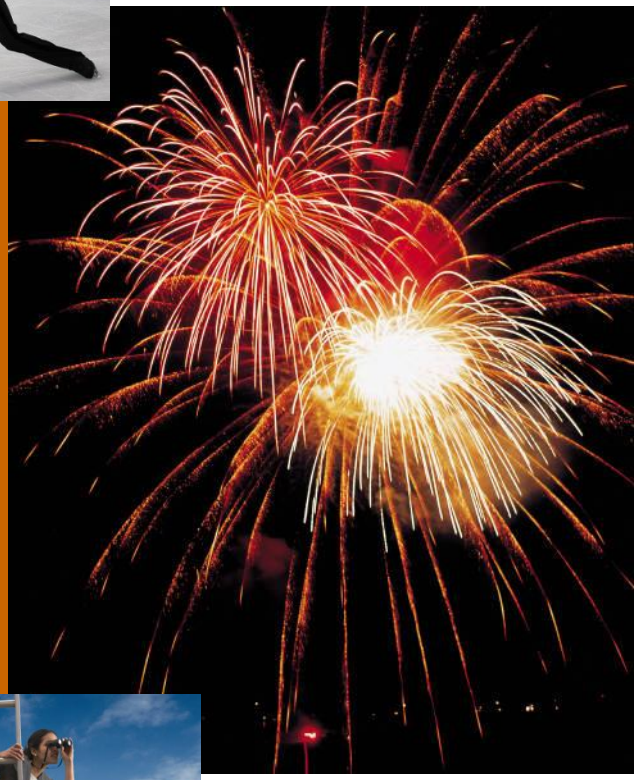
NICTA

Australia's ICT Research Centre of Excellence

INFORMATION INTEGRITY SOLUTIONS



Malcolm Crompton

Privacy by Design: An Oxymoron, An Impossibility or The Way To Go?

NICTA – Big Picture Seminar Series

Brisbane
1 June 2010

PbD

INFORMATION INTEGRITY SOLUTIONS

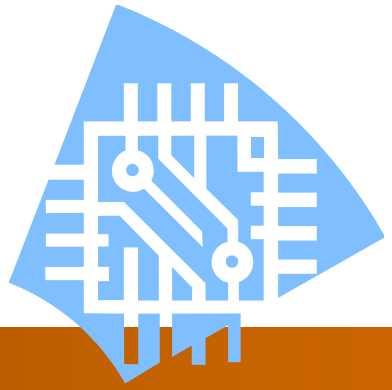
"Privacy" – Outdated? Incompatible? A problem?

Google's Eric Schmidt:
"If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place"

Facebook's Mark Zuckerberg:
"The Age of Privacy is Over"

Louis Freech former Director FBI:
"the American people must be willing to give up a degree of personal privacy in exchange for safety and security"

Sun Microsystems' Scott McNealy:
"You have zero privacy anyway.. get over it."



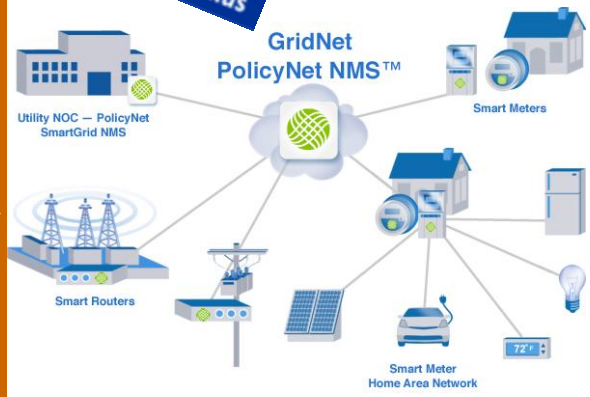
INFORMATION INTEGRITY SOLUTIONS

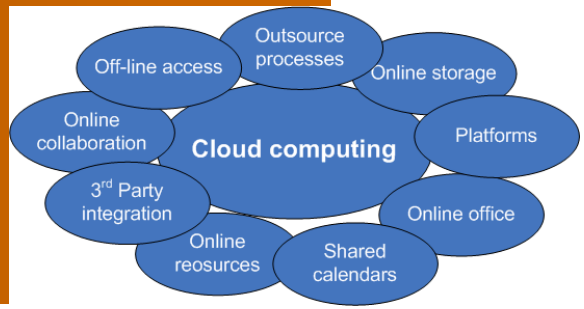
Explosion in new Technology…

- Electronic Health Records
- Social Networking
- Smart grids & other networks
- Location based services
- Mobile banking
- The Cloud
- ….

