

Privacy and Health: Getting the Balance Right



**Presentation to Health
Privacy Futures
Conference 2008**

by

**Prof Les McCrimmon
Commissioner, ALRC**



Australian Government
Australian Law Reform Commission

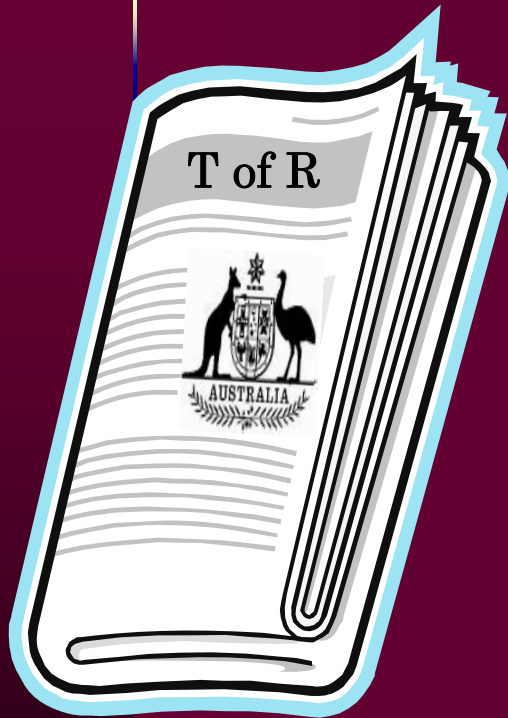
Focus of Presentation



- Overview - ALRC Privacy Inquiry
- Overview - *For Your Information: Australian Privacy Law and Practice* (ALRC 108, 2008)
- Key recommendations



Terms of Reference



- ALRC asked to look at effectiveness of privacy protection given:
 - rapid technological advances (information, communication, storage, surveillance, etc)
 - emerging areas requiring privacy protection
 - possible changing community perceptions
 - expansion of state/territory activity in this area
 - international and regional obligations, trends



Extensive Public Engagement

- Broad-based Advisory Committee
 - plus 3 specialist sub-committees: health; credit reporting; developing technologies
- Consultation papers
 - 2 Issues Papers; 2 Overview documents; Discussion Paper (3 vols, 301 proposals for reform)
- National Privacy Phone-in
- Special 'Talking Privacy' website for kids
- 250 meetings + public forums (incl health and research), roundtables, youth workshops
- Nearly 600 written submissions



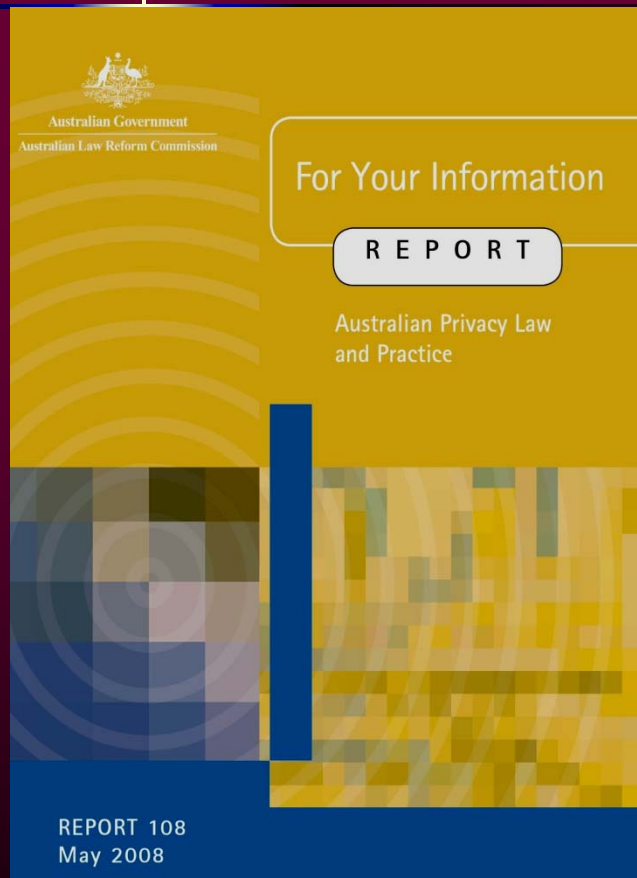
What we heard . . .



- Australians *do* care about privacy
 - perceived erosion of privacy – especially since ICT advances
 - ‘sensitive info’ (esp medical)
 - but understand need to balance privacy with benefits, security
- Privacy laws *much* too complex and confusing
- ‘Privacy’ often just an excuse (‘BOTPA’)
- Need stronger remedies in the event of breaches – esp serious ones



For Your Information: Australian Privacy Law and Practice (ALRC 108)



3 volumes, 74 chapters,
295 recommendations

- ❖ Part A – Introduction
- ❖ Part B - Developing Technology
- ❖ Part C - Interaction, Inconsistency and Fragmentation
- ❖ Part D - The Privacy Principles
- ❖ Part E – Exemptions
- ❖ Part F - Office of the Privacy Commissioner
- ❖ Part G - Credit Reporting Provisions
- ❖ **Part H - Health Services and Research**
- ❖ Part I - Children, Young People and Adults Requiring Assistance
- ❖ Part J – Telecommunications
- ❖ Part K - Protecting a Right to Personal Privacy



Key Recommendations

- One set of privacy principles
- Greater harmonisation
- Fewer exemptions
- Greater enforcement powers for the OPC
- Mandatory data breach notification
- More comprehensive credit reporting
- Cause of action for serious invasions of privacy



