



ATTORNEY-GENERAL
THE HON DARYL WILLIAMS AM QC MP

Keynote Address

25th International Conference of Data Protection and Privacy

Commissioners

Tumbalong Auditorium

Sydney Convention and Exhibition Centre, Darling Harbour, Sydney

9 am, Friday, 12 September 2003

Introduction

1. We live in a world that is constantly changing.
And these changes pose new challenges for privacy protection.
2. Although the basic principles and objectives of privacy regulation will remain, in this new environment we must update and refine these principles to take into account the rapid development of technology and of world events.
3. Around the world, people share an appreciation of the value of privacy.
We expect Government and business to treat our personal details and information confidentially.
We expect this information only to be used for the purpose it was provided.
And we expect that our basic right to privacy and our personal liberties will not be compromised by the advent of new technologies.
4. For governments and regulators, the task is to respond to these changes with policies that are practical and flexible while retaining and protecting

basic rights.

The focus of this Conference on practical privacy for people, government and business highlights the benefit to both regulators and consumers of having systems in place which can adapt to changes not only in technology, but also to advances in science and research and to changes in the global environment.

5. This was the philosophy that underpinned the OECD's landmark Privacy Principles of 1980, upon which Australia framed our own privacy principles.

Australia's International Efforts on Privacy

6. Australia has always strongly supported the OECD Privacy Principles and we continue to value the privacy work carried out by the OECD.

The Australian Government remains closely involved in the OECD's work on data protection and information security.

And we play a leading role in the development of the OECD Guidelines for the Security of Information Systems and Networks released in July 2002.

7. The Guidelines deal with problems arising from the growth of globally networked information systems, particularly the Internet.

They are relevant to operators and users of communication networks, critical information infrastructure and anyone with access to information systems, from software designers to home users.

The APEC Initiative

8. We are now in the process of building on the work undertaken by the OECD in the context of Asia-Pacific Economic Cooperation.

Many of you here today will be aware that the Electronic Commerce Steering Group of APEC has, at Australia's suggestion, established a

working group to approach privacy from an APEC perspective.

The working group is chaired by a senior officer in the Attorney-General's Department.

Using the OECD privacy guidelines as a starting point, it will develop a set of APEC privacy principles and implementation mechanisms.

9. The motivation for this initiative was our appreciation of the need for an international standard on privacy.

This is particularly the case in relation to the cross-border transfer of personal information.

10. It was also informed by our assessment that the European Union's privacy protection model is not suitable as the basis for such an international standard.

It is prescriptive, it gives significant powers to a bureaucracy and it does not allow for innovative developments.

11. Australia is continuing our discussions with the European Commission on an adequacy rating for Australia's privacy laws.

And we are preparing amendments which go some way towards meeting their concerns.

However, this is not the main focus of our international work on privacy.

12. APEC brings together the diverse viewpoints and interests of North American, Pacific and Asian economies.

We think it is a very suitable forum to develop standards that recognise the differing approaches of our economies.

13. The diversity of the APEC economies potentially presents the greatest challenge to developing an agreed, single approach to privacy protection.

However, that very diversity suggests that the approach may have significance well beyond the Asia-Pacific region.

14. A consensus drawn from the member economies of APEC will represent a significant achievement and will inform the rest of the world of what is possible.

It will set the standard.

15. Consensus and consultation are at the heart of APEC processes and I am happy to say that the privacy working group is proceeding on that path. Tomorrow's privacy workshop provides an opportunity to contribute to the working group's thinking.

And I encourage you all to attend and to share your thoughts.

