



Asian Based. Global Reach.

INFORMATION
INTEGRITY
SOLUTIONS

Malcolm Crompton

Enforcement of the PDPA: Reality Check for Data Abuser – the Australian Perspective

Personal Data Protection Roundtable and
Workshop

Kuala Lumpur

12th – 13th December 2011





Australian Privacy Law – Overview

- Privacy Act 1988 , also state and issue based law (see www.privacy.gov.au)
- Rights for individuals – access, correction, complaints
- Information handling rules for public and private sector – for example National Privacy Principles (NPPs)
- Regulators – for example the Australian Privacy Commissioner in the Office of the Australian Information Commissioner (OAIC)





Privacy Commissioner – role & powers

- Privacy Advice to government, organisations
- Information/education for community, organisation
- Investigate/resolve privacy complaints
- Make formal, enforceable determinations
- Investigate systemic issues
- Audits and inspections
- Reporting



(for example see [Privacy Act – section 27](#))

Enforcement = tools + approach + regulator resources

- Tools:
 - Individual complaints
 - ‘own motion’ investigations
 - Injunctions
 - Audits (public sector only)
 - Public reports or ‘name and shame

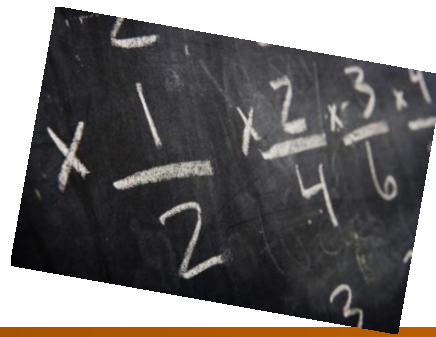


Enforcement Cont.

- Enforcement approaches – influenced by factors such as nature of law, public concern, resources etc
- see for example

Information Sheet (Private Sector) 13 -
2001: The Federal Privacy
Commissioner's Approach to
Promoting Compliance with the
Privacy Act

