potential risks associated with the information being disclosed.

[8] I believe that ESD acted appropriately in notifying the parents or guardians of all the children whose personal information was contained on the computer. It is also my opinion that ESD chose effective means (letters sent home with all children) to do so, and did so in a timely manner.

[9] The fourth step in responding to a privacy breach is prevention. The cause of the breach must be thoroughly investigated, and safeguards and policies must be created or updated and implemented to minimize, as much as possible, the risk of another breach occurring. In this case, the breach occurred when the personal information was saved to the laptop and the laptop was stolen from the teacher's home.

[10] It is not possible to determine whether the information contained on the computer was accessed. While the computer was password protected, passwords can be easily bypassed. Further, the program that contained the information (eClass) is not password protected, as there are no password controls built into the program. While it may be likely that the laptop was stolen for its "street" value and not for the information it contains, it is impossible to conclude that this is the case and that no files were accessed by the thief. Given the ease with which the personal information could be accessed, this is a real possibility.

[11] Section 36 of the *ATIPPA* states as follows:

> *36. The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.*

[12] As discussed in Report P-2008-002, "reasonable security arrangements" consists of a multi-layered approach to security, which encompasses technical, physical and administrative safeguards. While ESD had provided encrypted USB drives to all schools, as noted, the stolen laptop is not the property of ESD. While physical and technical security measures (beyond the provision of the USB drives) are outside the control of ESD in this case, administrative safeguards are extremely important, and are most definitely within ESD's control. If it is necessary for teachers to complete work that involves the personal information of students at home, it is imperative that effective policies and procedures be in place and effectively communicated to teachers. This is where ESD's responsibility lies with respect to section 36 of the *ATIPPA* in this case.

[13] At the time of the breach, ESD's schools had been informed that no personal data was to be taken from the school unless utilizing encrypted media and ESD had already conducted a needs assessment and supplied schools with encrypted USB drives so that personal information could be safely transported from school to other locations as necessary. School administrators had been trained with respect to access to information and protection of privacy issues, and were aware that they are the main individuals to ensure compliance with the *ATIPPA.*

Sufficiency of New Security Measures - Requirements under the *ATIPPA*

[14] Since the breach, ESD has become aware of shortcomings in the information given to schools around encryption and work practices. Some people misunderstood the role of the encrypted USB drive or did not realize that the information became unencrypted when it was taken off the USB drive; others did not realize there was a need to alter the past practice of working from one's own computer, instead of directly from the USB drive. As a result of this,

ESD contacted every principal within the district to inform them of the breach so they could create awareness among staff. ESD also developed a brochure to give to individuals as a companion to the encrypted USB drive, detailing its role and how it should be used to best secure information. Among other things, this brochure clears up the misconceptions and specifically states that one should work directly from the USB drive instead of copying files to a computer.

[15] As discussed in Report P-2008-002, what amounts to "reasonable security arrangements" under section 36 of the *ATIPPA* will vary depending on the circumstances and reasonableness must be measured on an objective basis. An assessment of the reasonableness of security measures includes the following factors:

1. The foreseeability of the privacy breach
2. The seriousness of potential harm (discussed above)
3. The cost of preventative measures
4. Relevant standards of practice

1. Foreseeability of the Privacy Breach

[16] As discussed in Report P-2008-002, thefts of laptop computers are very common, and thus foreseeable. However, the question in this case is whether the breach was foreseeable. I must determine whether it was foreseeable by ESD that a teacher would back up files containing personal information on his/her personal laptop, thus leaving the data vulnerable to unauthorized access. In the aftermath of prior privacy breaches, ESD has certainly increased its efforts to protect the personal information in its custody or control. It has undertaken ATIPP training with all school administrators and sent out a directive to ESD district office employees prohibiting the storage of personal information on ESD owned laptops, as well as adding three layers of password security and encryption technology to ESD owned laptops. Encrypted USB drives were also purchased and distributed to schools in order to secure information that had to be transported from location to location.

