



Michael Whitt

# Privacy, Security, and Portable Computing Devices

Michael Whitt and LeRoy Brower

Michael Whitt is a partner with Borden Ladner Gervais in Calgary

LeRoy Brower is the Director, Health Information Act, Office of the Information and Privacy Commissioner in Edmonton, Alberta



LeRoy Brower

As Laptops and other portable computing devices have become (and continue to be) pervasive in the workplace, and as work-forces becomes more mobile and connected, it becomes important for healthcare informaticians and those concerned with protection of personal data privacy to understand the security risks surrounding the loss of portable computing devices in order to advise clients with regard to security systems and policies (“standards of care”) and duties of compliance with, for instance, various regulatory schemes protecting data privacy.

The types of portable devices which attract our attention now, include cellphones, personal digital assistants (PDAs) such as Palm™ or Blackberry™ devices, MP3 players such as iPods™, Universal Serial Bus (USB) storage devices such as memory key-fobs, other portable storage media such as MemoryStick™ or Smart Digital (SD) cards and chips, digital cameras, tablet computers and laptop computers. In the near future, this list will almost certainly expand to include other devices such as memory-based video cameras, digital voice recorders, and the like. Additionally, concerns will arise related not just to the device, but to device-independent remote access to information stores, most commonly thought of today as access from a laptop to the home or central computing and storage location (typically over remote access logins and sometime over Virtual Private Networks (VPNs), but increasingly web or browser-based access over public networks using identification and security mechanisms such as user id/password combination sometimes coupled with physical device based encryption keys or biometric or RFID identification components.

Happily, there have been some recent investigative reports and guidance from the Alberta and Privacy Commissioner’s private sector and health information offices.

In the MD Management case (<http://www.oipc.ab.ca/ims/client/upload/ACFAB50.pdf>), a laptop computer was stolen from an employee’s unsecured vehicle. In the Calgary Health Region case ([http://www.oipc.ab.ca/ims/client/upload/H2006-IR-002%20\\_2\\_1.pdf](http://www.oipc.ab.ca/ims/client/upload/H2006-IR-002%20_2_1.pdf)), a laptop computer

was stolen from a locked residence. In each case, the storage devices within the computers contained personal information of third parties, and may have had the ability to remotely connect to larger storehouses of similar data.

In the MD Management case, Alberta’s PIPA (Personal Information Protection Act) applied, while in the CHR case, Alberta’s HIA (Health Information Act) applied; while there are some differences in those pieces of legislation, the underlying policy is the same: personal information warrants a reasonable degree of protection, which includes security aimed at mitigating risks arising from criminal theft.

In each case, the Commissioner’s investigator found that laptop thefts are on the rise in general, and that the risk of loss by criminal theft is a reasonably foreseeable risk. Both investigators reported that a variety of security mechanisms are available commercially, some of which are initially free of charge, such as: locking cables, operating system level encryption, log-on identity and password systems with properly configured preferences denying boot capability from peripherals, strong partition level and file-level encryption, and larger enterprise-scale security and public-key-infrastructure managements systems which can prohibit unencrypted storage, can lock-down or remotely disable devices, may provide “phone-home” systems, and can remotely implement “kill device” commands.

Of particular note, both investigators opined that social-engineering “policy and procedures”, or means of managing the “human element” could have profitably been paid more attention, finding that while policies had been put into place, they were not complied with or policed, nor supported by adequate technological mechanisms or user training. Policies are not sufficient to protect personal information in these circumstances.

Policies such as “only store relevant information on the laptop” and “files containing sensitive or personal information must be encrypted” were in place, but not

adequately supported by training, nor followed. Additionally, policies about locking laptops to furniture or vehicles, and safely storing computing devices out of sight when the operator is absent, and similar physical security practices, while promoted were not followed. Any of the above non-technological procedures, if followed, would have significantly reduced or even removed the threat of unlawful disclosure of personal information contained on the stolen equipment.

In the CHR case, the investigator also noted that had the CHR performed adequate and routine Privacy Impact Assessments with respect to its internal use of laptop and portable computing devices in all of its operations, the non-compliance with standard CHR policy by the particular subsidiary operation involved would have become quickly apparent and readily fixed (by imposition of otherwise standard CHR operating policies and systems in that subsidiary). Of note, Alberta's HIA requires the preparation and filing of a Privacy Impact Assessment for comment prior to a custodian's implementation of information systems or practices impacting personal health information.

In the MD case, the investigator suggests that a reasonable approach to securing personal information at risk due to the use of portable computing devices in an information system includes more than technological systems. She points the careful reader to a balanced approach to risk analysis and mitigation and suggests consideration be had of the following:

- technological protection mechanisms;
- policy and procedural protection mechanisms; and
- physical security protection mechanisms and that attention to one dimension alone is insufficient.

The Investigative Reports and discussion papers in the industry lead us to some interesting questions:

- What security technologies might prevent disclosure if a mobile device was stolen or is lost?
- What might be considered to be reasonable safeguards to protect personal and/or health information on a mobile device?

Some ideas from our review of the literature and our experience in practice include:

- When implementing technology to protect mobile devices, start with a risk assessment. This will allow you to prioritize your actions to protect the most sensitive data first. It should also help you to discover where there are any unauthorized or previously unknown uses of mobile devices in your organization. [Note – we see that custodians/organizations, even the ones with strong privacy and security practices, can have staff and/or entire program areas using mobile devices without the knowledge and guidance of its privacy/security experts. What we call the “rogue mobile devices issue”. Unless a fairly rigorous analysis of information systems, devices, and user behaviors is undertaken these “rogue device” issues will remain undetected until discovered in a breach scenario!]
- Mobile devices are highly susceptible to loss and theft. This is well known and documented by police services and IT departments. Your starting point should be to assume that some mobile devices will be lost or stolen and therefore any information on the device must be protected accordingly.

