



Private Word

News from the Office of
the Privacy Commissioner

The new generation: online and uninhibited

As younger people reveal their private lives on the internet, many parents are looking on with alarm.

New York magazine recently compared the sometimes uninhibited online diaries, photos, videos and virtual friends culture on social networking sites such as MySpace with an earlier generation's shock at the advent of rock and roll. The feature article points to many young people's desire for fame, acceptance of risk, and their view that a truly private life is an illusion.

However, a new study by the US Pew Internet and American Life Project (which reports on the impact of the internet on people's lives) has found that most US teens generally refrain from using full names or making their online profiles fully public. Pew reported that two-thirds of teens with profiles on blogs or social-networking sites had restricted access to them, such as

by requiring passwords or making them available only to friends. It also said 45 percent of online teens did not have profiles at all, a figure that contradicts widespread perceptions.

We asked several Wellington teenagers about social networking sites – none said they spent much time on such sites, but all said some friends did.

"I think parents' anxiety about their children's online socialising is unwarranted, but I also agree that many teenagers don't give any thought to the sort of people that could be viewing their profile," one of the 15-year-old boys said. He also pointed out that even a quick Google search can reveal a lot of information.

The New Zealand Internet Safety Group NetSafe has long encouraged parents to engage with their children about internet

use and safety. It is currently carrying out research about how high school students use cyberspace. The research (named 'The Convergence Generation') differs from much of the existing cybersafety research by focusing not only on cyber-risk, but also on resiliency after experiencing risk.

NetSafe Executive Director Martin Cocker says phase one results – looking at year 9 and 10 students' experiences in cyberspace – are due out soon.

The results will inform the development of a questionnaire due to be sent out later this year to about 6000 high school students around the country.

New York magazine: <http://nymag.com>

Pew: www.pewinternet.org

NetSafe: www.netsafe.org.nz

'Social' websites include: MySpace.com, bebo.com, facebook.com, YouTube.com

Page 2: NetSafe advice

In this issue:

Did you know ...

"A mirror image of all New Zealanders' passport data is stored in Australia ..." page 3

02 Consent given for photos

02 Case note

02 "Think carefully" - NetSafe

03 Data "going global"

03 Helping MPs help constituents

04 News around the world

04 Law Commission review of privacy: public registers

International privacy competition

The Privacy Commissioners of New Zealand, Hong Kong, Australia, the Northern Territory, New South Wales and Victoria have launched an international privacy writing competition (essay, poem or blog) for secondary school students.

Jointly hosted by the Asia Pacific Privacy Authorities (APPA), the competition is part of this year's Privacy Awareness Week, 26 August – 1 September, which has the theme 'privacy is your business'.

One of the aims of the competition is to encourage students to consider the importance of privacy in their daily lives, particularly when using websites such as MySpace and YouTube.

See www.privacyawarenessweek.org or www.privacy.org.nz for more information.



Privacy Awareness Week poster.

Consent given for photos

An investigation by the Privacy Commissioner has found that the Nurses' Organisation journal *Kai Tiaki* had fully informed consent to publish photographs in an essay on rest home carers looking after elderly people.

Privacy Commissioner Marie Shroff said the elderly people concerned or their families had known the photographs were to be published in the journal, as part of a project to highlight the work of carers with elderly people in residential care. They had given their consent at each step of the project.

The inquiry followed five complaints to the Privacy Commissioner about the May 2006 *Kai Tiaki* photographic essay.

Mrs Shroff considered that there were potential privacy issues at stake. Since none of the complainants were directly affected by the photography, she launched an investigation on her own initiative under section 13 of the Privacy Act.

The investigation concluded that there was no infringement of the privacy of any of the individuals, but that the case clearly raised a number of ethical questions. "The reality of the public and media environment today is that those of us who do not wish to be captured in the spotlight of public attention need to be increasingly cautious about revealing our personal information," Mrs Shroff said.

For more information see: www.privacy.org.nz

Case note

Malicious informant

A man complained to the Privacy Commissioner after he and his family were stopped and searched by Customs on returning to New Zealand from overseas.

Customs told the man the search was conducted because an 'informant' had claimed he would be carrying drugs. No drugs were found.

The man said it was likely the informant had acted maliciously because of a family dispute, and asked Customs for the informant's name. He said he travelled out of New Zealand frequently and was worried the situation might recur.

Customs acknowledged that it seemed the information had been provided maliciously but refused to reveal the informant's name. The man complained to the Privacy Commissioner about the refusal.

Under section 27(1)(c) of the Privacy Act an agency, such as Customs, can refuse access to personal information under privacy principle 6 if giving access would be likely to prejudice the maintenance of the law, including the preventing, investigation and detection of offences.

