

3-9 MAY 2009

Privacy Awareness Week

Survey on PSDs

The Privacy Commissioner has asked public sector agencies about their use of 'portable storage devices' (PSDs).

PSDs are small, lightweight, portable, easy to use devices capable of storing and transferring large volumes of data. They include USB sticks, cellphones, iPods, PDAs (personal digital assistants, such as a BlackBerry), iPhones and netbooks.

The use of PSDs in the workplace presents potentially major security risks, particularly if the devices contain unsecured sensitive data. They can be easily lost, misplaced or stolen. The storage capacity of PSDs has also grown dramatically in only a few years, exposing organisations to risks of major data leakages. However, there are some simple steps that agencies can take to ensure that PSDs are secured, and are used appropriately.

Because of their convenience, PSDs are increasingly being used by government agencies as well as private sector agencies. The Office of the Privacy Commissioner recently surveyed government departments to find out what sort of precautions they are taking to secure New Zealanders' data. The results of that survey will be equally interesting for private sector agencies that are looking at how they should use PSDs.

"We are concerned with the ongoing security risks businesses and agencies face when storing, using and transferring personal information," Privacy Commissioner Marie Shroff says.

Mrs Shroff will release the PSD survey results on 5 May at a *Business and Security* presentation in Christchurch, hosted by the Information Systems and Audit Control Association (ISACA). The results will be posted at www.privacy.org.nz the next day, and there will be a report in the next issue of *Private Word*.

The New Zealand survey was largely based on a similar survey undertaken by Privacy Victoria, Australia, which released its results in January. See www.privacy.vic.gov.au, and follow the link "Use of Portable Storage Devices".

Keep your BlackBerry safe

Help keep the information on your BlackBerry, a portable storage device, safe and secure:

- Use encryption.
- Have the proper firewalls, anti-virus and anti-malware protection in place.
- Keep your private information private. When using your BlackBerry, whether checking your email, making calls or checking your bank account, don't risk a potential breach by allowing someone else to view what you are doing.
- Keep your BlackBerry on you at all times. Common places for losing a BlackBerry include bars and restaurants. Even if it is missing temporarily, data can be stolen.
- Have a back-up by using a remote access security system. If you lose your BlackBerry it can be locked remotely so no one can get into it, or the information can be backed up and then wiped from your BlackBerry.

Source: www.computerworld.com



Privacy Awareness Week (PAW) is being held earlier than usual this year to allow the Canadian (federal) and British Columbian privacy offices to be more fully involved, along with other Asia Pacific Privacy Authorities (APPA) including New Zealand.

"Working with other privacy jurisdictions is essential today, in a world where data management increasingly occurs across borders," Privacy Commissioner Marie Shroff says.

"Personal information can be stored on servers anywhere in the world – it's important that agencies and individuals are aware of the implications of this."

Part of this year's PAW campaign is to get young people thinking about the information they post online.

The APPA team has made a video looking at consequences of uploading personal information – who might see that photograph of your weekend partying – your coach, your teacher, your parents?"

See page 3 for more PAW details, or www.privacy.org.nz or www.privacyawarenessweek.org

Case notes

MAN OBJECTS TO INFORMATION HELD BY POLICE

PREVIOUS OWNER'S INFORMATION ON MOBILE PHONE

A woman bought a mobile phone for her teenage daughter but the phone stopped working shortly afterwards so she returned it to the retailer and received a replacement. The retailer supposedly erased the daughter's information from the broken phone.

Two months later, the daughter received a text from a friend telling her about a stranger who had been sending text messages to the friend asking about her.

The mother discovered that the retailer had repaired the original mobile phone and on-sold it. But the phone still contained the daughter's contact list and photographs, and the stranger was using this information to try to find out more about the girl.