Residential tenancy databases

16. The Australian Government has also been working closely with State and Territory Governments to resolve privacy concerns at the domestic level. One issue which has recently generated widespread concern is the use of tenancy databases, which provide information on prospective tenants on a fee-for-service basis to real estate agents and lessors.
17. From both a fair trading perspective and from a privacy perspective, there have been calls for a review of the practices of tenancy database operators. The information in these databases can have an adverse effect on prospective tenants.
- And there have been criticisms that information contained in the databases can be outdated, incorrect, improperly entered or improperly disclosed. There have also been concerns about the validity of the consent obtained from prospective tenants for listing and disclosure.
18. The Privacy Act establishes privacy standards for personal information in the possession of private sector organisations.
- In addition, the National Privacy Principles give individuals the right to access and correct any personal information about them held in a tenancy

database.

The Privacy Commissioner is also able to advise database operators about meeting their obligations under the Privacy Act and to assist people in ensuring that their rights are respected in relation to tenancy databases.

19. The Ministerial Council on Consumer Affairs has established a working group to look at concerns relating to tenancy databases.

In order to ensure that a holistic approach is taken to resolving these concerns, I proposed at the recent Standing Committee of Attorneys-General that SCAG Officers participate in the working group.

20. State and Territory Attorneys-General agreed to my proposal.

The working group is being chaired by Treasury and includes representatives from the States and Territories, the Attorney-General's Department, the Office of the Federal Privacy Commissioner and the Australian Competition and Consumer Commission.

It is expected to report to SCAG and the MCCA in the first half of 2004.

Unauthorised Photographs

21. Another issue that has recently been raised at the Standing Committee of Attorneys-General is the unauthorised publication of photographs on the Internet, including indecent websites.

There have been reports of photographs being taken of children engaging in normal school activities without their consent or knowledge and then being placed on websites of a sexual nature.

There have also been reports of mobile phones with cameras being used in swimming pool change rooms.

22. Under the Online Content Regulatory Scheme, the Australian Broadcasting Authority can order Australian Internet content hosts not to host prohibited

content in Australia.

This scheme enables the context in which a photograph appears to be considered in determining whether it is prohibited content.

23. The Australian Government is developing offences targeting those who make child pornography available, or intentionally access it, using the Internet.

And these new offences will carry penalties of up to 10 years imprisonment.

24. Australia's Privacy Act also allows for the creation of sector-specific privacy codes, to be approved by the Privacy Commissioner, that provide at least the same level of protection as the Act.

And we are working with the Internet Industry Association to develop an Internet industry privacy code of practice to deal with this issue.

25. The borderless world of the Internet poses significant problems for effective regulation.

However, we have a responsibility to do what we can.

26. To develop a national approach, the Standing Committee of Attorneys-General has agreed to establish a working party to examine the issue of unauthorised photographs.

The working party will report back to SCAG Ministers on their findings.

Information security

27. Aside from issues created by the Internet, computer information systems contain vast amounts of personal and financial information.

We must be vigilant about any compromise or violation of this information.

Corporations and governments also need to ensure that information is only available to those people who need, and are authorised, to access it.

28. The Australian Government is acutely conscious of the need for security in the information technology field.

Our computer systems manage this information and form the so-called 'critical information infrastructure' which underpins virtually every aspect of economic activity.

This ever-increasing reliance on computer systems has also created a new vulnerability which, if exploited, could have significant consequences.

29. Any attack on the critical information infrastructure, be it by viruses, hackers, denial of service attacks, information warfare hackers or cyber-terrorists, has the potential to cause immense economic disruption and to compromise the privacy of millions of people.

30. Like governments around the world, the Australian Government is determined to protect our critical infrastructure from attack.

We want our economy to continue to grow and we want to ensure the information held in computers is not improperly accessed or used.

31. The difficulty we face is that no single level of government and no single organisation has total responsibility for our critical infrastructure.

Ownership is spread across the economy.

This means that any effective protection strategy must involve all stakeholders from across business and government.

32. The Government recognises that the effective cooperation of all participants involves the sharing of data which may be commercially sensitive.

The privacy implications of this information-sharing is one of the

significant issues we have had to deal with in securing participation in this crucial information sharing.

