

Privacy: myths and realities

Privacy Commissioner Marie Shroff has urged social agencies to use common sense – and not take a ‘blame the Privacy Act’ approach.

Speaking at the *Keeping Kids Safe* Presbyterian Support National Conference in April, she said the key thing was to turn your mind to the various interests involved and reach a reasoned position.

Mrs Shroff said there were a lot of myths about the Privacy Act. “It is not about keeping secrets. It is not just yet more political correctness. It is not about stopping good people from doing their jobs properly. If you feel confident you have made your best efforts and tried for a reasonable position, you’ll be unlikely to be too far off the track.

“For example, if a young child runs away from home, of course their parents or guardians should be informed where they are, unless there are very strong reasons not to do so – such as that breaching the child’s confidence would somehow be contrary to the child’s best interests.

“The need to protect a person’s safety is also a very strong reason for disclosing information, even when that would mean breaching a confidence – though you need strong reasons to breach the confidence of someone 16 years or older if they are safe where they are.”

Mrs Shroff emphasised the importance of developing information-handling policies. “Privacy law covers areas where there are competing interests. Balances need to be struck, and there may be no easy answers in complex situations. But if you have a clear, well thought through privacy policy, are transparent about it and act in accordance with it, you will be on firm ground.”

Mrs Shroff noted that social workers and police officers could disclose information where that was one of the purposes for holding the information in the first place, for instance, for the care and protection of children or, in the case of the Police, law enforcement and prosecution. (Disclosure must not be excessive or include unnecessary information.)

She also noted that the Privacy Act could be overridden by legislation that specifically allowed for the disclosure of some personal information, such as provisions in the Children, Young Persons and Their Families Act 1989 covering the care and protection of children.



Newborn screening

Privacy Commissioner Marie Shroff, speaking at a recent National Screening Unit (NSU) Screening Symposium, said there was a strong need for legislation or other regulations to govern the use of the genetic information held on the newborn metabolic screening database.

Mrs Shroff said, “DNA testing is only going to get easier and cheaper. Demand for tests – of all varieties – will certainly grow. There will be pressure to make specimens such as the Guthrie blood spots available for other purposes.

“Effective and ongoing participation in the programme is dependent upon building and maintaining high levels of trust within the community.”

Newborn metabolic screening is available to all New Zealand babies and done at 48 hours after birth. The sample includes information about the baby, such as its name, sex, date and time of birth, National Health Index number, the mother’s name, and contact details for the Lead Maternity Carer.

Although, parents are now asked to give consent on behalf of the child to have a blood sample taken, there are no clear rules about the indefinite storage and future uses of the data.

A 2003 report issued by the Office of the Privacy Commissioner noted the range of information able to be obtained from old blood samples, the growth of a huge database of blood samples, and the absence of a clear, legal protection of the samples against third party access and future uses.

The National Metabolic Screening Programme Advisory Group to the NSU is considering a number of options for retention and secondary uses of the samples, and is expected to make recommendations towards the end of May. NSU staff have said they will then consult with the Office of the Privacy Commissioner about how best to proceed.

In this issue:

Case notes | 02

Exploring identity and privacy | 03

SSC initiatives | 03

List Warrant Register | 03

Privacy Awareness Week | 03

News around the world | 04

Education unique identifier | 04

New tech team leader | 04

Case notes

DHB DENIES FATHER ACCESS TO INFORMATION

A 14-year-old boy suffered from a life-threatening psychological condition and was hospitalised. His parents had separated, but both had been involved in his care.

Differences of opinion arose between the boy's father and doctors at the district health board (DHB) about the treatment the boy was receiving, and the father's level of involvement in that treatment.

The boy's father requested access to all the information that the DHB held about his son. The DHB provided most of the information, but withheld some on the basis that the disclosure would be contrary to the boy's interests.

The father was his son's representative, and an agency is allowed to refuse a representative's request in some circumstances. Those circumstances are specified in section 22F of the Health Act, and in rule 11(4)(b) of the Health Information Privacy Code. Rule 11(4)(b) of the Code states that an agency may refuse the request if:

- (i) the disclosure of the information would be contrary to the individual's interests;
- (ii) the agency has reasonable grounds for believing that the individual does not or would not wish the information to be disclosed; or
- (iii) there would be good grounds for withholding the information under Part 4 of the Privacy Act if the request had been made by the individual concerned.

The Privacy Commissioner was satisfied that the DHB had balanced the father's rights with the need to withhold certain information. The DHB gave the father most of the information it held about his son, and also involved the father in meetings, provided summaries, updates and so on. It kept the minimum amount of information back on medical grounds. The son's doctors made a careful decision that giving the father the remaining information would be contrary to the son's interests. The reason was because it could actively harm the son's recovery for the father to have complete access.

The Privacy Commissioner stated that it would have been inappropriate for her to substitute a non-medical view for this properly considered medical opinion.

Case Note 95042 [2008] NZ PrivCmr 1

COVERT RECORDING USED IN DISCIPLINARY ACTION

A man and his colleague were employed by a care agency, working as caregivers for clients with disabilities. They worked as a team, looking after clients in their own homes.