The mother was very concerned for her daughter's safety, and the daughter was upset that her details were in the hands of a stranger. The woman made a complaint to the Privacy Commissioner. The complaint raised issues under rule 5 of the Telecommunications Information Privacy Code 2003, which states that:

- A telecommunications agency that holds telecommunications information must ensure:
 - (a) *that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against:*
 - (i) loss;
 - (ii) access, use, modification, or disclosure, except with the authority of the agency; and
 - (iii) other misuse; ...

The retailer unreservedly apologised for the incident. Its policy was to make every attempt to ensure that personal information was deleted when customers swapped phones as part of the warranty process.

The retailer recovered the phone, deleted the daughter's information and then destroyed the phone. The retailer stressed to all staff that they must protect their customers' privacy by checking all phones and clearing all stored information.

The retailer learned that the daughter was soon to travel overseas and gave her a new, more expensive, mobile phone for her trip.

Case Note 204348 [2009] NZ PrivCmr 6

The Police were informed that a man had assaulted a young woman and it was noted on the National Intelligence Application, the Police database. The man concerned found out and asked the Police to delete the information because he believed it was incorrect.

The Police refused to remove the information from the database because they believed it was correct, and told the man that they could retain the information on their database indefinitely. The man then complained to the Privacy Commissioner. The complaint raised issues under principles 7 and 9 of the Privacy Act.

- Principle 7 states, among other things, that:
 - (1) *Where an agency holds personal information, the individual concerned shall be entitled –*
 - to request correction of the information; and*
 - to request that there be attached to the information a statement of the correction sought but not made.*

The man and the Police had different views about the accuracy of the information. The Police therefore did not have to comply with the man's request. Instead, they attached a statement of correction, which expressed the man's views that the information was incorrect. Anyone now reading the information would be able to see the original information and also that it has been disputed.

By attaching the statement of correction to the database, the Police had not breached principle 7.

- Principle 9 provides that:
 - An agency that holds personal information shall not keep that information for longer than is required for the purposes for which the information may lawfully be used.*

Most agencies do not have a lawful reason for keeping information indefinitely. However, the legitimate purpose of the Police intelligence database is to maintain a record of information to support the Police in detecting, preventing, investigating and prosecuting crime. Where someone has alleged that a person has committed a criminal offence, the Police have an ongoing lawful purpose for retaining the information.

The Police are still subject to the other privacy principles such as the need to check accuracy of information before use, and to provide access and correction on request. These are important protections for people's rights. However, retaining the man's information did not breach principle 9 in this case.

Case note 204195 [2009] NZ PrivCmr 5

WOMAN'S HEALTH CONDITION ON ENVELOPE

A woman employee at a hospital was voluntarily admitted for a short time as a mental health inpatient. After being discharged, the hospital sent discharge summary notes to her home address in an envelope stamped on the back with "Mental Health Inpatient Unit".

The woman was distressed by this. As she was flatting, any of the flatmates could have seen the letter in the mailbox. Her flatmates were previously unaware that she lived with a mental illness.

As a hospital staff member, the woman was aware of the hospital's policy to delete departments' names from outgoing mail, so that envelopes did not disclose patients' health conditions.

The woman initially complained to the hospital, which had agreed that her complaint was justified. However, it could not agree on an appropriate outcome. The woman believed she should receive financial compensation given the distress the incident had caused her.

The complaint raised issues under rule 5 of the Health Information Privacy Code 1994, which states:

- A health agency that holds health information must ensure:
 - (a) *that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against:*
 - (i) loss;
 - (ii) access, use, modification, or disclosure, except with the authority of the agency; and
 - (iii) other misuse...

The hospital accepted that stamping the envelope with the department name breached rule 5 of the Code and agreed to make a payment to the woman.

Case note 203014 [2009] NZ PrivCmr 8

New on website www.privacy.org.nz

Two new sections will feature on the Office of the Privacy Commissioner's website during Privacy Awareness Week.