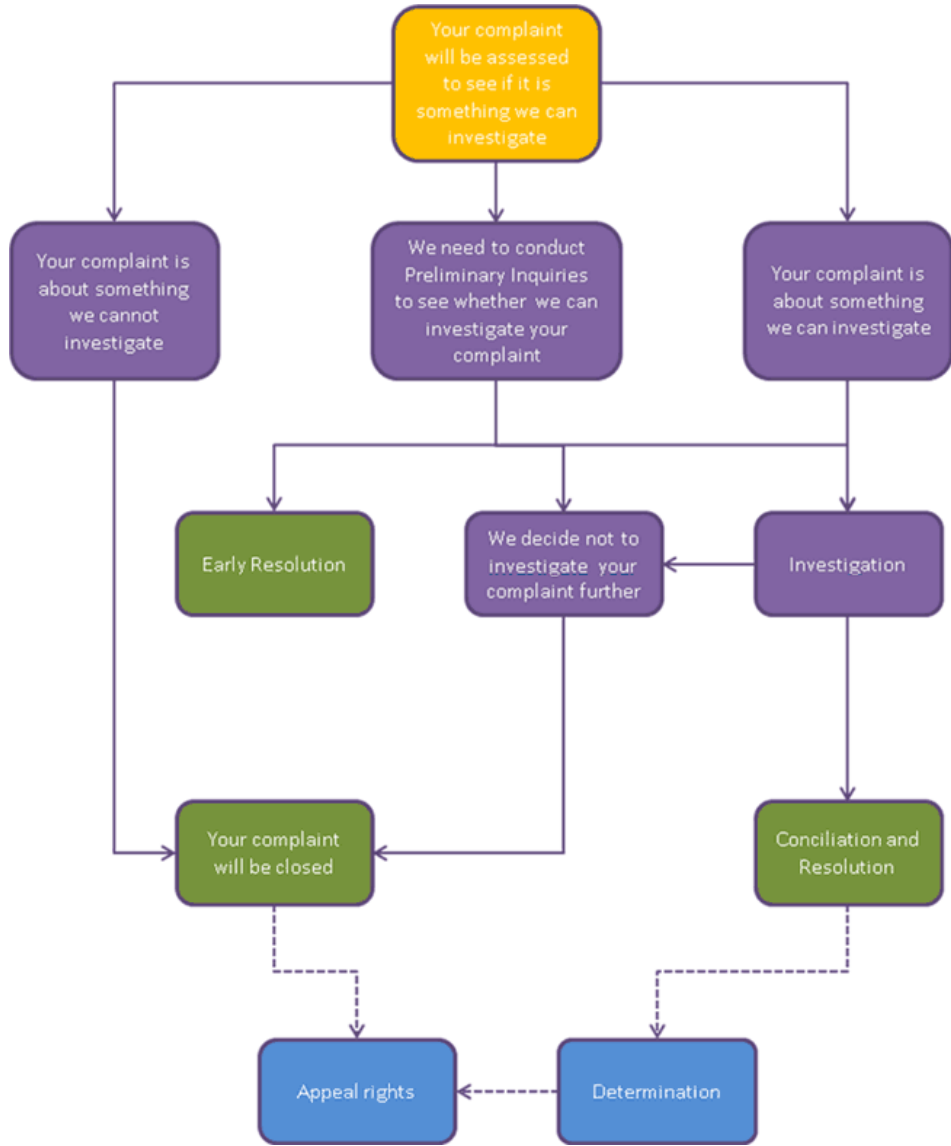




Privacy complaints – OAIC process

- First step – complain to organisation
- No resolution – complain to regulator
- Regulator powers to investigate and resolve complaints subject to matters such as:
 - Jurisdiction
 - Principles and complaint subject matter
 - Steps organisation has taken
 - What the complainant wants

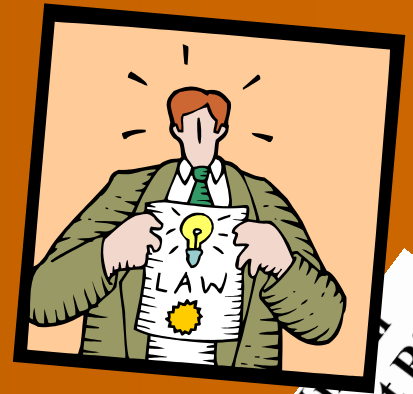
OAIC Privacy Complaint Process





Privacy complaints – outcomes and consequences

- See case notes for examples
- Likelihood of complaint – low
- Consequences of complaint – significant
- Outcome - breach or no breach
- If breach:
 - Conciliated outcome – apology, training, new systems, compensation (\$800 - \$20,000)
 - If no resolution, Privacy Commissioner 'Determination', enforced through courts



**Sony Hacked Again; 25 Million
Entertainment Users' Info at Risk**



INFORMATION
INTEGRITY
SOLUTIONS

Major data breaches – consequences

- Increasing public, political concern
- Increasing consequences
- More likely to play out in the public arena ↑ risk cost, reputation risk
- See for example [Vodafone investigation](#)

First State Super customers have been left in the dark over a serious security breach at the company, saying they only learned through media reports that hundreds of thousands of accounts may have been exposed.





INFORMATION
INTEGRITY
SOLUTIONS

Privacy Act – next generation

- Significant changes in train
 - Review of the law
 - Framework ok but more strength, consistency needed
 - Government – accepts many recommendations:
 - Coming – more powers, more sanctions, data breach notification(?)
 - Regulator – responding to community concerns, tougher action



Resources

- IIS Paper – [Accountability and the Privacy Act](#)
- [Office of the Information Commissioner](#)
- [Privacy Complaints Practice And Procedure Manual](#)
- OAIC [Case Notes](#)
- OAIC – [Determinations](#)





You are not alone

- 76 countries have data protection laws
- OECD Guidelines on the Protection of Privacy & Transborder Flows of Personal Data
- APEC privacy framework & CPEA
- Australian privacy law
- Singapore proposals – Discussion Paper
- Philippines proposed Data Privacy Act 2011



**INFORMATION
INTEGRITY
SOLUTIONS**

Malcolm Crompton

Managing Director

53 Balfour Street

Chippendale NSW 2008

Australia

+61 407 014 450

MCrompton@iispartners.com

www.iispartners.com