



Private Word

News from the Office of
the Privacy Commissioner

Defending data – taming surveillance

Online privacy, identity management and CCTV were put under the spotlight at recent technology and privacy forums hosted by the Office of the Privacy Commissioner.

Dr Judit Bayer, senior research fellow in cyber law at Victoria University, spoke about the obligations of employers, schools, libraries, forum moderators and internet service providers to preserve the privacy of their end-users.

She said it was important to be aware that deleting data did not mean it was removed from a computer system, and that 'deleted' data that could be recovered by specialists needed protecting.

The law had not adapted to the 'deleted'-but-not-'erased' issue, Dr Bayer said. Technology might provide a solution to prevent copying, searching and automatic deletion but, in the absence of a legal response, the issue might be best addressed by an organisation's internal policies.

She said it was especially important in schools and work places that computer users learned not to disclose information about themselves, fellow students or colleagues to unauthorised people or on the web. "This education happens best by way of small-group training, where users are given a short list of very clear instructions, and it is explained to them why it is important to follow those rules."

Speaking at the same 'Defending Data and Protecting Privacy' forum, Michael Burling - Oracle's general manager, security and identity management solutions for the Asia Pacific region - emphasised the importance of managing access to information in the corporate environment.

He said the security issues critical to business continuity had changed from amateur hackers, website defacement, viruses and infrequent attacks in 1996 to the current issues of organised crime, intellectual property theft, identity theft and constant threat of attacks.

Mr Burling said the majority of security breaches occurred from within organisations because of fragmented security policies, leaked passwords, errors and IT administrators who were unaware of organisational and role changes.

At a separate forum, Manukau City Council's Helena Numa spoke about developing a CCTV strategy for local government. She said the council was aware that there was huge public pressure to increase investment in CCTV to combat crime and antisocial behaviour, but it lacked the means to measure effectiveness. There was also a confused public perception - a "silver bullet mentality" - about the benefits of CCTV.

The purpose of the strategy included ensuring there was a clear process to determine appropriate use and implementation, managing demand, ensuring emerging technologies were considered, and meeting privacy needs.

For further forum information, see: www.privacy.org.nz/training-and-education.

Dr Bayer has a PhD in constitutional aspects of internet regulation from Hungary's Eotvos Lorán University. Her research focus is on liability of internet service providers.

Mr Burling's job includes building new opportunities for computer company Oracle's security and identity management solutions.

Helena Numa is adviser (CEO Advisory Unit) at the Manukau City Council. She has been involved in CCTV and crime prevention since being the council's community safety planner 2002-06, which included developing New Zealand's first CCTV strategy for local government.

In this issue:

Human Rights Review Tribunal suggests Police reconsider consent forms for employment "vetting"
- page 3.

02 Case notes

02 A day in the life

03 Assignment to Canada

04 News around the world

04 Law Commission privacy review

04 OPC staff news

Consultation on health code

The Privacy Commissioner is planning to issue draft amendments next month to the Health Information Privacy Code 1994 and will be available at www.privacy.org.nz.

Individuals and organisations interested in making submissions on prospective changes should email submissions@privacy.org.nz. For further information, please contact Sebastian Morgan-Lynch, at the Privacy Commissioner's Wellington office, (04) 474 7590.

Case notes

Disclosure to new employer

Aman complained that a former colleague had disclosed personal information about him to his new employer, a university. He asserted that as a result, his new employer distrusted him, work relations were soured and he eventually resigned. He wanted a significant financial settlement from his previous employer, also a university.

An investigation by the Office of the Privacy Commissioner found that the former colleague had proactively contacted the new employer, saying she believed the man was not suitable for his new job and that he had left under a cloud. This information was mostly opinion, rather than fact.

A provisional opinion was formed that

the university, as the former colleague's employer, had breached Privacy Act principle 11 (disclosure of information) but that the complainant had not suffered adverse consequences sufficient to find there had been an interference with his privacy (see section 66).

There was evidence that the new employer accepted the complainant's version of events and continued to trust him, and that his resignation was not the result of the disclosure.

On the Office's suggestion, the university negotiated a modest settlement with the complainant to acknowledge the principle 11 breach and any embarrassment suffered.

PhD exam correspondence

A PhD student complained to the Privacy Commissioner that she had been refused access to email correspondence between

the examiners of her thesis. In particular, she had requested email correspondence that occurred after the examiners had written their reports but prior to the release of those reports to her.

The university refused the request, relying on Privacy Act 1993 section 29(1)(b), which provides that an agency may refuse to release personal information if it is "evaluative material" and disclosure would breach an express or implied promise that it would be held in confidence.

The Office concluded that the university had a proper basis to withhold the email correspondence because it was evaluative material and releasing it would have breached the examiners' understanding that it was confidential.

See www.privacy.org.nz for full notes.



