

Private Word

News from the Office of
the Privacy Commissioner

Technology: “A silent revolution”

The day-to-day work of the Privacy Office in acting as a ‘watchdog’ to protect personal information and promote good practice has become increasingly focused on technology and science-driven issues, Privacy Commissioner Marie Shroff says in this year’s *Annual Report*.

“All kinds of organisations and businesses use advanced technology to collect, sort, store and trade our personal information, both to make our lives easier in dealing with them and also for their own use,” she says.

“A silent revolution has occurred in the way our personal information is handled.

This revolution has the potential to be as far-reaching and pervasive in its effects as the invention of the printing press more than 500 years ago. We need to grasp this change, direct and use it. But we also need to protect our identities in the process, and value our information as much as do those who profit from it.”

In common with people in other countries, New Zealanders are concerned about the challenges posed by technological developments and changes in business practice. More than 80 percent of people surveyed by the Commissioner’s office earlier this year pinpointed the internet and business as key privacy concerns,

while 93 percent rated good personal information practices by business as more important than convenience.

Marie Shroff says that, as a result, the Office of the Privacy Commissioner’s role in monitoring and advising on technology (for example, by setting up technology and privacy forums), is becoming increasingly important.

The work of the Office overseeing government inter-agency information matching programmes also continues to expand. Forty programmes were in operation during the 2005/06 financial year, compared with 36 in 2004/05. There was a 45 percent increase in the number of government information matching programmes using online information transfers.

Key points from the Privacy Commissioner’s 2005/06 *Annual Report* are on the Office’s website home page at www.privacy.org.nz. The full text is also available on the website or by request to the Office.

TC/DRM challenges for governments

An Office of the Privacy Commissioner presentation on *Trusted Computing (TC), Associated Digital Rights Management (DRM) Technologies and Privacy in Government* was well received at a recent international conference.

Technology Team Leader Lindy Siegert presented the paper at the International Working Group on Data Protection in Telecommunications (IWGDPT) 40th meeting, held in Berlin. She represents the Office on the State Services Commission (SSC) cross-government steering group on TC/DRM.

Software developers and information providers aim to provide more security for internet users through systems that relay information back to them to check whether an application has been compromised by malicious software, or whether the person using the computer is permitted to read a document.

Ms Siegert says the SSC’s key concerns

are how TC/DRM may affect government-held information. The risk areas include privacy, legal requirements under public records, archives and freedom of information law, compatibility with legacy information management systems, and possible bypassing of anti-virus controls.

The draft New Zealand resolution presented to the Berlin conference has now been formally adopted by the IWGDPT.

The resolution recommends governments consider adoption or adaptation of the principles and policies developed by New Zealand, such as not implementing TC/DRM technologies in ways that may compromise subject access rights, endanger the confidentiality and integrity of official records, endanger the privacy of personal information, or compromise the security of government information systems.

For further information on the SSC project: www.e.govt.nz/policy/tc-and-drm

In this issue:

Law professor says biometrics Employment Court judgment “should be approached with some caution” - page 2.

- 02 Law Commission privacy review
- 03 Asia Pacific forum promotes ideas exchange
- 03 A day in the (digital) life ...
- 03 UK privacy reports
- 04 News around the world
- 04 Slane cartoon

Biometrics in the workplace



An Employment Court judgment that an employer should have consulted workers before introducing biometric finger scanning for time keeping purposes should be approached with some caution, writes Otago University Law Professor **Paul Roth**.

In the recent case of *OCS Limited v Service and Food Workers Union Nga Ringa Tota Incorporated* (Wellington, WC 15/06, 31/8/06), the Employment Court held that the employer's contractual and statutory obligations required it to consult the workers concerned and their union before introducing a biometric time-keeping system.

As far as the Court's approach to the relevant employment agreement was concerned, the judgment was unconvincing. The agreement did not specifically require consultation over matters such as time-keeping methods, and the Court regarded as irrelevant the statutory obligation of employers to keep wages and time records. The Court also found that the employer had a good faith obligation under the Employment Relations Act to consult on any change in workplace practices, which seemed like a breathtakingly broad proposition.

The factor on which this case actually turned was the particular context: most of the nearly 50 employees concerned were Samoan. They regarded finger-scanning as culturally insulting because it implied that, like criminals, they were not to be trusted. Expert evidence was also introduced to substantiate the nature of Samoan beliefs concerning

the sacredness of parts of the body and the concept of *Va Fealoia*, "the sacred space which governs and manages all relationships between people including employers and employees".