33. To facilitate a holistic and strategic response, the Government has established the E-Security Coordination Group.
The group consists of representatives from key government agencies. In addition to its focus on security standards, the group also works on incident reporting, awareness-raising and skills shortages.
34. Based on the findings of the Business-Government Task Force on Critical Infrastructure, the Government has also established the Trusted Information Sharing Network for Critical Infrastructure.
The goal of this network is to facilitate the sharing of information between owners and operators of critical infrastructure on generic threats and vulnerabilities.
It will also provide advice on measures to mitigate risk.
35. As the network is focused at the systems level, there will be no need for its members to share the private information of their clients.
The structure of the TISN is being developed in consultation with regulators, including the Australian Competition and Consumer Commission, the Australian Securities and Investment Commission and the Australian Stock Exchange to ensure that legislative issues regarding information sharing are addressed.

Genetic Privacy

36. Of course not all technology applies to computer systems.
Privacy considerations extend beyond information management and security.

37. Advances in medical technologies have brought concerns about the privacy and sanctity of genetic information into the spotlight.

38. To look into the protection of genetic information and samples, the Australian Government established a joint inquiry by the Australian Law Reform Commission and the Australian Health Ethics Committee.

The terms of reference for the inquiry required these bodies to examine what regulation may be needed to protect the privacy of human genetic samples and information.

In addition to looking at the strict regulatory position, the inquiry also took into account the ethical considerations involved in the collection and uses of human genetic samples and information.

39. The joint inquiry reported in May 2003, making 144 recommendations in total.

The number of recommendations, published in two large volumes, reflects the complex nature of genetic privacy.

40. Among other things, the report recommended that the concept of personal information and records in the Privacy Act be extended to include bodily samples.

It was recommended that individuals be given right of access to their own samples and to those of their first degree genetic relatives.

Another key recommendation was that 'health information' under the Privacy Act should include information about an individual who has been dead for 30 years or less.

At present the Act applies only to the living, with next of kin given decision-making powers.

The Government is in the process of developing its response to the report, which is available on the Australian Law Reform Commission's website.

I encourage anyone with an interest in the subject to have a look at it.

Response to Terrorism and Privacy

41. The Australian Government believes that the right to privacy is fundamental to all Australians and must be protected.
However, the Government also recognises that privacy interests must be balanced with the needs of law enforcement and security agencies in investigating serious criminal activity and potential threats to security. This is even more the case in light of the events of September 2001 and October 2002.
42. Protecting Australians from the threat of terrorism has involved making some hard decisions about where the balance should lie.
43. For example, our principal security and intelligence agencies are explicitly exempted from the operation of the Privacy Act.

However, the Government has been careful to ensure that measures put in place to protect our community from the threat of terrorism do not unduly encroach upon the individual rights and liberties that are fundamental to our democratic system.

The ASIO Act, for example, contains extensive safeguards to ensure that ASIO's powers are properly exercised and that the right balance is maintained.

These include a rigorous process for seeking and issuing questioning and detention warrants, access to legal representation, external scrutiny processes, a special regime for people between 16 and 18 years of age, and offences for failing to comply with safeguards.

44. The Government has gone to great lengths to listen to and respond to concerns raised about its national security policies, including privacy concerns.

The robust way in which the Government's anti-terrorism policies have been played out in the public and parliamentary arena is testament to the strength of our democratic processes.

It also reflects the Government's determination that these measures are necessary and thus worthy of significant debate and effort to ensure their effective implementation.

Conclusion

45. This conference provides data protection and privacy commissioners with a valuable opportunity to share their experiences of privacy regulation and to discuss trends in the information and global sectors.

The topics covered at this conference highlight your awareness of the need to ensure that privacy regulation adapts to the constantly changing environment.

The topics also highlight the importance of the principles of openness and transparency in privacy regulation.

46. It is vital that we have a lasting and comprehensive privacy protection regime that can be widely applied and can readily adapt to change.

The basic privacy principles help us to ensure that privacy is respected, protected and observed in all situations.

I wish you well with this final day of your conference.