Student loan data on half a million people was left unsecured: watchdog

Employees handling the device were not aware of the sensitivity of the information it contained, concludes the report from interim privacy commissioner Chantal Bernier. (file image)

By Jim Bronskill, The Canadian Press
Published Tuesday, March 25, 2014 10:26AM CST
Last Updated Tuesday, March 25, 2014 4:42PM CST

OTTAWA -- A portable hard drive containing personal information on more than half a million people who took out student loans was left unsecured for extended periods and lacked password protection and encryption, says the federal privacy czar.

Employees handling the device were not aware of the sensitivity of the information it contained, concludes a report from interim privacy commissioner Chantal Bernier.

Human Resources and Skills Development Canada acknowledged last year the drive held data on 583,000 Canada Student Loans Program borrowers from 2000 to 2006.

The missing files included student names, social insurance numbers, dates of birth, contact information and loan balances, as well as the personal contact information of 250 department employees.

Bernier's report, tabled Tuesday in Parliament, reveals that other details -- including a borrower's gender, language or marital status -- may also have been compromised.

A gap between policies and practices at the department -- now known as Employment and Social Development Canada -- led to weaknesses in information management, physical security controls and employee awareness, the report says.

The commissioner found that department employees violated sections of the federal Privacy Act related to the use, disposal and disclosure of personal information.

Information security cannot be assured by having policies on paper -- they must be put into practice every day, Bernier said.

The department has begun implementing her recommendations, she added. "We hope this investigation will prompt other federal departments and private-sector organizations to review their own privacy policies and practices."

The privacy commissioner's office opened its investigation in January last year after the department reported that the hard drive had been missing for two months. It had been stored in a lockable filing cabinet in an employee's cubicle, in an envelope hidden under suspended files.

"Our investigation established that the hard drive was often left unsecured for extended periods of time without being stored in a filing cabinet," the report says. "Even when stored in the cabinet, the cabinet was not always locked and other employees were aware of the location of the keys."

Officials did not know whether it was a case of human error or ill intent.

Bernier's report came as a Federal Court judge certified a class-action lawsuit filed by some of the students, who are seeking damages for breach of privacy and breach of contract.

The students allege they were exposed to a greater risk of identity theft and are owed compensation for time and frustration associated with changing credit cards, getting credit reports and dealing with student loan information.

The hard drive has never been recovered and there is evidence it may have been stolen, said lawyer Ted Charney, who called the judge's decision significant.

"In our digital age there are just so many breaches now," he said in an interview.

"It's just an endless chain of breaches by the governments and by large corporations and we're all trying to come to grips with how these types of breaches should be compensated."

Bernier said the department assures her there is no evidence of fraudulent use of the sensitive information.

Staff of the department's student loans program had used the one-terabyte hard drive to make a backup copy of program information stored in the central computer to ensure its preservation when that data was being transferred between networked drives, her report says.

Bernier recommended:

-- Severely restricting the use of portable storage devices and introducing system software which blocks unauthorized use of such devices on desktop computers;

-- Periodically examining portable storage devices to ensure they are being used solely for legitimate reasons;

-- Reviewing holdings, disposing of transitory records and classifying remaining records at the appropriate security level;

-- Mandatory training on personal privacy protection and testing every two years.

The commissioner plans to follow up in a year to gauge the federal department's progress.

In a statement, the department said most recommendations had already been implemented, with all to be in place by autumn.

A spokeswoman for Employment Minister Jason Kenney said he was unavailable to answer questions.

The vast majority of federal data breaches last year were not reported to the privacy commissioner, said Charmaine Borg, the NDP digital issues critic.

"Government departments tend not to divulge data breaches to the commissioner, or to the people affected by the breach," she said.

"We need a system that requires people to be notified when their data has been breached. Canadians deserve to know when their personal data has been lost by the government."