Customs relies on the supply of information about possible offences so that it can fulfil its statutory function to protect the borders. If it became known that Customs released names of informants, it would deter people providing information. This does not change if an informant is motivated by malice.

The Office of the Privacy Commissioner acknowledged that the malicious provision of false information created particular concerns for people in the complainant's position. It suggested that under privacy principle 7, the complainant should request that a note of the incident be made on his Customs' records to reduce the chances of serious inconvenience in the future. He did so and Customs attached his statement of correction to his file.

While the man was not wholly satisfied with this outcome, he chose not to pursue his complaint further.

Case Note 92046 [2007]

'Think carefully' advice for young

New Zealand's Internet Safety Group advises young people to think carefully when using social internet sites such as MySpace and Bebo. The following is a summary of its web-based advice.

What you are saying: Your blog, profile and your comments can be seen by anyone who has access to the internet. Do you want everyone reading about the fight you had with your best mate? Or the confessions you thought were private?

Pics of yourself: Who do you want to see you? How do you want to be seen? Would you be ok with your grandma checking out the pics of you at that party? It pays to think really carefully about your pics and to remember that once you put them up there you don't know where they'll go or who will see them.

Pics of your friends: Asking permission before you post a pic of someone else is the decent thing to do. Would you appreciate a mate posting that 'funny' pic of you at the afterball?

Online social networking

1. Be aware that talking online can be disinhibiting. This means that you might

act in ways that you wouldn't offline because you feel like no one will know who you are. Also, the fact that you can talk to people online many times a day can make you feel like you know them really well really fast, even if you don't!

2. Remember that people online can experiment with different personalities and can tell you lies about who they are, where they are and what they want – so just think about whether you really know who you are making friends with.

3. It's smart to be careful with the personal stuff you tell your online friends.

4. Don't add just anybody as a friend. Remember: quality not quantity.

5. Don't feel pressured into responding to comments posted on your page. You wouldn't necessarily talk to just anyone in the street, so why talk to them online?

6. If someone is creeping you out, don't talk to them. Block them and report them to the social networking site you are on.

With thanks to NetSafe. For more information see: www.netsafe.org.nz

Did you know ...

- ❑ A mirror image of all New Zealanders' passport data is stored in Australia to facilitate the advanced passenger processing system.
- ❑ The 'StaffCV' product used by various government departments as part of their online recruitment process uses servers provided, maintained and hosted by Rackspace, a US Microsoft-backed organisation.
- ❑ Some New Zealand home alarms are monitored in Australia.
- ❑ Credit reporting company Veda Advantage, (formerly Baycorp Advantage) has been developing plans to store its financial and credit information – about pretty much all of us – on its databases in Australia.
- ❑ Most banks in New Zealand are Australian-owned, making it likely that information is held in Australia. Overseas call centres may also hold some New Zealanders' personal information.
- ❑ Concerns have been raised about the international banking network SWIFT (Society for Worldwide Interbank Financial Transactions), which supplies services and software to over 7900 financial institutions in more than 200 countries. A report by the Canadian Privacy Commissioner noted that "an organisation that has legitimately moved personal information outside the country for business reasons may be required at times to disclose it to the legitimate authorities of that country".
- ❑ International airline passenger information is transmitted electronically from travel agencies worldwide to Atlanta. The US Department of Homeland Security has sought access to it for security and anti-terrorism purposes.
- ❑ The US Patriot Act potentially allows the US Government to access any personal information sent to or stored in the US. It also prohibits public and private sector organisations from saying whether information has, in fact, been accessed.

From Privacy Commissioner Marie Shroff's GOVIS speech – see top right of this page.

Data going global

The huge growth in government sector information matching programmes, as well as cross-border data flows, were highlighted by Privacy Commissioner Marie Shroff when speaking to the Government Information System Managers' Forum (GOVIS) last month.

"One of the original purposes of the Privacy Act was to make sure government information matching programmes are monitored. That need is more acute now than when the Privacy Act was passed in 1993," Mrs Shroff said. At that stage there were just three information matching programmes – for the 2005/06 year there were 76 authorised programmes recorded, of which 46 were active.

"These figures represent a phenomenal growth in both the number and range of data matching being conducted by government. And yet I suspect few New Zealanders are aware of that escalation. Apart from the simple increase in the number of matches, and the range of agencies involved in matching work, there are matches which involve data being sent offshore."

On top of this is private sector data matching and overseas flow – the size and scale of both is unknown.

Mrs Shroff said the speed of developments

– and the natural tendency of the law to follow rather than lead – meant New Zealand was scrambling to provide adequate controls.