## Summary

The guidance which we may take from these two cases is that:

1. portable computing devices are known targets of for criminal theft, the risk of loss of personal information through such thefts is foreseeable, and loss of control over personal information stored on (or “accessible with”) portable computing devices is a risk which reasonable protection mechanisms must be aimed at reducing or eliminating, even when the risk of disclosure is through the criminal act of a third party thief
2. weak user i.d. and password login systems are not adequate protections
3. encryption of personal information using robust techniques (including both the encryption/decryption systems and the password and user interface elements) will essentially eliminate the risk of disclosure through theft (and in several pieces of US legislation absolves the data-keeper from obligations arising from disclosure of personal information if the information is adequately encrypted)
4. pro-active security practices, such as Privacy Impact Assessments of portable computing device use within systems containing or accessing personal information will uncover foreseeable risks, and provide pre-emptive mitigation (and some degree of immunity from blame or liability if a reasonable standard of data care or stewardship is met)
5. the analysis cannot be restricted to technological mechanisms, but should follow a balanced review of the following elements: (i) physical security, (ii) procedural and policy (administrative) security, and (iii) technological security
6. the analysis and implementation of data protection mechanisms may be done on a “cost/benefit” basis, and if “reasonable” levels of security are provided in the light of the whole system's operation and costs, it is not necessary (nor is it possible in every case) to provide absolute protection of personal information.

- The very best defense is to avoid putting health or personal information on mobile devices. For users who must have access to health or personal information when away from the office, there are technologies that when necessary allow secure remote access to data held on the organization's server. This may not be practical, but may be administratively simpler to centrally manage than a large number of independently managed remote devices. On the other hand, a single breach may expose a much larger data set to unlawful disclosure, and even large systems are only as secure as the weakest point of protection.
- If a device must store personal/health information, the best protection is always strong encryption, properly implemented. Again, we stress that password or passphrase policies, user identification management, and issues around implementation in a social setting are important.
- Other technologies, such as devices that can "phone home" and give their location (computer "lo-jack"™ type systems) depend on the device to be connected through a network (cellphone or internet) to a server. Similar concerns with "kill command" systems which can remotely disable devices, or simpler systems which self-destruct if they are not able to "call home" are also available. These may assist in helping to recover the device eventually, but the data may have already been copied elsewhere.
- Reasonable safeguards ALWAYS include administrative (policies and procedures), physical and technical safeguards. When we look at most system failures in the security realm, the failure path analysis almost always leads to a human failure, whether a failure to follow procedures, a failure in understanding or training or communication of policies and procedures, or some conscious failure to comply with procedures (whether malicious or simply a "workaround" to permit a task to be performed in the face of a badly designed, awkward, or difficult security procedure).
- Generally, 128 bit encryption is adequate for protecting data. However, the level of encryption necessary should be determined only after conducting a thorough risk assessment. Encryption systems are like very secure locks, so the control of the "keys" to the locks and the ability to hand out or copy the keys is also important. Organizations need to ensure continued access to organizational information (for example if an authorized person leaves the organization for whatever reason, the individual's access rights need to be removed, but the organization's access to information encrypted with that individual's "key" will need to be accessible/unlocked by another authorized user; at the same time, the individual's use of the key cannot be interfered with or duplicated while the individual is authorized. (This is the "private key infrastructure" or PKI issue, which can become unwieldy very quickly as the number of users gets larger)
- It is generally accepted best practice to use encryption systems that have been vetted in open forums (e.g. AES, RSA, OpenPGP), rather than those that are closed or proprietary. Proprietary systems are more vulnerable to attack simply because fewer people have examined them in detail for flaws.
- It is important that the encryption system be implemented by those with cryptography expertise. Training and ongoing support is critical for users. Users need to understand when they need to encrypt data and the possible risks of data loss if they forget a password [Note – we see that organizations can have policy to encrypt, but it is useless if staff don't know how to do it or understand the risks if they simply choose not to follow the policy]. The best crypto-system can be compromised if users are not given detailed instructions. For example, you may have implemented 256 bit AES encryption on your hard drive, but if the user chooses a weak password, all your efforts will be in vain.
- Many security experts will advise that you should only encrypt data that needs to be encrypted. This relies on the user making a decision about whether to encrypt each time he puts data on a mobile device. This may work well if users are highly aware of security issues and well trained. An easier approach would be to automatically encrypt all data on all mobile devices, eliminating the human error factor. There may be a performance cost to doing this for some devices, but with today's computing technology, this is becoming less of an issue.

**NOTE:** Portions of this article first appeared in the publication "Lawyers Weekly" (LexisNexis) 19 January 2007 edition.

---

*Some recent case law and resources:*

**MD Management Ltd.** (Alberta Information and Privacy Commissioner – Report of an Investigation into the Security of Personal Information – 26 September 2006 – Investigative Report P2006-IR-005)

**Calgary Health Region** (Information and Privacy Commissioner of Alberta – Report of an Investigation Concerning a Stolen Laptop Computer – 5 December 2006 – Investigation Report H2006-IR-002 – Investigation H1441) Readers may access these reports through the web-site of the Alberta Office of the Information and Privacy Commissioner at [www.oipc.ab.ca](http://www.oipc.ab.ca)

**Federal Privacy Commissioner and Bank of Montreal brochure:** [citation]

**Alberta Privacy Commissioner's "Key Steps to Responding to Privacy Breaches":** [citation]