» Unravelling the privacy principles

New material will explain privacy principles 6 and 7 (access and correction) in plain English and allow users to work through the Act in a logical way. The explanatory information will have links to the appropriate case notes, Human Rights Review Tribunal and court decisions, drawing all the relevant material together.

This new resource will help legal staff, employers, privacy officers and other individuals work through privacy issues and help resolve them. Information about the other principles will be added later in the year.

» Online Forum for privacy officers

Privacy Officers now have an online space to discuss privacy issues and concerns within their agencies. They will be able to draw on combined knowledge and experience to help answer their questions and share resources. The Forum will offer another way for the Office of the Privacy Commissioner to answer queries. See the privacy officers page on the website for more details: www.privacy.org.nz/privacy-officers

Justice's information security campaign

The Ministry of Justice is starting an internal campaign about information security and privacy responsibilities during Privacy Awareness Week.

Aimed at its staff, and including both Justice and Court information, the campaign intends to:

- increase an understanding of privacy responsibilities;
- establish information security habits;
- encourage secure mobile computing practice and use of encryption;
- introduce the new responsibilities to be adopted as part of the package; and
- show staff where they can get further information and support.

The key component of the campaign is an informational DVD for staff training and inductions. The DVD will be launched in June. For more details contact Ivan Ravlich, Ministry of Justice, ivan.ravlich@justice.govt.nz

PAW calendar of events

MONDAY 4 MAY, WELLINGTON

Privacy Officers' Round Table meeting

PORT is a voluntary group of Privacy Officers (or people working in that field) employed by both public and private sector organisations. It provides members with an opportunity to network and informally discuss issues or trends in the privacy and information management areas.

Contact sandra.kelman@bp.com for more information – new members welcome.

TUESDAY 5 MAY, CHRISTCHURCH

Seminar: Business and security – portable storage devices survey

The Information Systems and Audit Control Association (ISACA), in association with the Institute of Internal Auditors (IIA) will host this seminar to launch the results of the Privacy Commissioner's portable storage devices survey.

Guest speaker: Privacy Commissioner Marie Shroff

To register, email peter.mulligan@corrections.govt.nz or call 03 363 4548

TUESDAY 5 MAY, WELLINGTON

iappANZ event

iappANZ is the leading association for privacy professionals in Australia and New Zealand. Hosted by PricewaterhouseCoopers, iappANZ is meeting to celebrate Privacy Awareness Week. For more information see www.iappanz.org

To register, call Sandra Kelman 04 903 3634; Graeme McLellan 04 462 7112

TUESDAY 5 MAY, WELLINGTON, & WEDNESDAY 6 MAY, AUCKLAND

Forum: Sensible Sensors, Technology and Privacy

This forum will look at sensor technology, including RFID tags and nano-sensors, and the implications of collecting and storing information from sensors.

To register, email amir.shrestha@privacy.org.nz

THURSDAY 7 MAY, AUCKLAND

Exhibition opening: Chris Slane cartoons

Forty-two Chris Slane cartoons will be exhibited for the first time in Auckland. Many aspects of privacy have featured in Slane's cartoons – the impact of technology, business use of information, health and government databases.

Open to the public 8–15 May – free admission

Gosling Chapman Tower Foyer, 51-52 Shortland Street

FRIDAY 8 MAY, WELLINGTON

Workshop: Security Breach Notification

This workshop will provide participants with an overview of data breach notification and the opportunity to work through several data breach scenarios.