nehta
National E-Health Transition Authority

Twitter
YouTube
Facebook
myspace.com
a place for friends





INFORMATION INTEGRITY SOLUTIONS

Plenty of evidence that Privacy interests not always well considered

- Road travel
  - E-tags track movements
- Online purchasing
  - ID theft, behavioural targeting
- Social Networking
  - Facebook's recent woes
- Govt. efficiency
  - Australia Card/Access Card
- Privacy v security
  - 9/11, anti-terrorism, surveillance
- Entering a pub or club
  - increasingly ID scanned

1. (noun) **zero-sum game**
a game in which the total of all the gains and losses is zero
Synonyms: zero-sum game

INFORMATION INTEGRITY SOLUTIONS

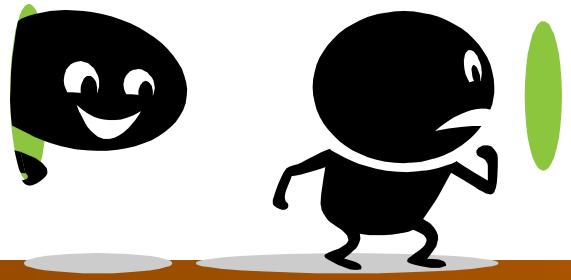
But even the experts don't agree

Mike McConnell, Director of National Intelligence:

"We have a saying in this business: 'Privacy & security are a zero-sum game.'"

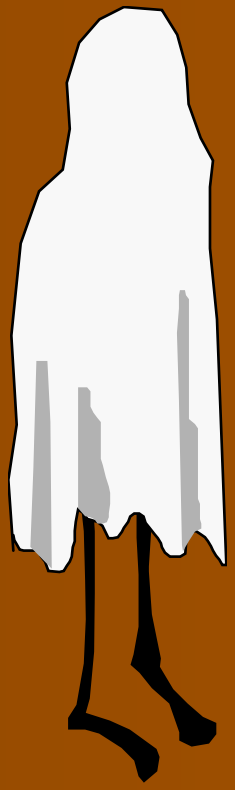
Bruce Schneier:

