

Wednesday, August 1st, 2007



## Mobile devices prone to ID theft

Wed Aug 1 2007

*On the Cutting Edge / Brian Bowman*

LAPTOPS, PDAs, cellular phones and USB drives -- these types of mobile devices help businesses carry out their activities in an increasingly electronic world. However, what most businesses may not realize is there is an emerging trend by provincial privacy commissioners to expect greater protections on such devices.

As a number of recent and well-publicized cases have illustrated, thousands of Canadians have been exposed to potential identity theft as a result of a string of losses of laptop computers.

As reported in the *Free Press* this summer, Winnipeg's Concordia Hospital recently had one of its computer hard drives stolen. In an unprecedented move, and to their credit, the Winnipeg Regional Health Authority publicized the theft and advised approximately 3,000 patients that their data may be vulnerable to identity thieves.

Earlier this year, Ontario's privacy commissioner ordered Toronto's Hospital for Sick Children to introduce a number of protections after the theft of a laptop computer containing the personal health information of 2,900 patients.

Last summer, Alberta's privacy commissioner reported that M.D. Management Ltd., an organization that offers financial products and services to Canadian Medical Association members and their families, had one of its laptop computers stolen that contained sensitive personal information.

In most situations, I suspect the laptop computers were stolen for the laptops themselves. However, increasingly thieves are becoming fixated on acquiring personal information for purposes of identity theft. Whether businesses seek to protect sensitive personal information in compliance with privacy-law requirements or safeguard confidential commercial information such as trade secrets and client lists, the protection of data on mobile devices should be assessed and acted upon on an ongoing basis.

A big problem is that most businesses do not really know what data are leaving their offices on laptops, PDAs, cellular phones and USB drives. Such organizations should immediately take stock of their data-management practices by, for example, conducting a privacy impact assessment.

## Minimize potential

Once businesses do know what data are leaving their offices, they should take steps to minimize the potential for the loss or theft of information on mobile devices.

Ontario's privacy commissioner has stated that "a multi-layered approach is needed to guard against unauthorized access" to mobile devices.

The first step to safeguard against the loss or theft of data is to simply avoid storing sensitive information on such devices. If, however, sensitive data must be stored on mobile devices, save only the minimal amount of data necessary.

Most businesses utilize user ID and password protection for their mobile devices. Both Ontario and Alberta's privacy commissioners, however, have recently indicated that such measures may not be sufficient. Instead, the commissioners have called for the use of data encryption technology.

In addition to technological measures, businesses should implement appropriate privacy policies and procedures to protect personal information. Such policies can also be used to protect confidential corporate information.

Finally, businesses should train staff to take common-sense measures to prevent the loss of data on mobile devices. For example, laptop computers should never be left unattended in parked vehicles, as a number of reported cases involved laptops being stolen from parked vehicles.

Laptops, PDAs, cellular phones and USB drives are gold mines for identity thieves. As greater amounts of data find their way onto mobile devices, the market for criminals to steal such devices and the information contained on them will almost certainly rise.

Businesses should keep pace with the emerging reality and risks associated with mobile devices and take proactive measures to protect the most valuable business assets -- personal information and confidential corporate information.

*Brian Bowman is a business lawyer with the Information & Ideas Group of Pitblado LLP. He can be reached at (204) 956-3520 or [bowman@pitblado.com](mailto:bowman@pitblado.com).*