Marie Shroff

"I am conscious that law-making in this area is difficult, partly because some of the incursions are small and apparently annoying rather than harmful in themselves but they have widespread impact, which ultimately can amount to a significant level of social harm (spam might be an example). I liken it to 'privacy pollution', where each harmful action contributes in a small way to a thick grey cloud of contamination of our privacy environment."

The Privacy Act was fortunately 'technology neutral', but there was not much chance of enforcing the Act's good information handling provisions where data was sent overseas, Mrs Shroff said.

"We are all confronting the business pressures to do more with less, to work smarter and faster and more efficiently. These are not new pressures, but they test us in novel ways because we are living and working in an online, interconnected age where information has become the currency."

Full speech available at www.privacy.org.nz

Helping MPs help constituents

Government agencies face daily requests for personal information, including some from MPs acting on behalf of constituents. While departments have a responsibility to protect personal information, they do not need written authorisation to begin looking into matters raised by MPs on behalf of constituents.

This advice from the Privacy Commissioner follows concerns from an MP that when he or his electorate agent approached government agencies on behalf of an individual constituent, the agencies often insisted on written authorisation from the constituent before looking into the matter.

Under Section 45 of the Privacy Act, agencies are required to ensure a person claiming to be acting on behalf of someone else is properly authorised to do so. This does not necessarily mean an agency must insist on written authorisation.

Ordinarily there will not be any reason to doubt that a constituency MP is properly authorised. The following practical suggestions may assist government agencies with such requests: start looking into the concerns straight away; contact the constituent directly and ask if s/he is happy for personal information to be disclosed to the MP; and/or consider whether information could be sent directly to the constituent.

News around the world

□ Citing US federal privacy law, MySpace.com has said it will not comply with a request by letter from eight state attorneys general to hand over the names of registered sex offenders who use the social networking website, saying it would only do so when proper legal processes were followed. MySpace also said it had recently used new software to remove “every registered sex offender that we identified out of our more than 175 million profiles”. *Source: Privacy Times*

□ UK Civil liberties groups are warning that the details of every Briton could soon be on the national DNA database, raising fresh concerns of a ‘surveillance society’. Controversial plans being studied by the British Government would see the DNA of people convicted of even the most minor, non-imprisonable offences, such as dropping litter, entered on the national database. The proposals are part of a wide-ranging government review of the Police and Criminal Evidence Act (Pace), which campaign groups warn may have profound ramifications for society. *Source: guardian.co.uk.*

□ The UK’s first police “spy drone” has taken to the skies. The remote control helicopter, fitted with CCTV cameras, will be trialled in Merseyside to track criminals and record anti-social behaviour. The spy plane was launched as a senior police officer in Hampshire warned that the surveillance society in the UK is eroding civil liberties. Assistant chief constable Simon Byrne responded: “People clamour for the feeling of safety which cameras give.” *Source: guardian.co.uk.*

□ A survey of 1,200 UK consumers found that more than half are reluctant to shop at businesses, both online and brick-and-mortar, that have experienced security breaches. Forty-five percent do not believe banks and retailers are taking adequate measures to safeguard customer data. Overall, 14 percent of respondents said they had been victims of data theft. One third of the respondents did not offer personal information online, yet 11 percent of them had still experienced identity fraud. *Source: www.theregister.co.nz*

Law commission review of privacy: public registers

Stage 2 of the Law Commission’s review of privacy focuses on public registers.

The recent heated debate in the press about the Births, Deaths, Marriages and Relationships Registration Amendment Bill has brought public attention to the issue of whether (and to what extent) public registers should be open to public inspection.

The Law Commission is researching the reasons for the existence of public registers, and their accessibility to the public. It is also looking at what constitutes a “public register” (as defined in the Privacy Act 1993 and in some overseas jurisdictions), and considering various categories of public register and statutory provisions protecting personal information in registers.

The Commission has devised and sent a questionnaire to the main agencies responsible for maintaining public registers, asking (amongst other questions) about

the purposes of the register, access and any problems or issues, especially since computerisation of the registers. Most agencies have responded helpfully and thoroughly, and these responses will inform the inquiry, particularly as to current perceived issues. The Commission will also talk to some users of registers and individuals whose personal information is listed on registers.

By late August, the Law Commission plans to have completed a consultation document outlining options for solving the problems identified.

□ *For any enquiries, please contact Janet November (phone 04 914 4801) or Rachel Hayward (04 914 4811) at the Law Commission, Wellington.*

□ The Privacy Commissioner has made a submission on the Births, Deaths, Marriages and Relationships Registration Amendment Bill. This will be outlined in a future issue.

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.