Australia: state of play in a changing environment

Recent highly publicised privacy breaches affecting Australian citizens have highlighted the legal and technological limitations of the current privacy framework. Kevin Shaw and Malcolm Crompton examine national and regional developments addressing privacy concerns.

The CardSystems, ChoicePoint and other well known incidents in the USA have had direct impact in Australia. The recent CardSystems breach is reported to have affected 130,000 Australian credit card holders, one of the 'big 4' banks was forced to reissue 11,000 compromised cards and had 400 customers actually compromised, while other banks had to reissue between 1000 to 3000 cards each. Interestingly, it was the superior system for detecting patterns of fraud in one of the Australian banks that resulted in it being one of the first to sound the alarm about a privacy breach of unprecedented scale.

These incidents and the claims in the UK that personal information was for sale in India led to an Australian TV program also buying stolen Australian customer data there. The journalists were able to purchase personal information on Switch Mobile customers in India, including Drivers licences, passport numbers and birth certificate details. The program showed an Indian data broker selling the names, addresses, telephone numbers, birth certificate details, driver's licence numbers, Medicare numbers and ATM card numbers of Australian customers. This incident is still under investigation by the Australian Privacy Commissioner.

All these incidents should be seen against the volatile environment in Australia for considering privacy issues ever since the so called 'Australia Card' proposals of the 1980s. These proposals were first proposed by the Labour Government of the time but were successfully opposed by a broad community of interests in which our current Prime Minister played a prominent role. Identity management is still a particularly sensitive issue for governments in Australia as a consequence. It also means that when incidents occur or proposals come up that appear to compromise privacy, the media is on a short fuse to highlight the issues, even in the more recent environment overshadowed by efforts to contain terrorism.

Other recent incidents have also contributed to the debate.

The difficulties of the Victoria Police in recent months are the most noteworthy. The Government of Victoria faces a potential payout of up to A$145 million to individuals whose sensitive police files were leaked in one of the biggest breaches of privacy in the state's history.

In the first incident, Police indicated a worker at IBM, who conduct audits of the police 'Law Enforcement Assistance Program' (LEAP) Database, had emailed information, believed to include the full name and addresses of some victims of crimes and alleged offenders, to a prison officer-turned-whistleblower who had applied to see his file. The former prison officer is reported to have then received up to 1,000 files on others who shared his surname.

The prison officer had been trying for 21 months to find out who had inappropriately accessed his personal file. On receiving the files on his office email, he then sent them to his personal email address, and allegedly within hours someone hacked his work email and deleted the files.

In a separate incident, police information in the files of more than 400 people was allegedly sent to a woman in Victoria who had complained to the Office of Police Integrity (OPI) about privacy breaches.

In a recent interview with a local radio station, the State Premier Steve Bracks resisted calls for an independent investigation into the leaking of sensitive information from police files, but did say he was "sick and tired" of these breaches.

Later Mr Bracks said a Commissioner for Law Enforcement Data Security would be appointed to head a new independent agency and will have the final say over who can access the files - including police, government agencies and individuals.

About A$50 million will be spent over the next three years to replace the LEAP database.

In West Australia, the Local Government Association recently was reported as saying that local councils needed more resources to combat the misuse of personal information. This comes after a Corruption and Crime Commission investigation into government agencies, and two local councils, highlighted a misuse of medical, criminal and financial data. The study also found the checks and balances that could detect inappropriate access are inadequate.

There are also a number of cross-currents in the debate over the privacy of health information in Australia. The health privacy debate is driven by the increased collection of health information into a very diverse and often poorly connected set of electronic health records and the desire to integrate these collections both to improve treatment and facilitate health research. Australia is blessed with a mixed public sector / private sector provided health system,

overlaid by Federal-State government rivalries and this complexity has made progress difficult. At the national level, efforts have centred round an ambitious HealthConnect program (www.healthconnect.gov.au) which was originally intended to create a system of standardised health records in a well connected infrastructure. However this approach has changed in recent months to a stronger focus on setting standards through a National eHealth Transition Authority instead of direct provision of infrastructure.

The key to these changes, though, is a way of uniquely identifying health consumers and protecting their health records in a way that goes beyond mere promises. As might be expected, the debate over health identifiers has been a major stumbling block with claims of inadequate legal, technological and governance protections. Recently, however, there have been encouraging signs that a way forward can be found based on a clear recognition that electronic health records are created primarily for direct treatment of the individual involved with all other possible uses subsidiary to this objective and undertaken in a way that does not undermine that person's trust that the record will stay private.

Stumbling blocks remain and the road ahead will continue to involve wrong turns. According to one report, for example, health consumers in New South Wales will be given no choice about the Government collecting their "confidential" health information. The only choice they will have is about who else will get access, and then only on an "opt out" basis.

In another example, Western Australia has one of the world's most comprehensive cradle to grave, integrated collection of health records. This system has been used to produce remarkable research results, ranging from significantly reducing the incidence of spinal defects through proving the need for higher intake of foliate during pregnancy to analysing deep vein thrombosis. However, the debate is still unresolved about the robustness of the governance and technological protections of this very potent collection of personal information, which places this kind of research at risk should something go wrong and the community, through its elected representatives, acts capriciously in response.

Western Australia has one of the world's most comprehensive cradle to grave, integrated collection of health records

Australia's privacy law does allow the collection and use of health information for research purposes without consent if it is impracticable to obtain the consent of the people involved and the research cannot be undertaken with de-identified health information. Such research has to be approved by Health Research Ethics Committees, but this is a process strongly dependent on volunteer effort from community leaders. The world renowned joint review of genetics and privacy by the Australian Law Reform Commission and the Australian Health Ethics Committee, released in 2003 and titled Essentially Yours, recognised this and called for more resources for the work of these committees.

Indeed, Colin Thomson, consultant in health ethics at the National Health and Medical Research Council, was quoted recently in the media as saying that the laws must be streamlined to cut through a "jumble of jurisdictions". He pointed to a "spectacular" example in which scientists conducting a study of trauma treatment in Victoria spent 18 months gaining approval to access data from 140 sources.

At the highest level, therefore, the recent review by the Privacy Commissioner of Australia of the operations of the Federal Privacy Act that cover the private sector is particularly important. The fundamental conclusions of the report were that the private sector provisions were working well although the Australian Government "should consider undertaking a wider review of privacy laws in Australia to ensure that in the 21st century the legislation best serves the needs of Australia". The report with its 85 recommendations is online at www.privacy.gov.au/act/review/index.html and is well worth reading.

One topic that the report did not cover, and which really only became an issue in Australia while the report was being finalised, is the mandatory reporting of security breaches of personal information. Australian privacy laws do not require mandatory reporting of such breaches and the Australian Privacy Commissioner said the concept of mandatory reporting was not raised during the review. The Attorney-General of Australia, Philip Ruddock, has stated that the existing Privacy Act, which carries no criminal sanctions, is strong enough to compel companies to keep their data safe from theft and misuse. He has however warned companies operating in Australia to take the Privacy Act and its penalties seriously.

Kevin Shaw Leader
Security Services Group, Deloitte
Malcolm Crompton Managing Director
Information Integrity Solutions Pty Ltd
kevshaw@deloitte.com.au
mcrompton@iispartners.com