To register, email sharon.newton@privacy.org.nz

News around the world

- British internet companies are being asked to sign up to a new code of conduct for behavioural advertising in an attempt to quell privacy concerns over this controversial marketing technology. The UK's Internet Advertising Bureau, a trade organisation representing more than 450 companies, has announced a set of guidelines, which include a number of stipulations such as telling users clearly what behavioural tracking involves and gaining their consent for its use. Google, Yahoo and Phorm have already signed up to the guidelines. *Source: www.guardian.co.uk*
- A US Senate Bill will allow doctors and hospitals to create an electronic records system. The bill passed in March after lengthy debate over patients' privacy rights and the logistics involved in changing the way physicians keep and send medical and mental health records. Patients can at any time request a report of who has accessed their records, and must annually give permission for records to be placed in the system. *Source: www.lcsun-news.com*
- Swiss bank UBS says it has about 47,000 accounts held by Americans who didn't pay US taxes on their assets, and has accepted responsibility for helping Americans hide assets from the US Government. The bank has turned over the names of about 300 US clients, but is not providing any more names and says nearly all accounts have been closed. The US Government could proceed with a criminal prosecution of the ban. *Source: www.nzherald.co.nz*
- China has amended its law to be able to potentially impose criminal penalties not only on government agency staff but also on those in financial, telecommunications, transportation, educational and medical institutions who sell personal information or provide it to others. Possible penalties for misappropriating personal data include imprisonment for less than three years, a fine, or detention. *Source: www.huntonprivacyblog.com*
- More than 40 major British construction companies face legal action for allegedly buying secret personal data about thousands of construction workers they wanted to vet before employing them. The UK Information Commissioner alleges that firms have, for many years, covertly bought details of worker's trade union activities and their conduct at work. The database appears to have been run for over 15 years by a private detective. *Source: www.guardian.co.uk*

News in NZ

- The Privacy (Cross-border Information) Amendment Bill had its first reading in Parliament on 1 April. The Bill will have two main impacts: first, it will help ensure New Zealand law meets the expectations of our trading partners, and second, it will remove an anomaly so that non-New Zealanders living overseas can access their personal information held in New Zealand.
- The Privacy Commissioner has made a submission to the Justice and Electoral Select Committee on the Criminal Investigations (Bodily Samples) Amendment Bill. The Bill would allow Police wider powers to collect DNA from people before they are charged or convicted. This is an expansion of the current regime, which permits Police to collect DNA after conviction of certain specified offences.
- In response to several recent privacy breaches, the Privacy Commissioner has requested from agencies explanations of why the breaches occurred. The breaches include:
 - Housing NZ documents mistakenly sent out with eviction notices, revealing the address of a senior manager to gang members and forcing her to leave her home under police protection.
 - A sensitive police manual left with Mongrel Mob members during a raid.
 - A Police camera containing hundreds of evidence photos such as crash scenes, burglaries and battered women, left at a house.
 - Massey University's intranet exposed thousands of students' personal details. During a five-hour period students logged-on to the system could view other students' IRD numbers, exam results, addresses and phone numbers.
 - As part of the recent HPV vaccination campaign, girls' personal contact details were given to district health boards from school roll information. Students and parents were not always aware that this would happen. The Office of the Privacy Commissioner was involved in advising on the process and recommended that parents either be asked to consent or that schools notify parents of the proposed disclosure so they would have the chance to object.

DIRECTORY

The Privacy Commissioner has offices in Auckland and Wellington.

Commissioner: Marie Shroff

**Assistant Commissioner,
Policy:** Blair Stewart

**Assistant Commissioner,
Legal:** Katrine Evans

**Assistant Commissioner,
Investigations:** Mike Flahive

**Senior Adviser, Legal & Public
Affairs:** Annabel Fordham

AUCKLAND

Tel: 09 302 8680

Fax: 09 302 2305

email: enquiries@privacy.org.nz

Auckland privacy enquiries, call:
302 8655

WELLINGTON

Tel: 04 474 7590

Fax: 04 474 7595

email: enquiries@privacy.org.nz

For enquiries outside of Auckland,
call the enquiries line: 0800 803 909

Postal address:

Privacy Commissioner
PO Box 10 094
Wellington
New Zealand

Website

www.privacy.org.nz

Private Word - Not "The Word"

Private Word is an informal newsletter, and should not be relied upon for legal advice. Individual privacy cases differ, so please contact a lawyer for advice on specific situations.