



NEWS RELEASE

For immediate release

October 12, 2017

Commissioner's investigation determines inadequate video surveillance controls put student information at risk

HALIFAX - Inadequate passwords and insufficient technical controls led to video surveillance images of schoolchildren being live streamed on the internet, says Catherine Tully, Nova Scotia's Information and Privacy Commissioner, in a new report issued today.

In May 2017, the Office of the Information and Privacy Commissioner (OIPC) began investigating a breach of personal information from the Rankin School of the Narrows in Iona, Nova Scotia. The breach resulted when a link to the live feed from one school camera was picked up and distributed by a Russian website that specializes in linking non-secured video surveillance cameras. An unsecured technical vulnerability enabled viewers to access the school's other two cameras as well.

"If video surveillance is used, it must be properly secured," Tully said. "When video surveillance images from the Rankin School were streamed on the internet for all to see, this was a violation of Nova Scotia's privacy laws. Video surveillance images of schoolchildren streaming unsecured to the internet created a risk to student safety."

The report noted that the Cape Breton-Victoria Regional School Board (Board) changed the passwords on all its video surveillance cameras once it learned of the privacy breach. However, the Commissioner found that the Board has not yet implemented adequate technical or administrative controls to reduce the risk of future privacy breaches.

Commissioner Tully recommended several changes to the Board's technical security practices to strengthen controls on its protection of personal information.

In addition to the security failures, the report also considered the Board's rationale for the installation and use of video surveillance. Commissioner Tully found that the Board had not established that its video surveillance is legally authorized under the *Freedom of Information and Protection of Privacy Act (FOIPOP)*. Like all school boards in Nova Scotia, it implemented video surveillance without first conducting a privacy impact assessment to ensure compliance with *FOIPOP*.

"As video surveillance tools have gotten cheaper and easier to use, school boards across Nova Scotia have installed them, citing the need to ensure the safety of the children," said Tully.

"There is no question that the safety of our children is of fundamental importance. Yet video



surveillance is highly privacy invasive. It is essential that school boards conduct a thorough privacy impact assessment of their video surveillance systems in order to find the proper balance between ensuring the safety of children while respecting their privacy.”

Commissioner Tully was pleased to note that every school board in Nova Scotia, except the Cape Breton-Victoria Regional School Board, has voluntarily agreed to participate in a privacy impact assessment workshop facilitated by the OIPC.

Commissioner Tully made six recommendations to the Board:

1. That the Board develop its own privacy breach policy.
2. That the Board further secure its cameras either behind a firewall or by another equivalent technical strategy.
3. That the Board replace its two exterior cameras which are no longer supported by the manufacturer once it has completed a privacy impact assessment.
4. That the Board update its policies and practices to include privacy training, updated confidentiality agreements, mandatory audits of video surveillance, a Board specific breach policy and a password policy.
5. That the Board immediately disable the video surveillance camera outside of the boys’ washroom at Rankin School.
6. That the Board conduct a privacy impact assessment of its video surveillance system and provide the OIPC with a copy.

The Board has 30 days to respond to the Commissioner’s recommendations.

-30-

For more information, contact:

Catherine Tully
Information and Privacy Commissioner for Nova Scotia
Phone: 902-424-4684
Email: oipcns@novascotia.ca
Twitter: [@NSInfoPrivacy](https://twitter.com/NSInfoPrivacy)

