– Meeting privacy challenges –
The ALRC & NSWLRC Privacy Reviews
2 October 2008 (UNSW)

Panel 1:
The ALRC proposals and
consumer trust in electronic commerce

Chris Connolly (Galexia)
www.galexia.com

galexia

Overview

- **Protecting Privacy in Internet E-Commerce** – Key issues
- **Privacy Solutions** – Things that work
- **Privacy Solutions** – Things that don't work
- **ALRC Report:**
  - Definition of personal information [Rec 6-1]
  - Anonymity and pseudonymity [UPP 1]
  - Privacy policies [UPP 4]
  - Trustmarks [31.70]
  - Direct marketing [UPP 6]
  - Data breach notifications [Rec 51-1]
  - Non-commercial activity [11.21]
  - Unsolicited personal information [Rec 20-1]

galexia

Key issues – Behavioural tracking

- **UK ICO investigation** – Phorm / BT compliance with privacy legislation
  - » "Phorm will only be legal in the UK if it is an opt-in service"
- **US Senate Commerce Committee**
  - » Self-regulatory model has been offered by major ISPs
  - » Microsoft IE8 (Beta 2) offers *InPrivate Blocking*
  - » NebuAd strengthens privacy controls:
    - – "NebuAd meets both the letter and spirit of all relevant privacy requirements"
  - » But NebuAd is still opt-out

galexia

Key issues – User generated content

- **Generated by subject**
  - » Consumers supply the information to the public themselves (e.g. MySpace)
  - » Later used for other purposes (e.g. media, employment)
- **Generated by third party**
  - » Another individual collects, collates or observes information on the individual
  - » Shared with the public:
    - – Nuremberg files
    - – Human flesh search engines

galexia

Key Issues – False perceptions

- **False perceptions:** Private browsing:
  - » Google chrome – Incognito
    - – "Going incognito doesn't affect the behavior of other people, servers, or software. Be wary of… surveillance by secret agents and people standing behind you"

  - » Firefox Private browsing
    - – "It is very important that the user understands that this feature enables local privacy on their machine, but that their ISP, corporation, or government will still be able to monitor their activities online. We don't want to have whistle blowers fired or dissidents jailed on account of bad UI. We may also want to consider not shipping this feature in certain regions where misunderstandings over the scope of this feature could have serious ramifications for the user."

galexia

Privacy Protection – Things that work

- **Legislation**
  - » Comprehensive (no gaps)
  - » Uniform (eases cross-border concerns)
  - » Active Privacy Commissioners
    - – SWIFT (Belgium)
    - – Google Streetview (Canada)
- **Enforcement and sanctions**
  - – Japan (Credit Suisse)
  - – Taiwan (Citibank)
  - – See: Privacy breach sanctions in the Asia-Pacific region (July 2007)
- **Anonymiser services**
  - » Some protection at the ISP or intermediary level (not at the browser)
  - » Really pseudonymity as subject to conditions (e.g. http://ctunnel.com/ used in Palin email hack)
- **Classification services**
  - » But notable inconsistency – eg classification / non-classification of Phorm as spyware

galexia

Privacy Protection – Things that don't work

- **Guidelines, Fair information principles, Frameworks**
  - Raise expectations of privacy protection where no protection exists
- **Trustmark schemes**
  - Major issues in practice re standards, enforcement and consumer understanding
  - Major structural issues (that cannot be resolved) re transience, timing issues, independence and scams
  - See: Trustmark Schemes Struggle to Protect Privacy (2008)
- **Registration requirements**
  - Very low cost to benefit ratio
  - e.g. Australian PIDs, some EU laws, EU BCRs, proposed APEC CBPRs
- **Abstinence**
  - Fails where information is observed (e.g. Streetview) or collected from public registers

galexia

ALRC: Definition of personal information [Rec 6-1]

- **ALRC DP 72:**
  - » IP address could be, or could become, personal information once that information was linked to a particular individual due to the accretion of information around the number or address.
- **Final report:**
  - » Recommendation 6–1
    - The Privacy Act should define 'personal information' as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.
  - » Recommendation 6–2 [Guideline only]
    - The Office of the Privacy Commissioner should develop and publish guidance on the meaning of 'identified or reasonably identifiable'.
- **Conclusion:**
  - » IP address included, subject to circumstances and conditions in PC guidelines

galexia

ALRC: Anonymity and pseudonymity [UPP 1]

