



The Attorney-General

Philip Ruddock MP

Search

Hot Topics

Biography

Media Centre Info

FAQs

Photo Gallery

Portfolio Links

Contact the AG

The Department

The Prime Minister

Opening Keynote Address to
Australian Smart Cards Summit 2005
Sydney Convention and Exhibition Centre
9.00 am, Wednesday, 29 June 2005

[Acknowledgements]

- Firstly, may I acknowledge the traditional owners of the land we meet on – the Gadigal people of the Eora nation – and pay my respect to their elders, both past and present.

[Other Acknowledgements]

- Distinguished guests, ladies and gentlemen
Page 2 of 16
Attorney-General Philip Ruddock - Australian Smart Cards Summit - 29 June 2005

[Introduction]

1. Good morning.
2. I am pleased to open the Australian Smart Cards Summit for 2005.
3. I see from the program that you have two very full and interesting days ahead of you.
The wide range of issues to be covered illustrates how this technology can touch many areas of our lives.
4. Individuals, businesses and governments are adversely affected by many types of fraud — such as counterfeit credit cards, skimming, false identities and phishing scams.
5. Although the problems can be complex, everyone affected wants a simple and cost effective solution.
6. Smart card technology has a crucial role to play in providing these solutions.
7. This can take the form of improving the security of personal credit cards through chip technology, or making personal identification documents harder to counterfeit.
8. Australia, of course, is not alone in facing these issues.
9. The recent events in the United States show how vulnerable we can be to this type of fraud.
10. During the Summit you will hear from a range of overseas and Australian experts and I encourage everyone to make the most of this opportunity to learn about these issues.

[Border protection]

11. Those of you who have travelled here from other countries, will have just experienced first hand the need to prove your identity.

You will have needed your passport to collect your ticket, to obtain your visa and to pass through customs and immigration.

12. Since September 11 2001, border protection has become more important than ever to nations around the globe.

13. Strong and reliable proof of identity is a key factor in our border security program.

It is essential that we know travellers are entering Australia for legitimate reasons.

14. And in issuing passports we need to know that applicants are genuine.

15. From October, Australia will start using ePassports.

These will incorporate a contactless chip containing biometric information.

This will greatly reduce the risk of passport counterfeiting and misuse.

16. We will also start to use facial recognition technology when issuing passports and in operating Australia's fraud detection systems.

17. Mr Bob Nash from the Department of Foreign Affairs will be speaking on this later this morning.

[National Security]

18. I don't have to tell you why we are so concerned with border security.

We can no longer rely on Australia's geographical isolation, which has provided such good protection in the past.

Al-Qaeda and its cohorts are targeting all advanced western economies, including our own.

19. The threat to Australia is all too real.

20. We know that terrorists use false or stolen identities to help them carry out their plans.

In fact, the 19 terrorists involved in September 11 used over 350 false names in planning and executing their attacks.



We also know the Bali bombers used false identification documents to operate bank accounts, to transport bomb-making materials and to avoid detection.

And we know that false or stolen identities play an ever-increasing part in financing terrorism.

[Law enforcement]

21. But it's not only terrorists who use false identities. Criminals have shown they are quick to use modern technology to counterfeit identity documents.

Forged driving licences, birth certificates, passports, and immigration documents can be used to obtain pensions or other government benefits.

Fake credit cards can be used to buy goods and get

cash advances.

These crimes leave credit providers, merchants, and the people whose identities have been stolen to bear the cost.

22. This type of crime is not, of course, limited to Australia.

It is a world-wide problem.

23. The good news is that our law enforcement agencies have achieved significant results.

24. Just over a year ago they smashed a major credit card counterfeiting ring.

25. Last month they took part in a world-wide sweep that closed down almost 1400 phishing sites — with 13 of these based in Australia.

26. In March this year our law enforcement agencies made arrests and seized equipment and documents being used to produce bogus passports, credit cards and government cheques.

27. These sorts of documents are used by people smugglers and the criminals involved in illegal immigration and money laundering.

They are also used to defraud government agencies.

[Cost to industry]

28. Identity fraud poses a serious threat to the business community, especially in the growing field of electronic commerce.

The Australian Bankers' Association estimates the cost to the banking industry at \$25 million a year. And two years ago Austrac estimated the annual cost of identity crime in Australia at \$1.1 billion. Globally, we are looking at a figure as high as \$2 trillion.

[Government services]

29. Government agencies are another target for identity fraud.

30. It is vital to Australia's security and economic interests that the identities of people can be accurately verified when they seek access to government services, benefits, official documents and positions of trust.

[Effect on individuals]

31. Of course, it's not only businesses and governments that suffer from identity fraud.

The cost to a person who has their identity stolen is huge — in both monetary and emotional terms.

