INFORMATION INTEGRITY SOLUTIONS

Gartner Summits

Closing the Gap: Security → Privacy

Malcolm Crompton
Managing Director
Information Integrity Solutions

Gartner Security & Risk Management Summit
Sydney, 19 August 2013

INFORMATION INTEGRITY SOLUTIONS

About IIS

- Building trust and privacy through global thought leadership and consultancy work for a range of public and private organisations
- Services: privacy governance & strategy; privacy impact assessments and audits; regulator, customer & stakeholder engagement; identity management; privacy training…..

Australian Government

ACC PREVENTION. CARE. RECOVERY.

Microsoft

CommonwealthBank

APEC

ebay

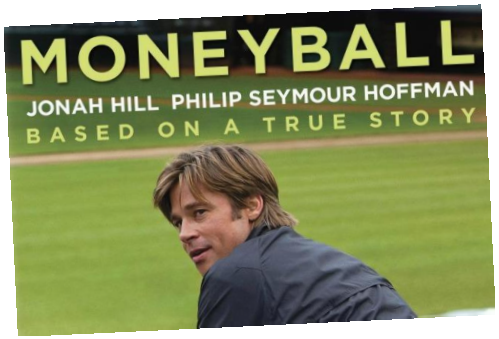
cisco

Google Singapore

Building trust and innovative privacy solutions

INFORMATION
INTEGRITY
SOLUTIONS

Data as asset



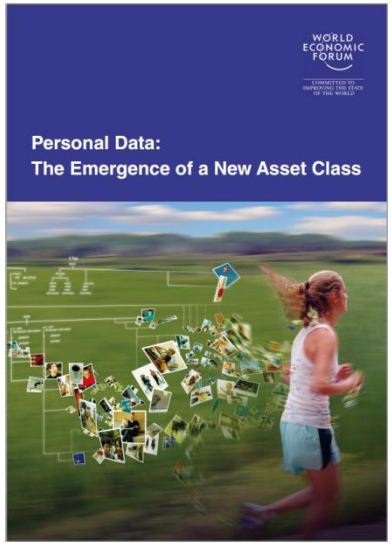
ACXIOM

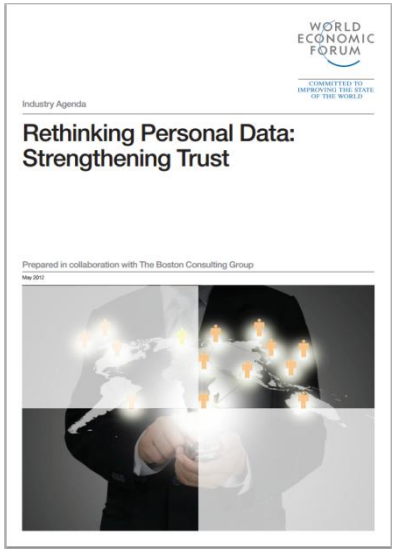
Experian™

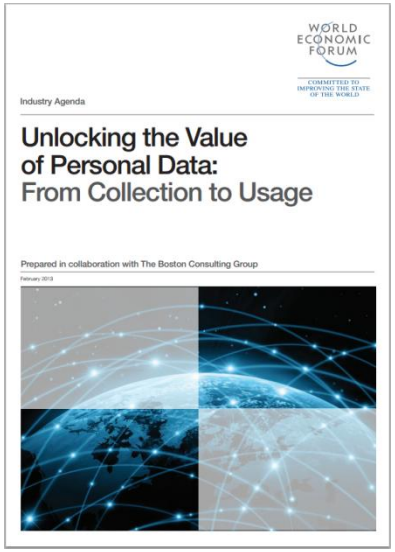
Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Data as asset







- "*As some put it, **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**.*" (2011)
- "*[Solutions to the trusted flow of data] need to reflect the unique characteristics of personal data as an asset class that **increases in value with use**, that can be **copied infinitely** and **distributed globally**, and that **intimately affects 7 billion agents** in the personal data ecosystem.*" (2012)
- "*[T]he economic and social value of big data does not come from its quantity. It also comes from its quality... It is up to the individuals and institutions of various societies **to govern and decide how to unlock the value** – both economic and social – and **ensure suitable protections**.*" (2013)