- **UPP 1. Anonymity and Pseudonymity**
  - » Wherever it is lawful and practicable in the circumstances, agencies and organisations must give individuals the clear option of interacting by either:
    - – (a) not identifying themselves; or
    - – (b) identifying themselves with a pseudonym.
- Difficult to say this is an improvement – may lead to abandonment of anonymity (e.g. default will always be pseudonymity 'just in case')
- However, possibly a good reflection of the reality in e-commerce

galexia

ALRC: Privacy policies [UPP 4]

- **UPP 4. Openness:**
  - » An agency or organisation must create a Privacy Policy that sets out clearly its expressed policies on the management of personal information, including…
- Subtle change from current Act in that IPPs and NPPs could be met by a variety of means, not necessarily a "Privacy Policy" – improves certainty
- **See also Recommendation 24–3:**
  - » The OPC should continue to encourage and assist agencies and organisations to make available short form privacy notices…

galexia

ALRC: Trustmarks [31.70]

- **Rejects trustmarks at this time**
  - » The use of trustmarks as a method of promoting compliance with, and enforcement of, the Privacy Act and other international privacy regimes should be explored. It is premature, however, to introduce the concept of trustmarks into the Privacy Act. The concept needs to be developed further before it would be appropriate for introduction as a mechanism under the Privacy Act. [31.70]

galexia

ALRC: Direct marketing [UPP 6]

- **UPP 6. Direct Marketing**
  - » 6.1 Improved test for existing customers:
    - – Individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing
  - » 6.2 Weak test for other consumers likely to be applied online:
    - – (ii) information is not sensitive information and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure; [followed by usual opt-out provisions]
- Missed opportunity for opt-in at time when the public has turned against behavioural tracking and direct marketing
- Also, very weak test for providing key information:
  - » (d) if requested by the individual, the organisation must, where reasonable and practicable, advise the individual of the source from which it acquired the individual's personal information.
- See also: Proposed Guideline on interaction of Privacy Act, Telco Act, Spam Act and Do Not Call Register [Rec 73-10]

galexia

ALRC: Data breach notifications [Rec 51-1]

- **Recommendation 51-1:** The Privacy Act should be amended to include a new Part on data breach notification…
  - (a) An agency or organisation is required to notify the Privacy Commissioner and affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.
  - (b) The definition of 'specified personal information' should include both personal information and sensitive personal information, such as information that combines a person's name and address with a unique identifier, such as a Medicare or account number….
- Popular and timely recommendation – more balanced than many other jurisdictions.
- Could be strengthened by a presumption that information made available on the WWW is automatically "reasonably believed to have been acquired by an unauthorised person".

galexia

ALRC: Non-commercial activity [11.21]

- **[11.21]** It is not practical or desirable to expand the scope of the Privacy Act to regulate individuals acting in a non-commercial capacity. There are other methods that could deal more appropriately with situations where an individual acting in a personal capacity interferes with another individual's privacy… (e.g. statutory cause of action).
- **[11.22]** The ALRC notes that much of the concern about individuals acting in a non-commercial capacity relates to information posted by individuals on websites. While a take-down notice scheme might help… the ALRC does not recommend the introduction of such a scheme.
- Difficult to see any alternative solutions – likely to be one of the most important issues in coming years
- See also: Guideline on social networking [Rec 67-3]

galexia

ALRC: Unsolicited personal information [Rec 21-3]

- **Recommendation 21–3:**
  - The 'Collection' principle should provide that, where an agency or organisation receives unsolicited personal information, it must either:
    - (a) if lawful and reasonable to do so, destroy the information as soon as practicable without using or disclosing it except for the purpose of determining whether the information should be retained; or
    - (b) comply with all relevant provisions in the model Unified Privacy Principles that apply to the information in question, as if the agency or organisation had taken active steps to collect the information.

- Useful improvement for user generated content and 'observed' information