

## Privacy Awareness Week

24–30 AUGUST 2008

Privacy Commissioner Marie Shroff is pleased to be part of Privacy Awareness Week 2008 with her Asia Pacific Privacy Authorities (APPA) international partners.

“The week aims to raise everyone’s awareness about privacy-related issues and to enhance the knowledge of businesses and agencies about the implications of dealing with personal information, especially in the digital environment. We are keen to look towards the future and the issues arising, for example, from the ability to collect and store DNA material. We want to further the debate about how agencies can share information correctly, especially where there is a joint responsibility in looking after the more vulnerable members of society.”

Privacy Awareness Week will officially begin in Auckland with the Office of the Privacy Commissioner and the Auckland Chamber of Commerce co-hosting a business breakfast on Monday 25 August. Mrs Shroff will announce the results of the latest UMR public opinion survey and the new book *Privacy at work – A guide to the Privacy Act for employers and employees* will be launched.

On Wednesday 27 August a one day Privacy Issues Forum will be held in Wellington. The Privacy Commissioner will begin the Forum by setting the scene about the current privacy environment and speaking about international privacy developments. The sessions following include genetic research, DNA databases, the role of the private investigator in modern criminal investigations, managing the digital shadow, and employment.

See [www.privacy.org.nz](http://www.privacy.org.nz) for the Forum programme.



### Cartoon exhibition

An inaugural Chris Slane privacy cartoon exhibition will open in Wellington in Privacy Awareness Week.

Privacy has received special attention in Chris Slane’s cartoons since the mid 1990s. Many aspects of privacy have featured – the impact of technology, business use of information, health, government databases – he has challenged them all.

The exhibition will be held at the Jimmy Café and Bar, Westpac St James Theatre, Wellington from 27 August 2008.



### Employment book

*Privacy at work – A guide to the Privacy Act for employers and employees* will be launched by the Privacy Commissioner Marie Shroff during Privacy Awareness Week. The book offers guidelines about applying the Privacy Act in the workplace.

“Privacy issues at work can affect a whole range of people. For example, an employer may be unsure about whom they can contact as a referee when processing a job application, or an employee may be concerned that CCTV cameras have been installed at work,” Mrs Shroff said.

“The guide looks at a range of workplace situations such as monitoring staff email and internet use. It offers guidelines for staff when handling personal information on databases, for example. There are many instances where privacy obligations need to be met by employers and employees need to understand these too.”

#### In this issue:

Case notes | 02

The future of the world’s Internet economy | 03

Modernising the law | 03

Privacy Bill helps trade, enhances personal rights | 03

News around the world | 04

UK reports released on data losses | 04

# Case notes

## LAW FIRM DISCLOSES PERSONAL INFORMATION

A woman had instructed a law firm to act for her in relation to a number of claims against a government agency.

One of her files was accidentally placed in a box at the law firm containing the files of another client who had claims against the same government agency. This other client discovered the woman's file among his own and briefly viewed its contents before advising the law firm that it was not his.

The woman complained to the Privacy Commissioner that the law firm had failed to ensure her personal information was adequately protected from unauthorised access and had disclosed her personal information to the other client. Her complaint raised issues under principles 5 and 11 of the Privacy Act.

Principle 5 places a general obligation on agencies that hold personal information to protect that information from loss, unauthorised access, use, modification or disclosure, by safeguards that are reasonable in the circumstances.

Principle 5 does not require that the safeguards are absolute, but that they are reasonable in the circumstances.

In considering whether a security safeguard is reasonable, the Privacy Commissioner takes into account matters such as: the steps and/or policies in place to guard against a breach of principle 5, whether those steps and/or policies have been followed, training provided to staff and the sensitivity of the information.

The Privacy Commissioner considered the safeguards taken by the law firm – which included the careful naming and storing of files – and was satisfied that they were adequate. In this case, the woman's file was marked with the same government department logo as the other client's files and was mistakenly placed in his box for this reason.

The Privacy Commissioner formed the opinion that this incident was a 'one-off' disclosure based on human error and, therefore, that the law firm had not breached principle 5.

Principle 11 provides that an agency must not disclose personal information unless one of the exceptions applies.

The law firm said that the disclosure of the woman's personal information was unintentional and so there was no breach of principle 11. However, a disclosure does not have to be intentional for principle 11 to apply.

The other client had read information about the woman's claim while the file was in his possession.

The Privacy Commissioner was satisfied that the law firm had disclosed personal information. Because no exception applied, the law firm had breached principle 11.

The disclosure included highly sensitive information and had caused the woman significant humiliation and loss of dignity. She therefore concluded that the law firm had interfered with the woman's privacy by breaching principle 11.

The parties agreed to attempt resolution and the Privacy Commissioner acted as mediator.

The law firm agreed to waive the fees (a substantial sum) that the woman owed. The woman was satisfied with this result.

*Case Note 83994 [2008] NZ PrivCrim 6*

## COURIER DELIVERS LOAN APPLICATION TO NEIGHBOUR

A bank prepared loan documents for a customer and arranged to deliver them to her home by courier.

