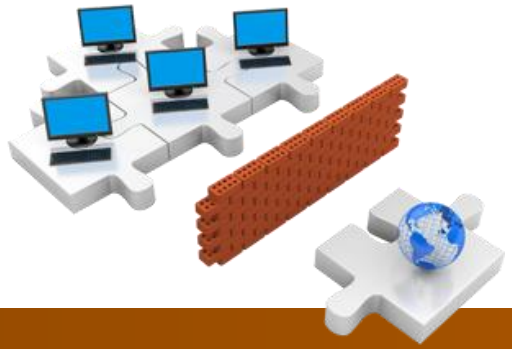
Malcolm Crompton

A Customer-Centric Approach to Privacy and Data Protection

Privacy and Data Protection Singapore 2011 Conference

Singapore

11 November 2011

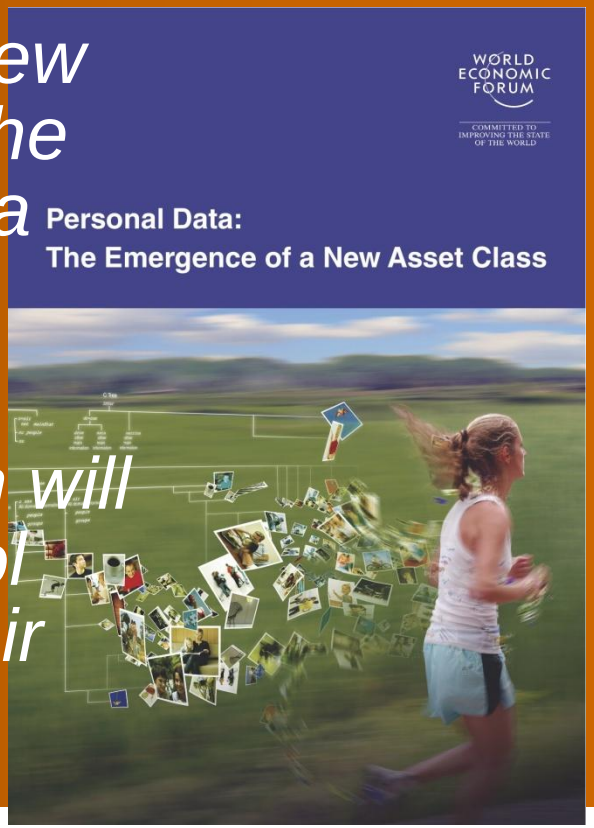


INFORMATION INTEGRITY SOLUTIONS

Getting privacy right – a business building proposition!

"… personal data will be the new "oil" – a valuable resource of the 21st century. It will emerge as a new asset class touching all aspects of society."

"The personal data ecosystem will be built on the trust and control individuals have in sharing their data"



INFORMATION INTEGRITY SOLUTIONS

Data Protection Law is coming to Singapore

- an opportunity for your business and customers?
- or just a compliance burden?

INFORMATION INTEGRITY SOLUTIONS

"Compliance – necessary and sufficient"…?

- World wide, DP principles are **minimum** standards:
  - consent based collection
  - reasonable use & disclosure
  - security & data destruction
  - access & correction rights

- Do these do enough to build consumer trust in data use?

INFORMATION INTEGRITY SOLUTIONS

Privacy – experience shows that

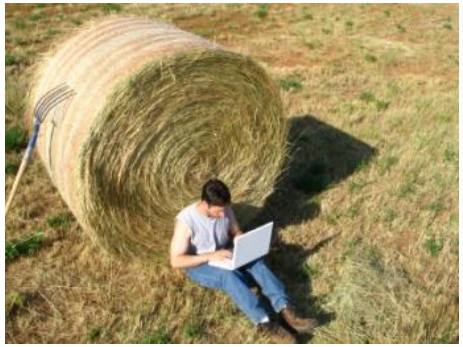
privacy is

- control – deciding what to reveal and when
- creepiness factor – big brother, too much information, too intrusive
- risk – who bears it …

privacy is not

- consumers wanting to keep everything secret
- simply having something to hide
- a blocker to using data
- only about security