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Data as liability

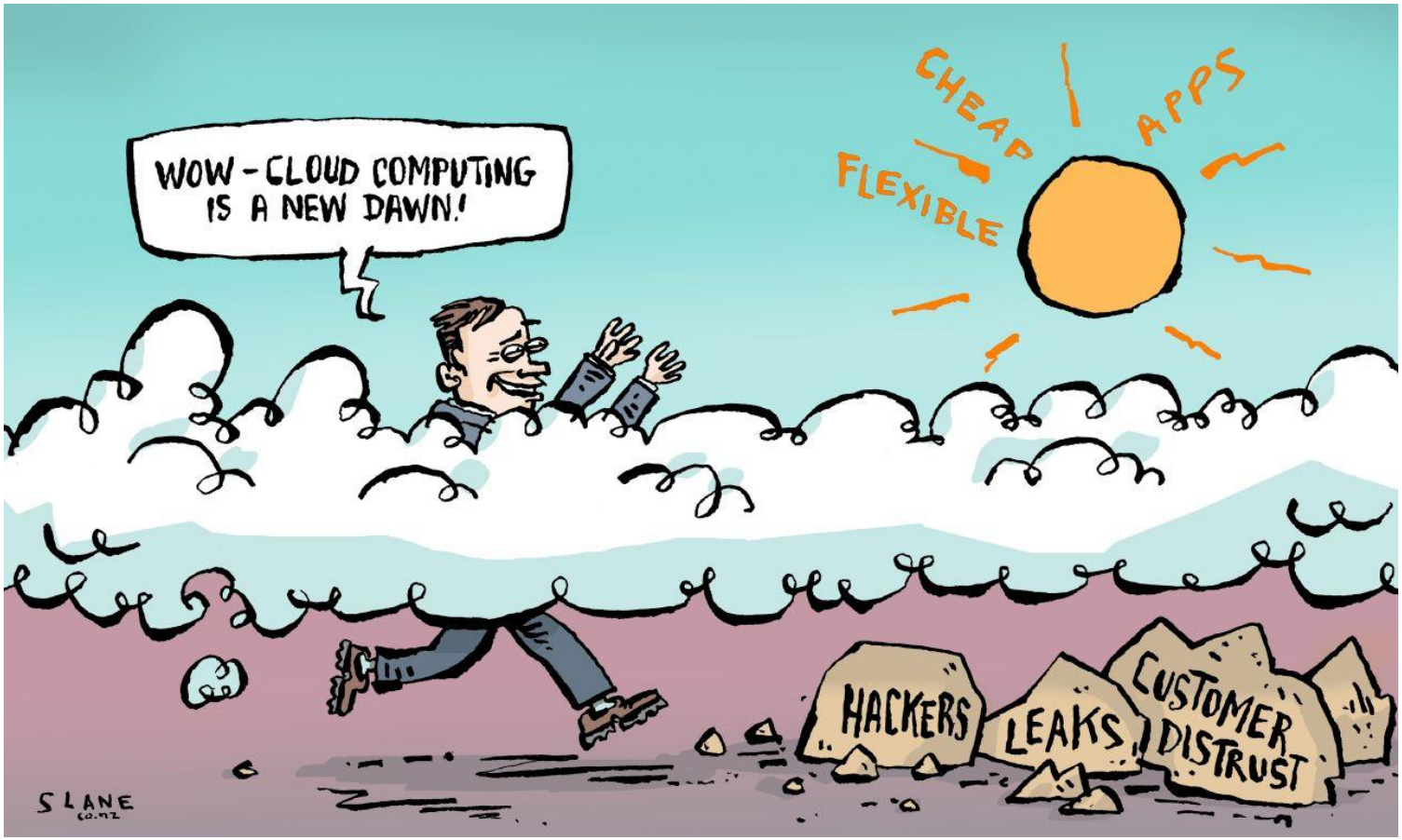
Growing complexity of the digital landscape – how to ensure individuals are not left behind?

