

Cloud computing

In the first of a series of lunchtime technology and privacy forums about 'cloud' computing, Scott Houston, of Intergrid and the New Zealand Supercomputer Centre, showed how the 'cloud' has turned computing power into a commodity.

Cloud computing is a vast reservoir of computing storage and processing power that is accessible over the internet, so that anybody can connect to it from work, home or mobile devices. The cloud provides remote storage that allows people to access their information from anywhere and also offers the processing power to get a large amount of analysis done quickly. This memory or processor capability is rented by the user – as and when they need it. The cloud is always on and always available.

Cloud computing services are provided by companies such as Google, Amazon, Sun, the New Zealand Supercomputer Centre and any other vendor with power or space to spare. Google's Gmail is an example of a cloud computing service that is widely used. An individual's desktop (if they still have one!) or their games console could become part of the computing cloud, sharing its power with others.

Mr Houston described how using the cloud could provide immediate and flexible access to computing power, reducing the need for agencies to invest in large amounts of fixed hardware.

He also explained that this came with hidden costs, such as the cost of data transfer. If an agency is sending and receiving large amounts of information over the internet, data transfer costs soon add up.

There are potential risks in cloud computing, particularly about the control over information. Information stored in the cloud may include a company's intellectual property, or personal information. Users of cloud services should consider what data they want to put into the cloud and how they can anonymise or encrypt it.

As cloud services evolve, the ability to choose the physical location of where an agency's data will be stored may become more commonplace – allowing informed users to pick territories with similar laws or cross-jurisdictional agreements relating to privacy and information management.

See <http://tinyurl.com/4vobzd> for the full presentation.



Cartoon: Slane and Sanson, 2008

Guthrie cards – what next?

The Privacy Commissioner has made a submission to the National Screening Unit (NSU) about the collection, retention and secondary use of the newborn bloodspot samples.

The submission looks at questions like the appropriateness of a fixed retention period and how long samples should be kept for secondary uses – indefinitely or for a specific time.

The Privacy Commissioner also addressed the need for legislation to regulate secondary use of samples and ongoing governance. She said there were also concerns about the information that was currently available to new parents and the consent gathering process.

The NSU carried out public consultation last year about the collection and use of the samples, and this year held stakeholder meetings and workshops to explore policy options. Recommendations will be made to the Minister of Health.

There is no specific legislative framework governing the operation of the programme, and currently the blood spot cards are retained indefinitely.

In this issue:

Case note | 02
Mosley v News of the World

Protecting world privacy | 03
DNA databases shut

Using offshore ICT providers | 03
Australian privacy law reform

Screening programmes and genetic research | 03

News around the world | 04
Privacy Awareness Week 2009

Security breach workshop | 04
Privacy Commissioner reappointed

Case note

COUNCIL CHARGES LAWYER FOR RATES INFORMATION

Instructed by a couple to complete the sale of their property, a lawyer requested from the Council details of the property's annual rates and whether all the instalments had been paid.

The Council provided a copy of the property details and charged a "Rates Enquiry Fee" of \$25. The lawyer queried this fee and the Council advised that it was a standard charge for business enquiries.

The couple complained to the Privacy Commissioner that the information requested by their lawyer was personal information, not a business enquiry. They didn't think that the Council was entitled to charge for this.

It is common practice for lawyers to request information on behalf of their clients. The Privacy Commissioner's view is that these requests should be treated as if they are made by the clients themselves.

The Privacy Commissioner was satisfied that the details of the couple's property and payments were personal information about them, and pointed out to the Council that section 35(1)(e) of the Privacy Act prevents public sector agencies from requiring payment when making information available under principle 6. The Council, as a public sector agency, was subject to this section.

The Privacy Commissioner considered that the Council had breached principle 6 by charging the couple's lawyer. As a result, the Council no longer charges for providing information in these circumstances. It also refunded the fee. The Council was willing to contribute to the couple's legal fees, but the lawyer suggested it provide some seasonal fruit instead.

Case Note 10318 [2008] NZ PrivCmr 8

Mosley v News of the World

Ursula Cheer, Associate Professor, School of Law, University of Canterbury, considers a high profile UK privacy case.