The bank gave the courier company incorrect delivery details. However, the woman's name and address were correctly printed and clearly visible in the window of the envelope.

The courier company had written instructions to place the package in the customer's mailbox if she was not at home. A compliments slip was attached to the envelope. It read "please find loan documents for your signing". The heading "Application for Finance" was visible through the window of the envelope.

The woman was not at home when the courier called. Contrary to instructions, the courier then left the package with the woman's neighbour to pass on to her when she returned home.

The woman complained to the bank that her loan documents had been handed to her neighbour and that it was evident the package was about a loan application.

The bank apologised to her. It explained that the envelope should have been placed in a courier bag.

The bank discussed the incident with the courier and advised staff of correct procedures when sending information by courier. The bank offered to waive the loan application fee for the woman.

This offer did not satisfy the woman. The day before the documents were delivered, she had made an offer to purchase the neighbour's property. She believed that as a result of the loan documents being delivered to the neighbour, the neighbour then inflated the asking price of the house.

The woman's complaint to the Privacy Commissioner raised issues under principles 5 and 8. Principle 5 states that agencies that hold personal information must take reasonable steps to ensure that the information is safeguarded against loss, unauthorised access, use or disclosure.

Under principle 8, an agency is required to take reasonable steps to ensure the accuracy of information.

The Privacy Commissioner was satisfied that the bank generally had reasonable processes to ensure that information was kept secure.

While there were some unfortunate oversights in this instance, the disclosure was limited. The envelope had remained sealed at all times. The courier company had the correct address on the envelope, and if the instructions to leave the package in the mailbox had been followed no disclosure could have occurred.

The situation was therefore primarily not the bank's fault. The courier company confirmed that its driver had made an error and should have contacted the bank to seek authorisation for the envelope to be signed for by the woman's neighbour.

After investigation, the Privacy Commissioner concluded that the situation was a one-off error that did not reveal systemic failings.

She therefore decided that the bank had taken reasonable steps to protect the security of the information. The customer claimed that she suffered financial harm, under section 66(1), because the neighbour raised the price of the house.

However, there was no evidence that the bank's actions led to this state of affairs. The Privacy Commissioner formed the final opinion that there was no interference with privacy. She also noted that the bank's offer of compensation and the other steps it took were appropriate to resolve the situation.

*Case Note 100962 [2008] NZ PrivCrim 5*

# The future of the world's Internet economy

Privacy Commissioner Marie Shroff attended the recent Organisation for Economic Co-operation and Development (OECD) Ministerial Meeting on the Future of the Internet Economy, held in Seoul, Korea.

Around 2200 participants from 68 economies, including privacy commissioners from the Asia-Pacific and Europe, gathered in Seoul to grapple with some key issues for the future of the world's Internet economy.

Participants agreed on the need for governments to work closely with business, civil society and technical experts on policies that promote competition, empower and protect consumers, and expand Internet access and use worldwide.

OECD Secretary-General Angel Gurría said, "As the individual becomes more of a focal point of the Internet economy, it is not a surprise that the currency of the Internet economy is personal information.

"The growth of business models built around the mining of this data and the explosion of social networking sites, require us to better understand and analyse changes both from an economic and a social perspective – what are the risks, what are the benefits and how do we adapt to this new environment?"

Mr Gurría added that there was a need to assess policies in this area on a global scale and that the global reach of the Internet challenges nations whose policies are geographically limited.

"More should be done in partnership with other public and private organisations to combat information security threats and identity theft."

Mr Gurría pointed out that it had been ten years since the landmark Ottawa OECD Ministerial Meeting on E-Commerce.



OECD Secretary-General Angel Gurría at the Ministerial Meeting on the Future of the Internet Economy, held in Seoul, Korea.

"We cannot talk about the importance of the Internet every ten years, which is an eternity in Internet time," Mr Gurría said. He pledged to review progress on the Seoul Declaration within three years.

The Declaration is available at [www.oecd.org](http://www.oecd.org).

## Modernising the law

A report that updates earlier recommendations for modernising New Zealand's privacy law has been released by the Office of the Privacy Commissioner.

The Privacy Commissioner has called for special consideration to be given to new mechanisms to help protect privacy in the 21st century, including:

- Requiring an organisation to notify affected individuals where a security breach by the agency puts individuals at risk.
- Empowering the Commissioner to conduct privacy audits.
- Exploring the establishment of a national do-not-call database as a response to telemarketing.

"Mandatory security breach notification, privacy audits and national 'do-not-call' lists exist in overseas laws but are not yet part of our privacy regime," Privacy Commissioner Marie Shroff said.

"We need a range of regulatory tools to effectively address the range of current and future privacy risks. These three proposals focus upon empowering individuals and employing techniques to proactively identify and address the risks of our digital world."

This fourth supplementary report surveyed international and national privacy developments over the past four years, and brought earlier reports and recommendations up-to-date. It joins three earlier supplements to the *First Periodic Review of the Operation of the Privacy Act 1993: Necessary and Desirable*. The report and recommendations are available at [www.privacy.org.nz](http://www.privacy.org.nz).