A day in the life of a privacy enquiries officer ...

By Marilyn Andrew

"Thank you, darling," enthused the effervescent voice of a mature female caller to one of our (male) enquiries officers (yes, they do have their own fan club), so delighted was she with the information she received from him.

I was listening on speaker-phone as part of my training, and the caller hadn't minded at all when she was asked if that was ok. The woman told us she was a member of a local club, and had rung the privacy enquiries line because the club president had told her he had received a complaint about her behaviour. She was shocked to learn this and couldn't recall doing or saying anything that might warrant a complaint. The club president refused to say what the behaviour was, but said that it must not be repeated.

Our caller was advised that under principle 6 of the Privacy Act she could make a request for access to information the club held about her, and that if there was no response within 20 working days or failure to disclose the information to her, she could make a complaint to the Privacy Commissioner. Armed with this information, the woman now felt empowered to approach the club and resolve the dilemma she had suddenly found herself confronted with.

To me, a "newey" to privacy enquiries, this call illustrates part of the valuable service our team provides. We receive phone calls, emails and letters from all sectors of society, covering every spectrum of privacy matters and ranging from the straightforward to the incredibly complex. Details about

each incoming enquiry are logged on our computer system and we also record the advice given and/or the action taken.

We aim to respond to all enquiries promptly and in the sequence in which we receive them. Written enquiries that require consideration naturally take us a little longer to respond to than telephone requests for general information. We make it clear to enquirers that our role is not to provide legal advice, but we do our best to assist where possible and send out a lot of information to help increase people's awareness about the Act and the privacy codes.

Telephone calls can present their own challenges, especially when we deal with enquirers who are distressed, even tearful. Aside from providing information, we realise that an empathetic ear is often what they really require. "Thank you for listening" is a comment we often hear from a grateful caller.

Sometimes, enquiries fall outside the scope of the Act. In such instances, we direct enquirers to the correct agency. However, we can't always help. For example, we were unable to assist a recent caller whose friend was to be released from prison that day. The caller wanted to know what time the bus his friend would be on was expected to arrive in town.

I feel fortunate and privileged to be part of the enquiries team. I have first-class colleagues, and every working day I have the satisfying experience of communicating with fellow New Zealanders about privacy matters important to them.

HRRT questions Police vetting consent form

The Human Rights Review Tribunal has suggested the Police consider reviewing the way they word consent forms for employment vetting.

The suggestion is included in a Tribunal decision (*EFG v Commissioner of Police 48/06*) that found the Police interfered with a man's privacy when revealing an indecent assault court case to an organisation he was contracting to. The man had been discharged under s. 347 of the Crimes Act 1961 (deemed an acquittal). The man's name was suppressed.

The Tribunal ordered the police to pay \$12,500 damages. It also said the case raised issues concerning the Police Licensing and Vetting Service Centre, the purpose of which is to 'vet' prospective employees and contractors who might work with children, young people and vulnerable members of society. About 3000 agencies are registered to use the service.

The Tribunal's summary of facts says the vetting centre checks criminal records and 'notings' recorded on the Police National Intelligence Application. Criminal record information is always released, subject to the Criminal Records (Clean Slate) Act 2004. Applications may be 'red stamped' with the words: *"The Police recommend that this person does not have unsupervised access to children, young people, or more vulnerable members of society"*.

The centre's senior officer, Inspector Joe

Green, told the Tribunal that of 900,000 job applications vetted between 2002 and 2004, 170 were 'red stamped'. He said that about four or five times a year police concluded that although an applicant ought not to be red stamped, prospective employers should know of information held by the Police, and 'notings' were passed on. This is what had happened in this case.

The plaintiff, a trained teacher and from the mid-1970s counsellor and therapist, had in 1990 been arrested and charged with two counts of indecent assault of a girl under 12. The accusations related to events that were said to have taken place at the Auckland Centrepoint Community in 1981.

The Tribunal heard that there were various occasions when police checks were done following the case, but none gave rise to the problems the man encountered in mid-2002 when, for an unknown reason, a copy of the Police noting about his s. 347 discharge was supplied to a counselling organisation that had required a Police check.

The Tribunal accepted evidence from the counselling organisation's director that the man's contract was terminated in April the following year because of other unrelated concerns about his conduct. The Tribunal also heard that the man believed the 'noting' had been disclosed to other potential employers and this made it difficult for him to find work.

After complaints to the Privacy Commissioner in 2003 and 2005, when

the Commissioner took the view that nothing the Police had done constituted an interference with privacy, the plaintiff filed his claim with the Tribunal.

The Tribunal dismissed his claims under Privacy Act principles 5, 9, 10 and 11, but said "in our view the facts establish a clear and substantial breach of principle 8", which imposes an obligation on agencies to check personal information for accuracy, currency, completeness, relevance and whether or not it is misleading.