In March 2008, the *News of the World* published a story "FI Boss has Sick Nazi Orgy with 5 Hookers" about Max Mosley, president of the FIA (the governing body of the Formula One industry). It contained lurid details of a sex party involving five prostitutes. Accompanying video footage, secretly obtained, of the alleged orgy was placed on the newspaper's website. Mosley sued the newspaper for breach of privacy and was awarded the highest damages to date for a privacy claim in Britain – £60,000.¹

Mosley shows that some public figures will be prepared to sacrifice their privacy further in order to show that their privacy was breached in the first place. And, the message to the tabloid media in Britain is that 'kiss and tell' stories are difficult to justify in the public interest.

Mr Mosley easily established that he had a reasonable expectation of privacy. Mr Justice Eady said, "...anyone indulging in sexual activity is entitled to a degree of privacy especially if it is on private property and between consenting adults (paid or unpaid)".²

Mosley also illustrates that immorality, and sometimes even criminal behaviour, does not prevent the courts from recognising and protecting a person's right to privacy. Even those whose behaviour appears abhorrent or unconventional are entitled to privacy, so long as they have behaved generally within the law.

News of the World argued that a number of crimes had been committed during the party. Mr Justice Eady rejected this and concluded that: "...it is not for the state or for the media to expose sexual conduct which does not involve any significant breach of the criminal law ... It is not for journalists to undermine human rights, or for judges to refuse to enforce them, merely on the grounds of taste or moral disapproval".³

The newspaper argued that the sexual behaviour had a Nazi and concentration camp theme and that there was a public interest in exposing this. Mr Justice Eady said

there would be public interest in such a theme because Mr Mosley had to deal with many races and religions as FIA president, and he had in the past spoken out about racism in the sport. However, Justice Eady concluded there was no Nazi theme to the activities.⁴

The newspaper also argued that it was in the public interest to know the general depravity and adultery displayed. But this, too, was rejected because the behaviour did not fall into any of the categories of public interest previously recognised in the UK (such as exposing criminal activity or public hypocrisy). Nor did it meet the higher standards set by European jurisprudence.⁵ Therefore, it seems clear that disclosure of minor criminal activity (such as smoking 'a spliff')⁶ or of behaviour which can only be judged in a moral sense, will be difficult to justify in the public interest.

Justice Eady identified the purpose of damages in privacy claims as connected to personal dignity, autonomy and integrity.⁷ But he said exemplary damages were not applicable to privacy claims in the UK because such claims had developed in the context of breach of confidence rather than a tort like defamation.⁸ This may not be the case in New Zealand where privacy is developing as a tort in its own right.

Post script: Mr Mosley took a case in October to the European Court of Human Rights to force a change in British law that would require newspaper editors to contact the subjects of any revelations before publishing allegations about their private lives. Source: nzherald.co.nz

¹ *Mosley v News Group Newspapers Ltd* [2008] EWHC 1777 (24 July 2008).

² See n. 1 above, [98].

³ See above, n. 1, [127]. See also [128].

⁴ *Mosley*, n. 1 above, paras [122]-[123]. The defendant was not helped when its main witness, Woman E, the participant it had promised to pay to secretly film Mr Mosley, was unable to give evidence in the case.

⁵ *Ibid*, para [131].

⁶ *Ibid*, para [111].

⁷ See n. 1 above, paras [214]-[217].

⁸ *Ibid*, [197].



Protecting world privacy

"Protecting privacy in a borderless world" was the theme at the 30th International Data Protection and Privacy Conference held in Strasbourg in October.

Bringing together 78 data protection authorities and privacy commissioners, the conference aimed to identify major challenges arising from protecting privacy in an international context that is subject to rapid technological, political, legal and international developments.

Prompted by the success of Asia Pacific Privacy Authorities' Privacy Awareness Week and the European Data Protection Day (held on 28 January 2008), the conference agreed to work on a proposal to have a global privacy day.

For more information see: www.privacyconference2008.org

Using offshore ICT providers

The State Services Commission has released draft guidance for government agencies looking at using offshore ICT providers.

Government Chief Information Officer (CIO) Laurence Millar says the guidance will assist agencies when considering offshore providers as an option to improve service delivery.

"Many agencies are looking at the way they handle information and whether it is appropriate to use offshore ICT providers to manage that data," Mr Millar said.

"The guidance we've produced identifies key risks associated with sending government data offshore or outsourcing data processing and management services offshore. We offer some possible suggestions for mitigating those risks that departments can consider."

Source: www.e.govt.nz/resources/news/2008/20081014.html

Australian privacy law reform

An Australian Law Reform Commission's report *For Your Information: Australia Privacy Law and Practice* recommends 295 changes to that country's privacy laws and practices. The three-volume, 2700 page report is the culmination of a massive research and consultation exercise conducted over two years.