The finding in this case, therefore, should be approached with some caution because it is quite specific to its own facts. The employees concerned belonged to a minority group that had cultural concerns relating to the new technology, and there was a specific statutory obligation for employers in the public health sector to be "good employers", which includes "recognition of...the cultural differences of ethnic or minority groups". Accordingly, the employees concerned ought to have been consulted before the introduction of a technology that was *prima facie* culturally offensive.

The finding is somewhat different to other cases. For example, in *PMP Print Limited v Barnes* (AA 317/04, 28/9/04), the Employment Relations Authority found that the introduction of a finger scanning system fell within the relevant contractual provision relating to time keeping. The employment agreement provided that "Employees are required to complete all time and wage records as required by the Company", and this was found to cover biometrics.

The employee concerned argued that the technology involved stamping him with the 'Mark of the Beast', as described in the Book of Revelations, so that he would be unable to participate in the Rapture. The Authority, however, found that there was no basis for a claim of indirect discrimination, as the technology does not actually stamp a mark on a person, or even store the image of a fingerprint. It merely records a mathematical representation that cannot be reverse-engineered to reconstruct a person's fingerprint.

Privacy Commissioners, both here and overseas, have also rejected finger scanning complaints. In a 2003 case note, the New Zealand Privacy Commissioner at the time rejected a union's complaint against a company that introduced biometric finger scanning for time-keeping purposes. Similar complaints were also rejected by the Canadian Privacy Commissioner in 2003, and the Irish Data Protection Commissioner in 2005. In each case, the biometric identification system concerned was not found to be an unreasonable intrusion into the privacy of workers.

The OCS Employment Court case reported here relates to cleaners working at Wellington Hospital who refused to undertake daily thumb scanning in order to clock in and out of work.

Law Commission privacy review

The Law Commission has released terms of reference for its *Review of Privacy*.

The Commission says the review will be undertaken in stages. The first will be a high-level policy overview to assess privacy values, changes in technology, international trends and their implications for New Zealand law. A survey of these trends will be done

in conjunction with the Australian Law Reform Commission.

In stage two, the Commission will consider whether the law relating to public registers requires systematic alteration as a result of privacy considerations and emerging technology. For stage three of the project, the Commission will consider and report on: the adequacy of New Zealand's civil law remedies

for invasions of privacy, including tortious and equitable remedies; and the adequacy of New Zealand's criminal law to deal with invasions of privacy.

The fourth stage of the project will see the Commission reviewing the Privacy Act 1993 with a view to updating it, taking into account any changes in the legislation that have been made subsequently.

Asia Pacific forum promotes ideas exchange

Privacy Commissioner Marie Shroff represented New Zealand at the 26th Asia Pacific Privacy Authorities' (APPA) Forum in Hong Kong last month.

APPA is a cooperative network through which regional privacy authorities can form partnerships and exchange ideas about privacy regulation, new technologies, education and the management of privacy complaints.

This year's forum included presentations and discussion about covert surveillance, consumer credit data, CCTV, Hong Kong's "Smart ID Cards" and privacy protection measures by corporations.



Privacy Commissioner Marie Shroff meeting Hong Kong's Secretary for Justice Wong Yan-lung. In the background are Roderick Woo, Hong Kong Privacy Commissioner, and Karen Curtis, Australian Privacy Commissioner.

A day in the (digital) life ...

Telecom technology architect **Tom Glover**, speaking at a recent Office of the Privacy Commissioner Technology Forum, outlined the following vision of the future - noting that the majority of the technology capability already exists:

6am: use RFID implant in hand to switch off internet radio alarm clock.

7am: lock and alarm house by hand-swipe using RFID. Car autopilots me to work using GPS/LBS system.

8am: arrive at office where Building Spatial Location System (SLS) greets me and allows access to smart lift.

9am: SLS tag reminds me of meeting; converged phone/PDA displays agenda.

10am: video conference meeting. VC scanner automatically tracks person based on facial and voice recognition. Virtual signature on document confirmed by biometric fingerprint acceptance on PDA.

11am: SLS auto logs on PC using combined SLS and RFID implant.

Noon: order sandwich over web - on delivery, RFID implant identifies me and fingerprint authorises bank payment.