In relation to principle 5, regarding storage and security of personal information, the Tribunal said it regarded it as "unfortunate" that the Police 'noting' did not include information about name suppression.

"We hope that the Police will consider this aspect of matters and perhaps review their procedures in this regard."

The Tribunal also commented that it had some doubts as to whether the plaintiff had been fully informed about the types of information that might be released when he signed the consent form.

"We wonder whether the Police form for consent to disclosure of information might be improved if there were added to it a statement listing the kinds of information that the Police might potentially be holding - so that anyone who signs the consent knows the kinds of information that might be conceivably held by the police."

For further information see: www.nzlii.org

Assignment to Canada

Assistant Privacy Commissioner Blair Stewart is currently in Canada on a three month Interchange Programme assignment with the Canadian Privacy Commissioner's Office (OPCC).

The Interchange Programme is part of a public service initiative funded by the Canadian Government, and offers great opportunities for the sharing of knowledge across jurisdictions.

Mr Stewart says that while with the Canadian Office he will be assisting with the

29th International Conference of Privacy Commissioners to be held in Montreal in September, and on several projects including some in relation to privacy impact assessment and breach notification.

He says there is a large amount of privacy policy work being done in Canada, both in the OPCC (which has over 100 staff) and within the government, universities and the private sector. Canada is also in the process of reviewing privacy law, with a review of private sector privacy law just completed and a review of public sector law

just starting. "I hope to bring some useful insights back to New Zealand," he says.

New Zealand Privacy Commissioner Marie Shroff says her Canadian counterpart Jennifer Stoddart is extremely pleased to have the opportunity for her staff to benefit first-hand from Blair's extensive knowledge of privacy issues.

"The assignment is an indication of the high regard in which Blair's expertise is held in the international privacy arena," Mrs Shroff says.

News around the world

□ US tech companies Google, Intel, Oracle, Microsoft, Hewlett Packard and eBay have formed the Consumer Privacy Legislative Forum “to support a process to consider comprehensive consumer privacy legislation in the United States”. *Source: www.e-comlaw.com*

□ University of Washington researchers have found that the *Nike+iPod Sport Kit* can do more than track an athlete’s time, distance, pace and calories burned. In a demonstration they showed how the sneaker transmitter and iPod surveillance system could be interfaced with Google Maps to track the wearer. The transmitter can be read up to 60 feet away and broadcasts a unique ID. *Source: www.cs.washington.edu/research/systems/nikeipod/tracker-paper.pdf*

□ Just over half of US teens use social networking websites such as MySpace and Facebook, according to a new Pew Internet & American Life Project study. But according to the researchers, of the 55 percent of those aged 12-17 who have created a personal profile online, 66 percent say their information is not visible to all internet users. *Source: www.news.com*

Law Commission Privacy Review

The Law Commission has begun its four-stage major review of privacy law.

The review is being led by Commission President Sir Geoffrey Palmer. The team also includes Professor John Burrows, an expert on media law and common law rights to privacy, and four research staff.

The Commission says the review is a very complex and wide-ranging project, and it will not be completed until late 2008.

Stage 1 is a high-level policy overview that will set the conceptual framework and help identify issues for more detailed examination in the later stages. The report for Stage 1, scheduled to be published in the second half of this year, will examine privacy values, changes in technology, and international trends, and consider their implications for New Zealand civil, criminal and statute law. This survey will be carried out in conjunction with a similar review of privacy law being undertaken by the Australian Law Reform Commission. In addition, the New South Wales and Victorian Law Reform Commissions are looking at particular aspects of privacy, and the New Zealand review will be informed by their work.

The Stage 1 report will consider different ways of conceptualising privacy, and discuss the implications of political, social and technological change for privacy protection. It will also look at privacy in particular contexts, such as health, the workplace, and the media.

The report will not include specific policy recommendations, the Commission says.

Stage 2 of the review will be concerned with public registers; Stage 3 will examine the adequacy of New Zealand’s civil and criminal law to deal with invasions of privacy; and Stage 4 will be a review of the Privacy Act 1993.

For further information, contact Ewan Morris at the Law Commission: emorris@lawcom.govt.nz or phone (04) 914 4821. Further reports about the review will be included in future issues of Private Word.

OPC staff news

Yvonne Clapham joined the Office of the Privacy Commissioner in January, replacing Alison Donovan as executive secretary to Privacy Commissioner Marie Shroff. Mrs Clapham brings a strong mix of management, administration and financial skills from previous positions with Road Transport Associations, Mitsubishi Motors and United Group. Mrs Donovan has moved to Hawke’s Bay.

Linda Williams joined the Auckland office in January as executive secretary, a new position. She was previously office manager and PA to the executive director in a Marine Industry organisation. She spent a number of years in the UK and completed the Diploma in Management Studies at the University of London.

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.