32. Once a victim realises their identity has been stolen — and this can sometimes take months — they have to convince organisations such as their bank, the Road Transport Authority and the Tax Office.

They have to re-establish their credit rating.

They have to contact every retailer where their credit card has been misused and convince them they have been the victim of fraud.

They may even have to prove that they do not

have a criminal record.

It can take years, and cost thousands of dollars, for someone to restore their reputation.

[Cyber-crime]

33. While technology has revolutionised the way we do business, it has also spawned cyber-crime.

34. AusCERT - Australia's Computer Emergency Response Team - has just released the 2005 Computer Crime and Security Survey.

This reports a serious rise in the number of cyberattacks, and that these have been orchestrated by criminals motivated by illicit financial gain.

The analysis reveals that online identity theft to facilitate fraud is the most common type of internet-based crime.

And it states that identity fraud is rapidly worsening - spreading across multiple business sectors.

In fact in the year to April 2005 AusCERT reported a 1,200 per cent increase in incidents of identity fraud.

35. The survey also points out that although most identity theft came from 'phishing' sites, there has been an increase in the number of ID theft trojans, which now account for 20 per cent of reported incidents.

[National ID Security Strategy]

36. The Australian Government is determined to make it as difficult as possible for people to use false identities.

37. Our approach will result in a strong, comprehensive, and consistent identity security framework.

38. There are two key components to identity security.

- establishing the validity of documents presented as proof of identity,
- and establishing that the person presenting the documents is the person to whom the documents were issued.

39. This is why we have developed the National Identity Security Strategy.

[Scope of the National Identity Security Strategy]

40. When the Strategy is implemented all relevant government agencies will be able to use a common range of documents to identify clients who register for services with them.

41. We are developing standards for these documents, including the appropriate use of biometric identifiers to make them harder to counterfeit.

42. Government agencies will have a secure electronic system to check the veracity of documents presented to them.

Secure post-registration authentication practices will be adopted.

And, if necessary, appropriate legislation will support the processes used.

[Need for Cooperative Approach]

43. The Strategy is based on a whole-of-government approach, to maximise its effectiveness and useability across government operations.

44. We are also working in partnership with the state and territory governments who are responsible for issuing primary identification documents, such as birth certificates, fact of death data and drivers' licences.

45. This has included extensive consultations in the development of the National Identity Security Strategy, and I appreciate the strong support and cooperation we have received.

46. The private sector also has a vital part to play and we will be consulting them as the project develops.

[Pilot Projects]

47. In the Budget last month the Government allocated \$5.9 million to fund two key pilot projects.

48. One project involves a prototype for the Department of Foreign Affairs and Trade and the Department of Immigration so they can verify online the documents people present to establish identity.

Privacy protection is being built in to the pilot, so for example, Austroads will not know that a check about a driver's licence is being made by Foreign Affairs.

I can also assure you that no personal details or identifying numbers will be retained in the system.

49. On this issue, Garry Compton from the Department of Finance and Administration will be talking this afternoon about the Australian Government e-Authentication Framework for Business.

50. The other pilot project will check 25,000 tax records against information held by other agencies.

This will identify key data matching elements that can be used to improve the accuracy of personal information held on government databases.

And it will help to identify false identities and inaccurate records.

[Privacy]

51. Protecting people's privacy in undertaking these activities is an essential requirement.

52. The federal Privacy Commissioner has been actively involved in developing the National Identity Security Strategy, and will continue to be involved throughout its implementation.

State and territory privacy officials have also been consulted.

53. And I can assure you that all the agencies involved

are taking great pains to make sure they work within the principles set out under Australia's Privacy Act.

54. In fact, I believe that the work being done under the identity security initiative will end up enhancing privacy, by making sure that only essential information is kept on record, and by removing inaccuracies and inconsistencies from existing records.

["Australia Card"]

55. There have been recent suggestions in the media that the Government is going to introduce a national identity card.

56. I can assure you that this is not the case.

57. We do not support the approach where all personal information is centralised on one database, and a single form of identification is issued.

58. This could increase the risk of fraud because only one document would need to be counterfeited to establish identity.

59. Instead, we support the use of a range of acceptable documents, with the ability to verify those documents quickly and simply.

60. This approach strengthens our proof of identity process and mitigates the risk of identity fraud.

[Conclusion]

61. This Summit is an opportunity to share information and learn about the fast-developing field of smart card technology.

62. As you do so, I would ask you to remember that:

- Strong identity security benefits us all,
- It protects us as individuals,
- It protects a business's transactions,
- It protects governments from fraud,
- And it helps us as a nation in our fight against terrorism.

63. It's my pleasure to formally open the Australian Smart Cards Summit for 2005, and I wish you well in your deliberations over the next two days.

[Copyright](#)
[Disclaimer](#)