New Regulatory Framework

One Set of (High Level) Privacy Principles

- 1 Anonymity and Pseudonymity
- 2 Collection
- 3 Notification
- 4 Openness
- 5 Use and Disclosure
- 6 Direct Marketing (org only)
- 7 Data Quality
- 8 Data Security
- 9 Access and Correction
- 10 Identifiers (org only)
- 11 Cross-border Data Flows

OPC Guidance

Eg:

definitions

data-matching

lawful and
practicable

existing
customer

templates

Regulations

- can impose more specific - and more or
less stringent - requirements

Industry codes


- to deal with operational matters



Achieving National Consistency

- *Privacy Act 1988* (Cth) - apply to Cth public sector and private sector
- State and territory privacy laws - not to apply to private sector organisations
- Major impact on health privacy legislation by excluding state and territory privacy laws applying to organisations
 - eg:
 - *Health Records and Information Privacy Act 2002* (NSW)
 - *Health Records Act 2001* (Vic)
 - *Health Records (Privacy and Access Act) 1997* (ACT)





**State and territory privacy laws
should adopt UPPs, relevant regs (eg
health) and relevant definitions (eg
personal info, sensitive info, record)**

Sensitive Information



- Definition of 'sensitive information' should include:
 - biometric info collected for the purpose of automated biometric verification or identification;
 - Biometric template info



Health Specific Regulation

- *Privacy (Health Information) Regulations* – contain only requirements that are different or more specific than UPPs
- Section 95 & 95A Guidelines to be consolidated
- OPC to publish document consolidating UPPs, health regs and relevant health info guidelines
- While specific legislation should underpin the establishment and use of Shared Electronic Health Record Systems and Unique Health Care Identifiers, the information itself should be regulated by the *Privacy Act*



Health Specific Regulation (cont)

- Compulsory use of intermediaries where a health service provider denies an individual access to health information
- Requirement to notify individuals when a health service is sold, amalgamated or closed down or a health service provider dies
- Requirement to transfer health information to another provider on request



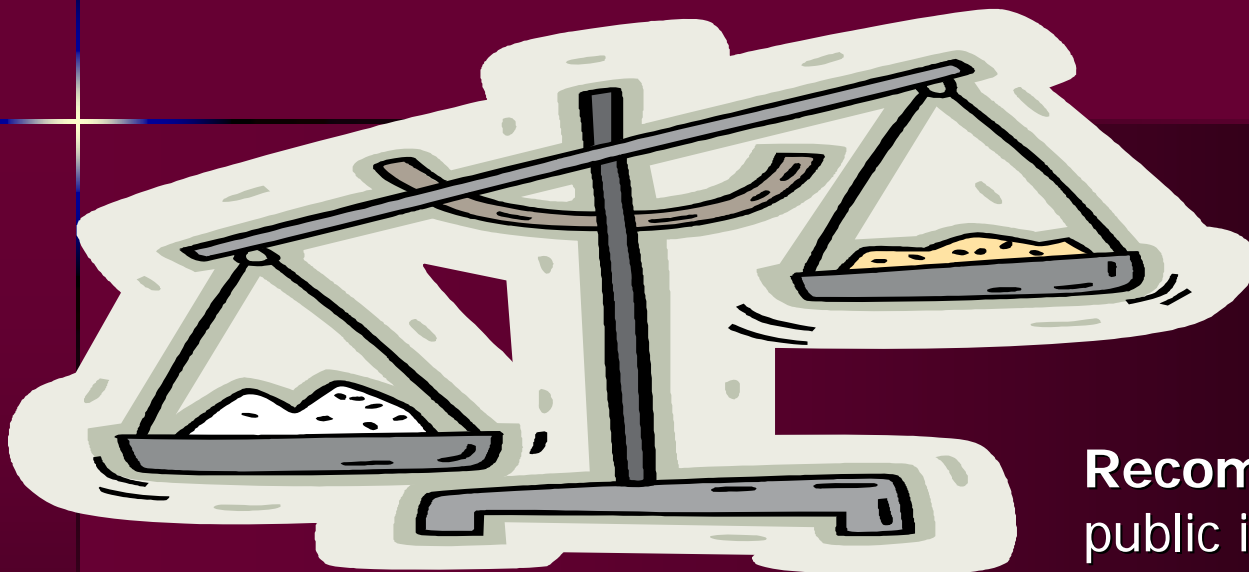
Research



- The *Privacy Act* permits use of personal information without consent for health and medical research if approved by an HREC
- ALRC – *Privacy Act* regime should be extended to research more generally



Public Interest Balance



Current test - the public interest in the research ***outweighs to a substantial degree*** the public interest in maintaining the level of privacy protection provided by the IPPs and NPPs

Recommended test - public interest in the research ***outweighs*** the public interest in maintaining the level of privacy protection provided by the privacy principles



Gov't Consideration of Report

Stage 1 (legislation w/i 12 to 18 mths of 11 Aug 08)

- one set of privacy principles
- credit reporting and health regs
- Education/legislation concerning issues of new technology
- work with states and territories towards harmonisation

Stage 2

- removal of exemptions
- data breach notification
- statutory cause of action

Concurrent

- Powers of OPC
- OPC guidance



Further Information

Web: *For Your Information: Australian Privacy Law and Practice* available at www.alrc.gov.au
Email: info@alrc.gov.au
Post: GPO Box 3708, Sydney, NSW, 2001



Australian Government
Australian Law Reform Commission