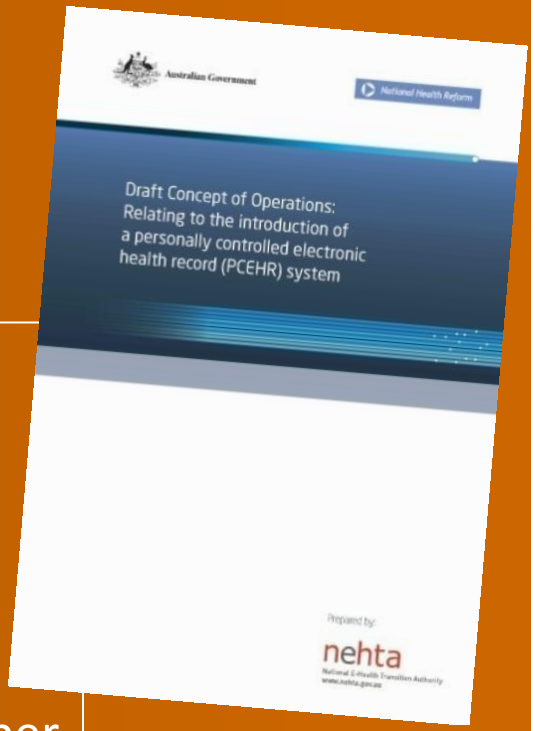
Sony Hacked Again; 25 Million Entertainment Users' Info at Risk



INFORMATION INTEGRITY SOLUTIONS

User-centric privacy – eHealth Australia

- Personally Controlled Electronic Health Record (PCeHR)
  - AU$467million project
  - secure + individual health identifier
  - stored in a network
  - accessed wherever I am

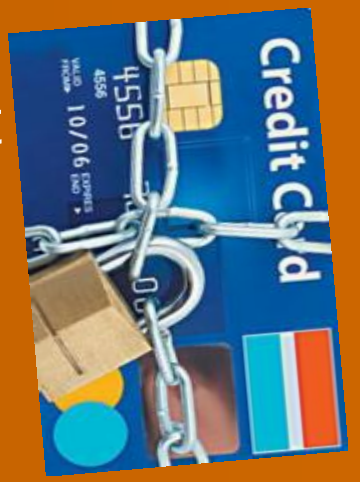


"The overall economic benefit from increased productivity and reduced adverse events that would be achieved with a national individual electronic health record in Australia has been estimated to be between $6.7 billion and $7.9 billion in 2008-09 dollars over 10 years."
National Hospitals & Health Reform Commission staff paper

INFORMATION INTEGRITY SOLUTIONS

How successful could these projects have been with a user-centric focus?

- Google Buzz – controversial launch, could it ever succeed?
- Google+ – more privacy is a marketing point, but 'real names' policy is a deterrent
- Facebook – could it do privacy better & prevent investigations eg Irish Data Protection Commissioner's?
- MasterCard, Visa – eroding consumer trust, more regulation? Customers walk?



INFORMATION INTEGRITY SOLUTIONS

And failing can cost you

- data breaches
  - USA since 2005 2 747 breaches, 542 355 201 records
  - Sony breach: US$20 per person = >US$2 billion
  - complaints handling – (in Singapore up to $1M if things go wrong)
  - increasingly, regulatory response includes alerting customers = data breach notification
  - loss of trust

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.