## Privacy Bill helps trade, enhances personal rights

Privacy Commissioner Marie Shroff welcomed the introduction of the Privacy (Cross-border Information) Amendment Bill on 2 July, saying it would have benefits for New Zealand's trading opportunities and enhance personal rights.

"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 people living overseas can access their personal information held in New Zealand," Mrs Shroff said.

"New Zealand business is operating in a global data processing economy and our data protection law needs to be recognised as stacking up internationally.

"It is important that our privacy law keeps pace in order to facilitate international trading opportunities. These changes should help to secure a finding from the European Union that New Zealand law offers an adequate standard of data protection."

The Bill will also give the Privacy Commissioner the ability to cooperate with overseas privacy authorities when dealing with, or transferring, privacy complaints.

This reflects a priority area in the privacy work of both Asia-Pacific Economic Cooperation (APEC) and the Organisation for Economic Co-operation and Development (OECD).

# News around the world

- The EU has mandated that by 28 June 2009 all EU passports (except those issued in the UK and Ireland) should include a chip storing the photo and two fingerprints of the passport owner. In January, a bill introduced to the Dutch Parliament not only implemented this requirement, but also provided for a national database of photos and fingerprints of all Dutch citizens. The Dutch Data Protection Authority said the bill violated Article 8 of the European Convention of Human Rights and that the database would pose a considerable security risk. *Source: The Privacy Advisor, April 2008, Volume 8 Number 4*
- Online job scams that trick individuals to get their bank account or social security numbers are the biggest source of identify theft from website job boards. "In an age of identity theft, resumes are the road maps," said Pam Dixon, founder of the World Privacy Forum in California, a non-profit public-interest group. *Source: www.eagletribune.com*
- One in three IT professionals admitted in a German survey to abusing administrative passwords to access confidential data such as colleagues' salary details, personal emails or board meeting minutes. The survey of 300 senior IT professionals at the InfoSecurity Expo 2008 in Frankfurt, Germany, also found that 47 percent said they had accessed information that was not relevant to their role. *Source: Privacy Times Volume 28 Number 12*
- North Oaks, a city of 4500 residents in Minneapolis, US, has demanded that Google Maps remove images of all its homes from Google's Street View. North Oaks' roads are privately owned by the residents and the city enforces a trespassing ordinance. Google said that the images of structures in North Oaks were removed shortly after the first such request in the US was made. *Source: Privacy Journal, June 2008, Volume 34 Number 8*
- A new law in Sweden, narrowly passed in June, gives the country's National Defence Radio Establishment the right to scan all international phone calls, emails and faxes without a court order. While supporters say the legislation will help avert terrorist attacks by keeping tabs on suspect communications and planned financial transfers, critics say it will encroach on privacy, jeopardise civil liberties and violate the European Convention on Human Rights. *Source: www.nzherald.co.nz*
- A US federal appeals court has made it more difficult for employers to legally snoop on their workers' email and text messages sent on company accounts. Employers that contract an outside business to transmit text messages can't read them unless the worker agrees. The ruling also lets employers access employee emails only if they are kept on an internal server. One non-profit group that advocates civil liberties called the ruling a "tremendous victory" for online privacy. *Source: www.nzherald.co.nz*

## UK reports released on data losses

Five reports were published recently that relate to the security of United Kingdom Government information systems.

- PricewaterhouseCoopers Chairman Keiran Poynter looked into the facts surrounding the HM Revenue and Customs' (HMRC) loss of child benefit data on 25 million individuals. The report states that the incident arose following a sequence of communications failures between junior HMRC officials and the National Audit Office. The loss was entirely avoidable, and the fact that it could happen pointed to serious institutional deficiencies at HMRC. [www.hm-treasury.gov.uk](http://www.hm-treasury.gov.uk)
- The Independent Police Complaints Commissioner, acting on its own initiative, investigated the events leading up to the loss of the HMRC data and concluded that individual members of staff were not to blame. [www.ipcc.gov.uk](http://www.ipcc.gov.uk)
- The Cabinet Secretary's report sets out how the UK Government is improving its arrangements around information and data security. The report calls for mandatory minimum measures across government, including encryption and compulsory testing by independent experts of the resilience of systems. [www.cabinetoffice.gov.uk](http://www.cabinetoffice.gov.uk)
- The Ministry of Defence published a report about the theft in January of a Royal Navy recruiter's laptop, which contained unencrypted records on more than 600,000 people. [www.mod.uk](http://www.mod.uk)
- *The Data Sharing Report*, an independent review undertaken by the UK's Information Commissioner Richard Thomas and Wellcome Trust Director Mark Walport, recommends stronger leadership and accountability in all organisations using and sharing significant amounts of personal information, and greater openness and transparency in the way personal information is handled by others. [www.justice.gov.uk](http://www.justice.gov.uk)

## 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](mailto:enquiries@privacy.org.nz)

Auckland privacy enquiries, call: 302 8655

### WELLINGTON

Tel: 04 474 7590

Fax: 04 474 7595

email: [enquiries@privacy.org.nz](mailto: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](http://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.