2pm: coffee order queued - authorise payment using my RFID implant.

3pm: PDA alerts me to courier at home - I remotely 'sign' for the package assisted by real-time video to PDA.

4pm: tried to get chocolate from vending machine but request requires second factor authorisation from wife. Access denied. Muesli bar it is.

5pm: Parking fee debited as leave office (RFID).

6pm: arrive home. Alarm auto-disabled and home automation system 'boots' house. Lighting, audio and heating activated to my preferences.

7pm: dinner - smart induction hob prevents child from changing controls while cooking food to personal preferences (via Bosch Online). Children's bedtime - lighting adjusts to parent's settings for child.

8pm: TV 'top box' automagically records both our channels while watching Coronation Street. Targeted ads actually show useful stuff we might buy!

10pm: bed time. The house enters a low-power standby mode. Security systems automatically armed.

2am: hear noise in garden. Voice command activates CCTV to pan and zoom in on garden - shown on my video phone. Just a cat (one without RFID implant).

UK privacy reports

A 'surveillance society' has come about almost without us realising what has happened, say the authors of a detailed report commissioned for the 28th International Data Protection and Privacy Commissioners' Conference held in London last month.

Surveillance Society looks at some of the problems of large-scale surveillance systems. The report notes that "surveillance grows as a part of just being modern" and that one of its unintended consequences is to undermine trust and foster suspicion.

In another recent report, *What Price Privacy?*, UK Information Commissioner Richard Thomas has called for prison sentences of up to two years for the illegal buying and selling of personal information.

The report looks at evidence of systematic breaches of privacy that amount to an unlawful trade in confidential personal information.

Both reports can be downloaded from: www.ico.gov.uk

News around the world

□ Australia's Centrelink has dismissed more than 100 workers, and disciplined hundreds more, for privacy breaches such as snooping on the records of neighbours and former lovers. A two-year dragnet of 25,000 Centrelink staff uncovered 790 cases of "inappropriate access" to the records of welfare recipients since 2004. *Source: <http://tinyurl.com/ejkvv>*

□ A perceived threat to privacy posed by radio frequency identification device (RFID) tags has emerged as the main fear in an EU study of the technology. Unveiling the study, EU commissioner Viviane Reding said citizens needed reassuring that radio tags would not lead to large-scale surveillance. *Source: <http://news.bbc.co.uk/2/hi/technology/6055416.stm>*

□ Some English householders have been incensed by local councils putting RFID tags in wheellie rubbish bins – without their knowledge – in order to weigh individual waste put out for recycling. Correspondents on *Computerworld* blogs say some 500,000 bins across England have been secretly fitted with "electronic spy bugs", and all councils are expected to follow suit in the next couple of years.

□ Microsoft Corp, Hewlett-Packard Co and other high-tech companies are preparing to push for data-privacy legislation next year to replace what they consider an outdated patchwork of US state and federal laws that are inconsistent and burdensome. "We think the time has come for a comprehensive privacy bill that would protect consumers' personal information while still allowing the flow of information needed for commerce online," Ira Rubinstein, a Microsoft lawyer, says. *Source: <http://www.msnbc.msn.com/id/16115003/>*

□ The Osaka High Court has ruled that listing people on Japan's *Juki Net* national resident registry network without their consent is unconstitutional. *Juki Net*, launched in 2002, links local authority residency registers by encoding Japanese citizens' basic personal information and assigning an 11 digit code to each person. The ruling is likely to affect other lawsuits filed by people opposing the computer network that connects local government across the country. *Source: <http://search.japantimes.co.jp>*

□ The EU's data protection head has challenged claims that privacy advocates are blocking governments' attempts to pass so-called anti-terror legislation. EU data protection supervisor Peter Hustinx said effective legislation could not exist without data protection controls to ensure only authorised access to sensitive details. *Source: http://news.com.com/2100-7348_3-6117629.html*



DIRECTORY

The Privacy Commissioner
has offices in Auckland
and Wellington

Commissioner: Marie Shroff

Assistant Commissioner:
Blair Stewart

Assistant Commissioner:
Katrine Evans

Manager Investigations:
Mike Flahive

Senior Legal & Communications
Adviser: 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 a newsletter, not legal advice. Individual privacy cases differ, so please contact the Office of the Privacy Commissioner or a lawyer for advice. Do not simply rely on material in these pages.