[17] However, while the encrypted USB drives were provided to schools, it is my understanding that no "directions" or explanations accompanied the USB drives when they were distributed to teachers. There was also no clear direction with respect to not saving personal information of students on personal computers. Encryption technology may not be familiar to everyone. In fact, it is only fairly recently, as we become more and more aware of data theft and privacy breaches, that this technology has gained mass popularity. It is not unreasonable to assume that some people (teachers included) still may not have a complete understanding of the way it works.

[18] Further, others may not appreciate that encrypted USB drives serve a broader purpose than just protecting information while "in transit". If information is to remain protected, one must work from the encrypted USB drive and only save information on it and not back it up on the hard drive of a home computer. This is exactly the situation we are dealing with in this case. The teacher did not realize that it was now necessary to cease the practice of backing up files on the hard drive of his/her home computer. By saving the information on the hard drive, the whole purpose of having an encrypted USB drive was defeated, and the information was vulnerable to unauthorized access, whether intentional or accidental. ESD should have provided teachers with some sort of explanation with respect to the need for and the use of encrypted USB drives when they were initially provided. ESD has now done just that with the brochure mentioned above which has already been distributed.

[19] Given the vast differences in technical knowledge from person to person, I am of the opinion that misuse or misunderstanding of the role of the encrypted USB drives was likely, thus resulting in a privacy breach. This leads me to the conclusion that, given all the circumstances, a breach was foreseeable.

2. Seriousness of Potential Harm

[20] As mentioned in paragraph 6, this type of information could be used for illicit purposes if someone was inclined to do so.

3. Cost of Preventative Measures

[21] In this case, the cost of preventative measures is minimal, and essentially involves developing, implementing and effectively distributing a directive that clearly articulates how personal information must be protected when working from home.

[22] Technical and physical safeguards, beyond the provision of encrypted USB drives for transporting information, are outside of ESD's control in this case. The laptop was a personal laptop and it was stolen from a teacher's home, along with other electronics.

4. Relevant Standards of Practice

[23] Again, given the circumstances of this case, relevant standards of practice are of minimal use. With respect to securing personal information kept on ESD premises and laptop computers owned by ESD, all the appropriate measures have been taken (see Report P-2008-002). While ESD and its employees are responsible for the protection of personal information in its custody and control, ESD cannot dictate to individuals the type of security that should be installed on their personal computer or within their homes. That would not be a "reasonable security measure" as contemplated by section 36 of the *ATIPPA*. However, there are certainly administrative measures that ESD could take; one of which would be to prohibit employees from taking personal information home. If this is not possible, ESD must ensure that employees are aware of the risks and implement directives to minimize the likelihood of breaches. ESD thought it had done this, however, this breach identified shortcomings in the directives that were issued.

[24] ESD has now sought to rectify this issue by producing a clearly written and user-friendly brochure that will accompany the encrypted USB drives that are distributed to teachers. As noted, this brochure clearly states that one must work directly off the encrypted USB drive and also that data back-ups should be done to "encrypted media, to a network drive at school, or uploaded to FirstClass from home." The brochure also makes it clear that personal information is not to be stored on unencrypted portable devices.

III CONCLUSION

[25] While a multi-layered approach to information security is necessary, in this case, ESD's ability to put in place technical and physical measures for information protection were limited in scope, with the exception of the provision of encrypted USB drives, which it had already done. However, ESD's obligation with respect to administrative measures remains. The best way to prevent a breach of this nature from occurring again is to prohibit employees from taking personal information home. However, if that is not an option, it is my finding that a further "reasonable security measure" would involve provision of encrypted USB drives along with the necessary information regarding the need for encrypted USB drives and how they should be used. By failing to provide this explanation when the USB drives were initially provided, ESD failed to make "reasonable security arrangements" to protect the personal information in its control. Therefore, I find that there was breach of section 36 of the *ATIPPA.*

[26] As discussed, ESD has now provided the necessary explanation and information to users of the encrypted USB drives. It is my opinion that such a measure meets the requirements of section 36 in this case, and thus, I have no recommendations to make.

[27] Dated at St. John's, in the Province of Newfoundland and Labrador, this 27th day of February, 2009.

E. P. Ring
Information and Privacy Commissioner
Newfoundland and Labrador