Law Commissioner Professor Les McCrimmon said that the extensive consultations had revealed that Australians cared about privacy and wanted a simple, workable system that provided effective solutions and protections. To see the full report go to www.alrc.gov.au.

Source: *LawTalk 717 29 September 2008*

DNA databases shut

Several DNA databases run by the US National Institutes of Health (NIH), the Wellcome Trust in London and the Broad Institute in Massachusetts were closed to public access at the end of August after researchers showed it was possible to extract the supposedly confidential identities of patients involved.

The concern is with studies in which researchers pool genetic data from hundreds of people to look for broad patterns of genetic inheritance. Because the pool consists of DNA from so many people, the assumption has been that it would be impossible to identify any one individual's DNA. The new study suggests that is not the case.

The greatest concern is that identifying an individual this way could reveal sensitive health information. Genome-wide association studies compare data from people with and without a particular disease, so knowing which pool a person falls into can convey whether they have, for example, cancer, diabetes or multiple sclerosis.

However, the likelihood of privacy breach is considered low, largely because the pooled data must be matched against a particular person's isolated DNA – something that, currently, only researchers generally have access to. As genetic information proliferates, it could be more of a concern five or 10 years from now.

Sources: *SCIENCE Vol 321, Scienceexpress / 4 September 2008, Nature Vol 455*



Researcher with DNA Sequencer

Screening programmes and genetic research

Screening programmes and genetic research featured at the Privacy Issues Forum in August.

Richman Wee, project manager and a researcher for the Human Genome Research Project, University of Otago, pointed out that anonymisation in genomic research might not be sufficient or in keeping with participants' interests or wishes, and might not be truly achievable in the near future.

Advances in genomic technologies with sequencing individual genomes, recent findings from health research involving genome-wide association studies, and changing societal and ethical expectations are triggering a rethink about privacy safeguards.

News around the world

- The UK Government's first identity cards have been unveiled. The controversial biometric card was issued in November, initially to non-EU students and marriage visa holders. The cards include the individual's name and picture, their nationality, immigration status and two fingerprints. Critics say that the roll-out to some immigrants is a "softening up" exercise for the introduction of identity cards for everyone. *Source: www.news.bbc.co.uk*
- Quebec businessman Mario Labbé, whose name is one of the many that have erroneously landed on the US Department of Homeland Security's flight passenger watch list, decided to legally change his name to avoid lengthy security hassles at the airport. In 2004, Labbé was placed on the Homeland Security's watch list after falling victim to identity theft. At the time, the department said there was no way for his name to be removed. Labbé legally changed his name to François Mario Labbé, which proved enough to foil the US customs computers. *Source: www.cbc.ca/news*
- A Marks & Spencer employee told the mother of a seven-year-old that the shop could not talk to her about the delivery of her son's Superman suit because it would infringe his data protection rights. The UK Information Commissioner's Office said this was a clear example of a "data protection duck out" – using the Data Protection Act as an excuse when dealing with enquiries from customers. *Source: www.ico.gov.uk*
- A former FBI undercover agent, Joe Pistone, warned that Russian and Italian Mafia were using data from websites to launch attacks against businesses and individuals. He added that social networking site users who included their work details in personal profiles were allowing organised crime gangs to identify them and their company. *Source: www.computerweekly.com*

Privacy Awareness Week 2009

Privacy Awareness Week (PAW) will be moved forward to May next year. "This is a good move for the Asia Pacific Privacy Authorities (APPA) as it means Canada and British Columbia will be able to join in from now on," said Privacy Commissioner Marie Shroff.

International links for privacy professionals

The International Association of Privacy Professionals Australia and New Zealand (IAPP ANZ) chapter was launched during Privacy Awareness Week.

IAPP ANZ is affiliated with the International Association of Privacy Professionals (IAPP), the world's largest association of privacy professionals. Based in York, Maine, USA, the organisation represents over 5000 members from business, government and academia across 32 countries.

The launch of the new chapter recognises the many issues in protecting personal information in an increasingly borderless world. See www.iappanz.org for more information.

Security breach workshop

A workshop on the Privacy Commissioner's Data Breach Notification Guidelines will be held in Wellington on Friday, 21 November.

The workshop will provide participants with an overview of data breach notification and the opportunity to work through several data breach scenarios. For more information and to register see www.privacy.org.nz/workshops.

Privacy Commissioner reappointed

The Governor-General has approved the reappointment of Marie Shroff as Privacy Commissioner for a further five years.



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

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