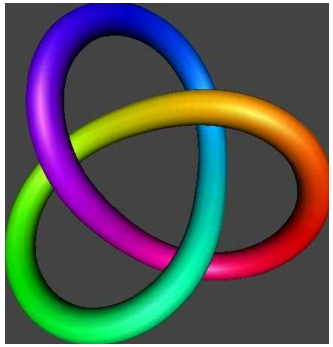
Accountability and Privacy-By-Design Go together Like Innovation and Productivity

www.informationpolicycentre.com

INFORMATION INTEGRITY SOLUTIONS

How can we get it right? – the emerging framework

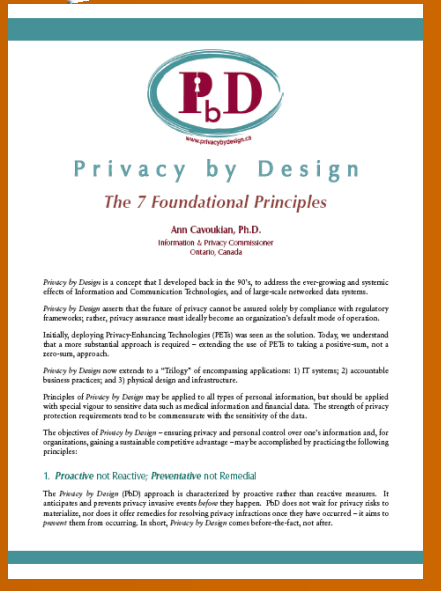
- tools we can build in to our work
  - layered defence
- how to build in the tools
  - Privacy by Design
  - Privacy Impact Assessment (PIAs)
- how to know the tools are being applied year in, year out
  - The Accountability Project



INFORMATION INTEGRITY SOLUTIONS

Privacy by Design (PbD) – privacy is "built in" rather than "bolted on"

- 7 foundational principles
  1. *Proactive* not Reactive; *Preventative* not Remedial
  2. Privacy as the *Default*
  3. Privacy *Embedded* into Design – (e.g. PIAs)
  4. Full Functionality: Positive-Sum, not Zero-Sum
  5. End-to-End Lifecycle Protection
  6. Visibility and Transparency
  7. Respect for User Privacy
- eg IBM, Ontario smart grid



PbD

Privacy by Design

The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is a concept that I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design asserts that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we understand that a more substantial approach is required – extending the use of PETs to taking a positive-sum, not a zero-sum, approach.

Privacy by Design now extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy protection requirements tend to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* – ensuring privacy and personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the following principles:

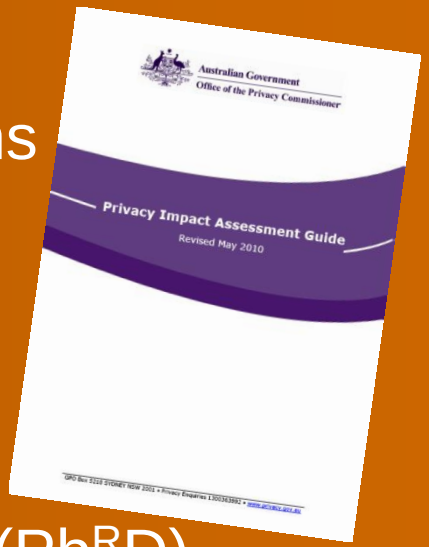
1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

INFORMATION INTEGRITY SOLUTIONS

Beyond compliance: going the extra mile

- new business – PbD
  - check if all that information really needed
  - add layered notices, transparent & readable privacy policy
  - review marketing practices with PbD lens
  - build in transparency and choice
  - privacy enhancing technology
  - privacy impact assessments



- existing business – Privacy by Re-Design (Pb^{R}D)

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 is largely complaints based (as proposed for Singapore)
- Malaysia Personal Data Protection Act 2010 (but no Commissioner/enforcement yet)
- Philippines proposed Data Privacy Act 2011

Protection

Respect

Identity

Value

Accountability

Control

Yield

INFORMATION
INTEGRITY
SOLUTIONS

Malcolm Crompton
Managing Director

53 Balfour Street
Chippendale NSW 2008
Australia

+61 407 014 450

MCrompton@iispartners.com
www.iispartners.com