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Data as liability

New technologies and familiar risks

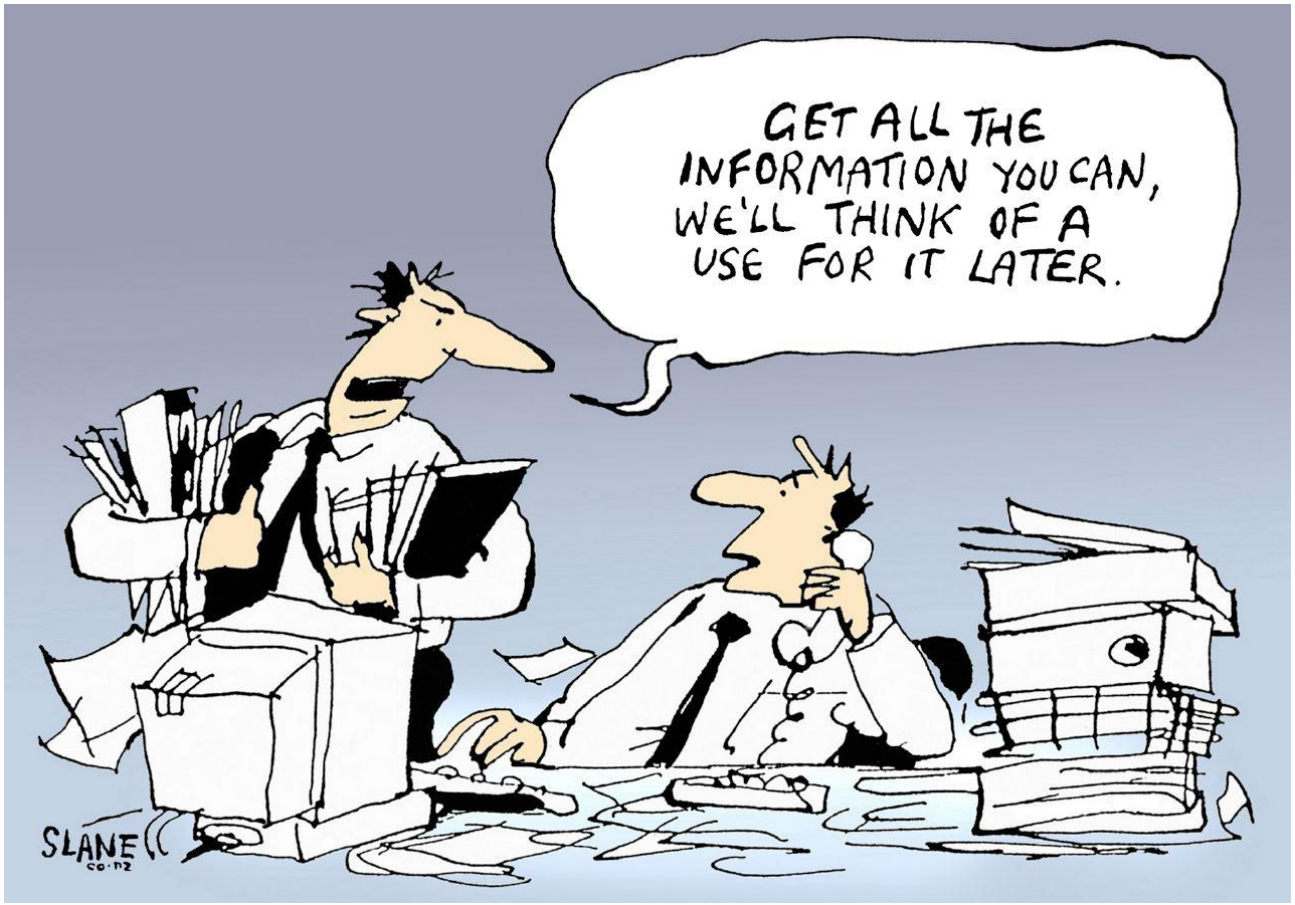


Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Data as liability

Short-sighted policies and practices increase privacy and security risks



Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Data as liability

The end result

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

What's to be done?

- From a security perspective:
  - An asset must be protected

- From a business perspective:
  - An asset can be used to create value

INFORMATION INTEGRITY SOLUTIONS

Common responses

- Confidentiality + integrity + availability = mission accomplished
- "Just encrypt everything"

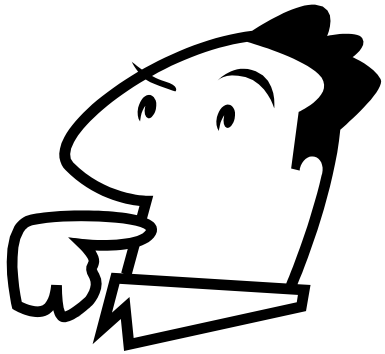
- "Trust us, we'll do the right thing"
- Head in the sand ("That's not my problem")

INFORMATION INTEGRITY SOLUTIONS

It's not that simple

- You can have security without privacy... BUT you cannot have privacy without security

- What's the difference?



