

Identity Theft, Information Privacy and the Photocopier

"Publicized threats (of identity theft) range from mailbox thieves and lost laptops to the higher-tech methods of email scams and corporate data invasions. Now experts are warning that photocopiers could be a culprit as well."

That quote came from a media report in 2007. Yet clearly, the problem has been largely ignored, and the public remains generally unaware of this potential threat, which could put the most critical and intimate information of an individual, business or state in jeopardy of loss, theft or compromise.

A television report in March 2010 begins:

At a warehouse in New Jersey, 6,000 used copy machines sit ready to be sold and almost every one of them holds a secret. Nearly every digital copier built since 2002 contains a hard drive - like the one on your personal computer - storing an image of every document copied, scanned, or emailed by the machine. In the process, it's turned an office staple into a digital time-bomb packed with highly-personal or sensitive data. If you're in the identity theft business it seems this would be a pot of gold. The types of information available on some of these machines are social security numbers, birth certificates, bank records and income tax forms.

The problem - the captured data is not removed from the hard drive unless the owner/operator is aware of the threat, appreciates the ramifications of the threat and employs special software designed to purge the hard drive of this stored data as photocopiers do not come with a "purge" button to remove the material on demand.

Until this report was broadcast, few people knew about the problem. Since then, through distribution across the internet, a storm of concern has erupted across North America. An investigation has begun in the U.S. Congress and it is hoped some action may result to deal with this problem.

What's being done to protect Canadians and their businesses, which generally remain unaware of this threat? The report revealed that even though software programs (at additional cost) are available to purge information, few lessees or purchasers are aware of the solution, or are electing not to take advantage of them.

When four used machines were purchased at random, in the production of the aforementioned television report, the hard drives were removed and downloaded, yielding sensitive police files, medical records and patient information as well as other data. Many of these used machines are sold offshore with little or no control over where they go. Those hard drives were not purged by the wholesaler.

Further exacerbating the potential for identity theft and critical information to be compromised is the fact that there is an enormous inventory of used equipment on the market due to the financial downturn and the resultant surplus of equipment from failed and down-sized businesses and government operations across the globe.

It is reasonable to assume, that if a person uses a computer, they are aware (or should be aware) that any data they introduce to that machine would be stored until removed and they would be responsible for it.

It is not reasonable to assume that users of digital photocopiers, whether in a public or business setting, would be aware that these machines capture and retain all information introduced to the machine.

The result is that anyone who copies personal or corporate data may be at risk of having that data fall into the wrong hands, within our borders or beyond Canadian jurisdiction, when used machines are shipped out of the country.

Notwithstanding the commercial risk to companies of the exposure of critical private data, research for this document found no information on how many of these companies are aware of the issues around digital photocopiers. It certainly poses some interesting legal questions of where liability lies under the *Personal Information Protection Electronic Documents Act* and any provincial legislation where applicable, when machines containing potentially sensitive documents are returned, resold or otherwise disposed of.

Some large firms and government agencies, particularly those with IT departments, are aware of the issue, and maintain policies to ensure data is protected. An RCMP member reported that all hard drives on all equipment are destroyed before their office equipment is disposed of.

In the wider world however, there exists the potential that great harm may be occurring, and the federal Office of the Privacy Commissioner should ensure that this problem is brought to everyone's attention along with guidelines to assist both the general public and business sector in dealing with it.

Recommendations

That the federal government:

1. Encourage and work with industry to develop and implement an information program to advise all users and operators of digital photocopiers and other similar devices with data storage capacity of the potential risks to the security of stored information when such equipment is returned following lease termination and/or resold, and
2. Encourage and work with industry to develop and publicize guidelines for users, operators and dealers of such equipment, on how to purge stored data after use.