The colleague became concerned that the way the man spoke to clients was sometimes abusive and inappropriate, and that this posed a safety risk to those clients.

Using his cell phone, the colleague recorded the man's conversations with clients and gave the recording to the employer. The man was unaware that he had been recorded. The employer then used the recording in disciplinary proceedings against the man, who was given a warning.

The man complained to the Privacy Commissioner about the fact that he had been covertly recorded.

Principle 4 states that personal information must not be collected by means that are unlawful, unfair, or intrude to an unreasonable extent upon the personal affairs of the individual concerned.

The Privacy Commissioner accepted that the colleague had serious concerns over the man's behaviour with clients. Those clients, who were unable to protect themselves, were potentially at risk as a result of the behaviour. Without the recording, the employer would have had to judge what the man had said to the clients without any clear evidence. Notes alone would have been less accurate. The recording only occurred on one occasion.

On the other hand, covert recording is intrinsically intrusive, and needs strong justification for its use. The colleague could simply have told the employer what he saw and heard.

The Privacy Commissioner decided that there was no breach of principle 4 here. The allegation was serious, and there was a risk of harm to the clients. They were not in a position to make a complaint to the employer on their own account. On balance, this was one of the rare occasions where it would be acceptable for an onlooker to make a covert recording to ensure that evidence of what was said was accurately captured. While it would have been less intrusive to simply report the incident to the employer, the best way of ensuring the safety of the clients in this instance was to record what was said.

However, the Privacy Commissioner cautioned the employer that such a recording should not generally be seen as acceptable. She recommended that the colleague and other employees should be discouraged from using cell phones to covertly record conversations.

Case Note 101213 [2008] NZ PrivCmr 4

UNIVERSITY DISCLOSES STUDENT'S LOCATION

The New Zealand Police contacted a university to obtain information about a student because they were attempting to serve the student with a notice of intention to revoke his firearms licence.

The Police informed the university that they had serious concerns for the student's mental health and needed to know where he was. The university disclosed the man's home address, but the Police could not find him there.

Upon a further request by the Police, the university revealed where and when the student would be sitting his examinations. This enabled the Police to find him and serve him with the notice.

The man complained to the Privacy Commissioner about the disclosure of this information to the Police.

Principle 11 of the Privacy Act states that an agency that holds personal information must not disclose that information unless an exception applies.

In this case the university acknowledged it had disclosed the information but stated that principle 11(e)(i) allowed it to do so. Principle 11(e)(i) permits the disclosure of personal information if the agency reasonably believes disclosure is necessary to avoid prejudice to the maintenance of the law by any public sector agency.

In the circumstances the Privacy Commissioner was satisfied that it was reasonable for the university to believe it was necessary to give the Police the information. The university knew that the Police were having difficulties locating the student, there were growing concerns about him, and there was urgency in the Police's need to locate him.

Case Note 97705 [2008] NZ PrivCmr 3



Exploring identity and privacy

"Today, we are at the cusp of very real and significant change: socially, technologically and politically. Identity and the way we manage it will define our era," said Privacy Commissioner Marie Shroff, who was a keynote speaker at an international conference on identity management held in Wellington 29-30 April.

The conference focused on state-of-the-art thinking, research and practice around managing identity.

Mrs Shroff explored the nature of identity, how one's identity changed over time, and why people cared about it. She noted that identity was at the very heart of what it meant to be human.

Identity management involved aspects of social control and placed some constraints upon the individual. "We are then confronted with questions about who should rightly perform that role in New Zealand," she said.

"Identity is both a means of control and a means of self-definition; in a social context, and in a government or business context.

"Increasingly, identity management is a central matter for us all. We are asked – or required – to identify ourselves in all sorts of arenas. We may dislike this. Technology today is a 'creator of identity'."

In considering who should manage identity in New Zealand, Mrs Shroff noted the peculiarities of New Zealand. New Zealand did not have the large and prominent civil liberties groups that played such a part in the US context, and New Zealanders were enthusiastic about new technology but also highly individualistic and averse to regimentation and privacy invasion, she said.

"Identity-driven systems must reflect the multiplicity of modern New Zealand. Those systems must give people options, flexibility and control." Mrs Shroff added that across both public and private sectors, there was recognition that policy and systems that were designed today needed to be future-proofed for 21st century needs.

"Our challenge will be to design systems that support our identities – however we choose to define them."

E-govt initiatives

The State Service's Commission's (SSC) Information and Communication Technologies Branch (ICT) will be split in two and the all-of-government operations moved to the Department of Internal Affairs. The first stage of the split is due to begin 1 July 2008.

Meanwhile, a new government initiative known as igovt, jointly led by SSC and the Department of Internal Affairs has been launched.

igovt is an identity verification service that will verify a person's identity – online and securely – giving the user access to government services, such as applying for a student loan.

It will only verify someone's identity to another government agency at the user's request and with their consent, using only the minimum identity information each time.