INFORMATION INTEGRITY SOLUTIONS

It's not that simple

- Security:
  - Protection and control of personal data

- Privacy:
  - Governance and use of personal data

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

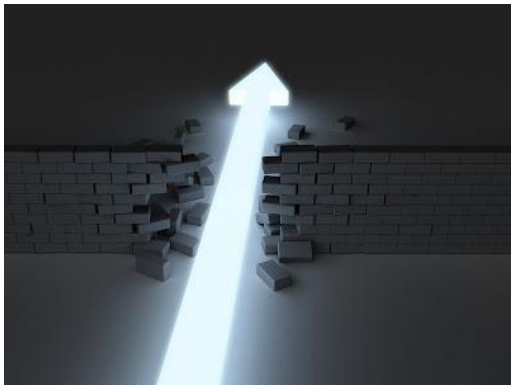
Privacy = security *and more*

- Privacy is not only about keeping the data safe, but also using it in the right way
- Why is this important? **Trust**
- The goal:
  - Derive *value* from the data,
  - In a way that is beneficial for *both* the business and its customers,
  - While maintaining and building *trust*

INFORMATION INTEGRITY SOLUTIONS

Shifting boundaries

- Traditional assumption: getting security right depends on knowing where the organisational boundaries are
- New reality: this has become increasingly difficult, if not impossible...
- Technology exacerbating this trend:
  - Social media – employee or company?
  - Cloud – data sovereignty issues
  - Big Data – how to define new purposes
  - Mobile – BYOD
  - Social media & cloud & mobile – BYOID



INFORMATION INTEGRITY SOLUTIONS

It's all connected

- Security is very much intertwined with privacy:
  - Eg, with BYOD – sometimes the company should know what the employee is doing, but other times it shouldn't
  - A security solution may create privacy problems – eg, monitoring the system through methodical collection of metadata

- Today, information systems architecture is driven by much more than technical factors, including:
  - **What the enterprise wants to achieve**
  - **Environmental factors** that will influence those achievements

  Ann Cavoukian & Marc Chanliau, *Privacy and Security by Design: A Convergence of Paradigms* (2013)

INFORMATION INTEGRITY SOLUTIONS

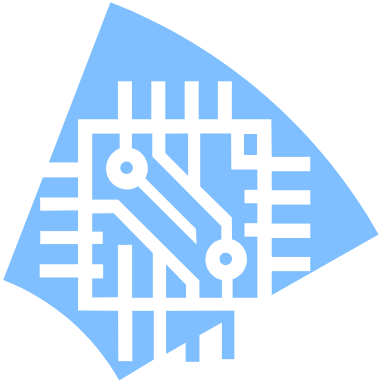
The law is catching up

- **APP 1 – Open and transparent management of personal information**
  - Entity must take reasonable steps in the circumstances to implement practices, procedures and systems that ensure compliance with the APPs
  - Entity must have a clearly expressed and up-to-date policy about management of personal information
- "The bedrock principle"
- Supports a Privacy by Design approach

INFORMATION INTEGRITY SOLUTIONS

What is PbD?

- The design and implementation of systems and processes to **respect individual privacy** while **meeting business objectives**, finding greatest expression in an organisation's:
  - Information technology
  - Physical design and networked infrastructure
  - Accountable business practices



Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

The 7 foundational principles

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial
2. Privacy as the ***Default Setting***
3. Privacy ***Embedded*** into Design
4. Full Functionality: ***Positive-Sum***, not Zero-Sum
5. End-to-End Security – ***Full Lifecycle Protection***
6. ***Visibility*** and ***Transparency*** – Keep it ***Open***
7. ***Respect*** for User Privacy – Keep it ***User-Centric***

PbD

www.privacybydesign.ca

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.

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Case study: Google Buzz

- Classic example of security without privacy (and thereby compromising both): **Google Buzz**

- Privacy missteps:
  1. Participate checkbox pre-selected
  2. Publicly visible list automatically populated from the users' most frequent email contacts
  3. Multiple and non-obvious steps necessary to change privacy settings
  4. Inadequate internal testing failed to detect problems.

INFORMATION INTEGRITY SOLUTIONS

Case study: Google Buzz

- Lessons learnt:
  - Extensive analysis and strong precautions are required when a project significantly alters the way personal information is handled
  - Context is important – business efficacy must be tempered by users' expectations
  - Defaults are powerful shapers of user behaviour
  - **Lack of usability** can increase both security and privacy risks – strong backend security measures not sufficient

INFORMATION INTEGRITY SOLUTIONS

Putting it together

Secure
- Information Security
- Database Security

Trust
- Data Quality Management
- Content Management
- Data Governance

Develop
- Training and Accreditation
- Data Integration
- Data Warehousing Platform
- Database Design and Data Classification
- Data Modelling

Analyse
- Advanced Analytics
- Business Intelligence
- Data Mining

Strategy
- Strategy Development
- Information Architecture

Operate
- Database Management
- Infrastructure Management

Business owner responsibility

IT responsibility

Adapted from: Steve Bennett, News Ltd (2013)

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

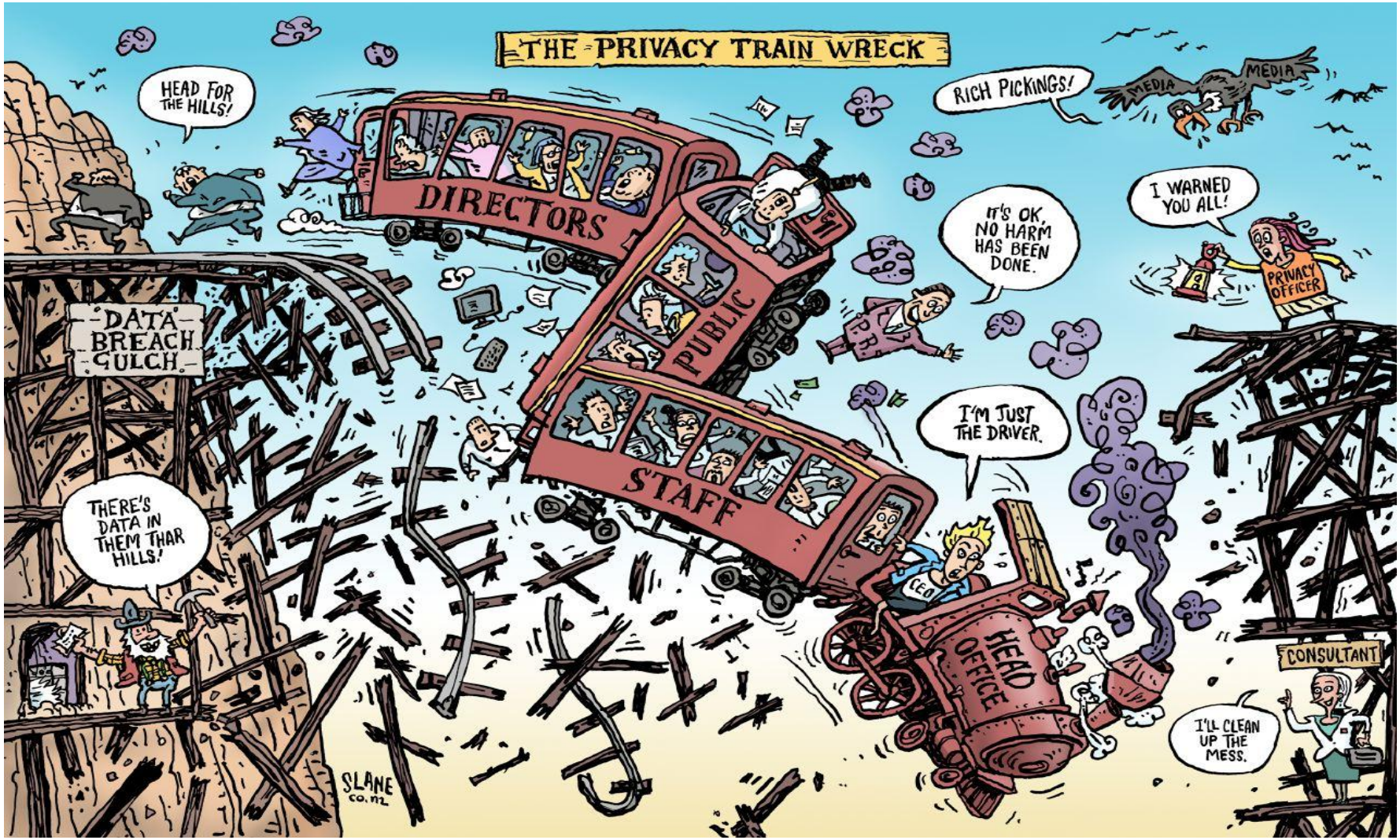
What now?

1. Seek **greater engagement** with:
   - Privacy officers and in-house counsel
   - Policy and business owners
2. Familiarise yourself with the **right tools**, eg:
   - IPC, *Operationalizing* Privacy by Design, Dec 2012
   - OAIC, Guide to Information Security, Apr 2013
3. Put **customer trust** first when developing new products/services as well as back-end systems.

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Don’t delay!



Questions?

INFORMATION
INTEGRITY
SOLUTIONS

Malcolm Crompton
Managing Director

53 Balfour Street
Chippendale NSW 2008
Australia

+61 407 014 450

MCrompton@iispartners.com
www.iispartners.com