For more information check out the new website www.i.govt.nz.

Marketing lists

A large number of New Zealand marketers use lists compiled by a list company for their own campaigns. The Marketing Association says that while there are good quality lists, which have been sourced legally, some lists contain information about people who have not given permission for their details to be passed onto other organisations.

The List Warranty Register (LWR) has been set up by the Data Advisory Network, a special interest group of the Marketing Association, to help avoid problems using such lists. The Association said that it had been difficult for marketers to be confident in using the list data for marketing purposes.

The LWR provides an assurance by list owners that they are compiling, using and/or maintaining lists in a way that is compliant with the Privacy Act 1993, and the Marketing Association's Codes of Practice and Best Practice Guidelines.

A list owner company can sign a warranty contract and, providing the Marketing Association is satisfied that the company fulfils the required warranty conditions, the list owner will be accepted as LWR registrant. Once accepted, the list owner can communicate their status to their prospective list users. Verification that a database is LWR approved can be checked on the Marketing Association website www.marketing.org.nz/list-warranty-register.

Source: Marketing Association, April 2008

Privacy Awareness Week

24-30 August 2008

Video competition for secondary school students

The Privacy Commissioners of Australia, Hong Kong, New Zealand, Canada, the Northern Territory, New South Wales and Victoria have launched an international video competition for secondary school students. Students are invited to make a short video about privacy. Prizes include a video camera and gift vouchers to the value of approximately \$3,000.

The competition closes on 25 July 2008. The winners will be announced during Privacy Awareness Week. Further details of the competition are available at www.privacy.org.nz or email competition@privacy.org.nz.

Privacy forum

Keep your diaries free for Wednesday, 27 August 2008. The Office of the Privacy Commissioner will be hosting a day-long privacy forum, to be held at the Intercontinental Hotel Wellington. Programme and registration details will be available soon at www.privacy.org.nz.

News around the world

- Where are you? A new mobile phone service allows you to be located by a friend with an electronic map showing your location. The Social Network Integrated Friend Finder (Sniff) is an application, accessed via Facebook or mobile phone that provides users with a detailed map of their friends' locations. The phone sends a signal to nearby base stations and positioning software converts the information into a geographical location. *Source: www.theaustralian.news.com.au*
- Sir Tim Berners-Lee, creator of the world-wide web, said he did not want his internet service provider to track which websites he visited. "I want to know if I look up a whole lot of books about some form of cancer that it's not going to get to my insurance company and I'm going to find my insurance premium is going to go up ...," he said. His remarks came after Facebook was widely criticised for introducing a system called Beacon, which sends data from external websites to Facebook. The company changed the way Beacon operated after an uproar from customers so that users now have to opt into it. *Source: NZ Herald*
- Patients concerned about potential genetic health issues are avoiding DNA testing out of fear that they will be denied insurance. Linda Vahdat estimated that 20 percent of her patients at the New York-Presbyterian Hospital chose to pay with cash for the DNA test for inherited breast cancer risk, to avoid submitting insurance claims. Last year, hundreds of customers paid a DNA testing company for tests to ensure that no third party, even a doctor, had access to their results. *Source: Privacy Times Volume 28 Number 5 March 1, 2008*
- A murderer in the US, who had killed ten people and had eluded police, was caught after the DNA of his daughter led to his arrest in February 2005. Investigators obtained a court order for a Pap smear specimen the daughter had given five years earlier. A DNA profile of the specimen almost perfectly matched the DNA evidence taken from several of the crime scenes, leading detectives to conclude that she was the daughter of the killer. This case was an early use of an emerging tool in law enforcement – analysing the DNA of a suspect's relatives. *Source: www.washingtonpost.com*
- Thousands of US citizens have wrongfully been declared dead due to an average of 35 data input errors per day by the Social Security Administration (SSA). Many other agencies rely on the data provided by the SSA, such as the Inland Revenue Service (IRS). People who have been wrongfully declared dead face many problems, such as rejection of tax returns, cancellation of health insurance, and closure of bank accounts. Social Security says an erroneous death record can be removed only when it is presented with proof that the original record was entered in error. *Source: www.msbcn.msn.com*

Education unique identifier

The Privacy Commissioner is proposing to revoke the Post-Compulsory Education Unique Identifier Code as she believes that it has been superseded by Part 30 of the Education Act 1989. The Commissioner is now consulting on the proposed revocation and asking for submissions.

For more information and a copy of the consultation discussion document, please go to www.privacy.org.nz, email code@privacy.org.nz, or call 0800 803 909. Submissions close Friday, 4 July 2008.

New technology team leader

Rosie Byford (*pictured right*) has recently joined the Office of the Privacy Commissioner as the new Team Leader (Technology).

Rosie came from the Ministry of Research, Science and Technology, and also brings with her UK policy experience.

She will lead the team responsible for monitoring information matching and policy related to technology and privacy.



Winner

Congratulations to Greg Robins, Wellington, winner of the Private Word survey book prize draw.

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 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 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.



Privacy Commissioner
Te Mana Matapono Matatapu