What Our Top Spy Doesn't Get: Security & Privacy Aren't Opposites



INFORMATION INTEGRITY SOLUTIONS

Privacy – what it isn't …



Keeping everything about yourself secret

or

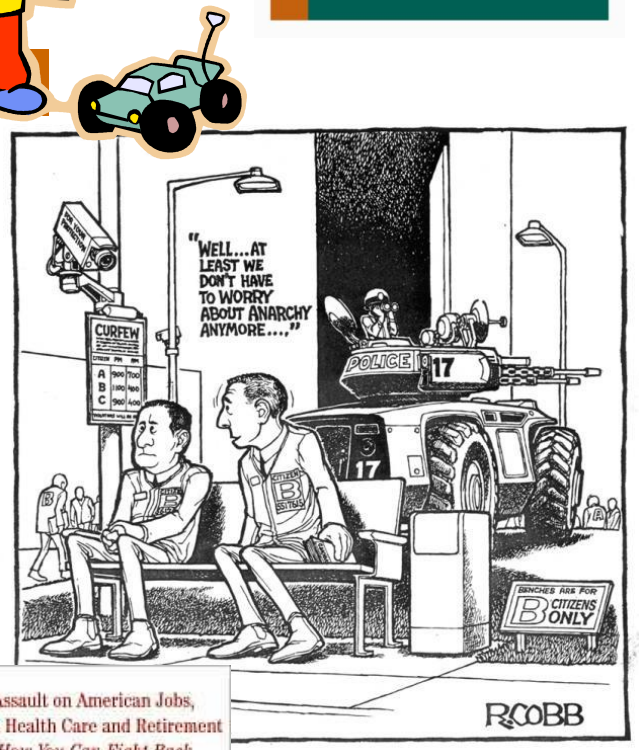
Simply having something to hide

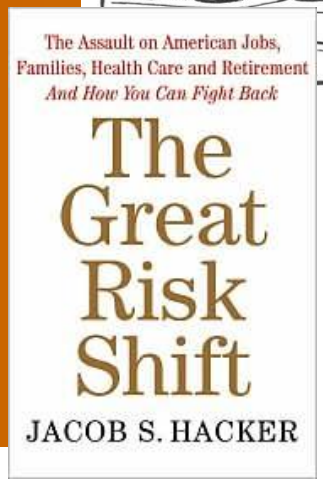
Think about it!

INFORMATION INTEGRITY SOLUTIONS

Privacy – what it IS …

- Control
  - deciding what to reveal and when
  - ‘You can choose your friends, but you can’t choose your relatives’
  - solitude, reserve, autonomy, intimacy
- Creepiness factor
  - big brother, too much information, too intrusive
- Risk
  - who bears it…





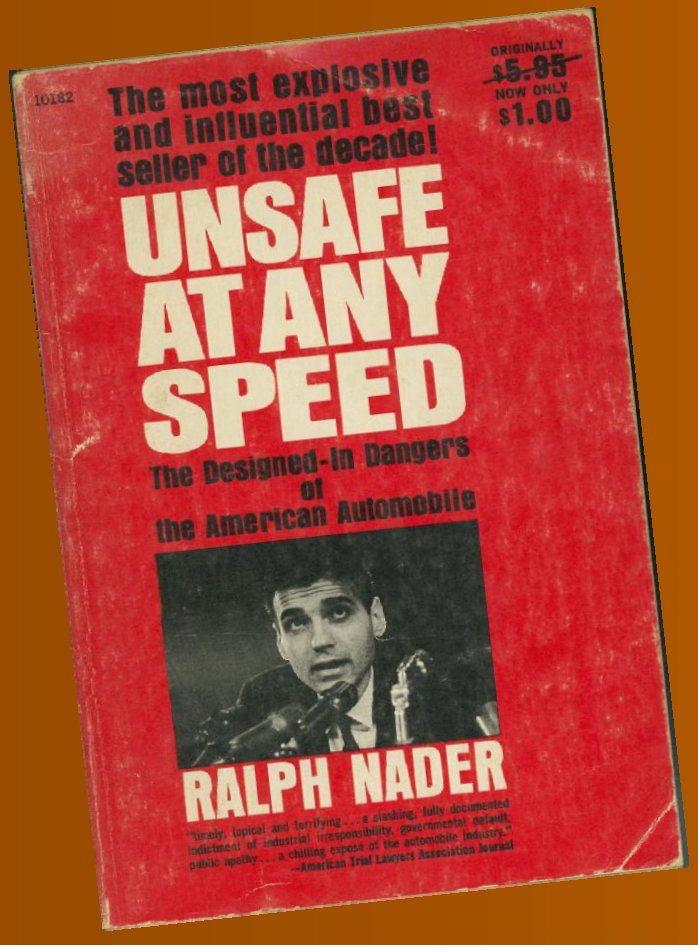
INFORMATION INTEGRITY SOLUTIONS

Is the answer simply more compliance with privacy laws?

- Privacy laws: a great start, but ...
  - don't necessarily cover all that consumers expect or worry about
  - tend to be reactive – they help with the "how" but not with the "what"
- Pace of technology change, amount of information flowing around = getting privacy right even more of a challenge

INFORMATION INTEGRITY SOLUTIONS

"There has to be a better way"



"Unsafe at Any Speed"

▼

Car safety by design

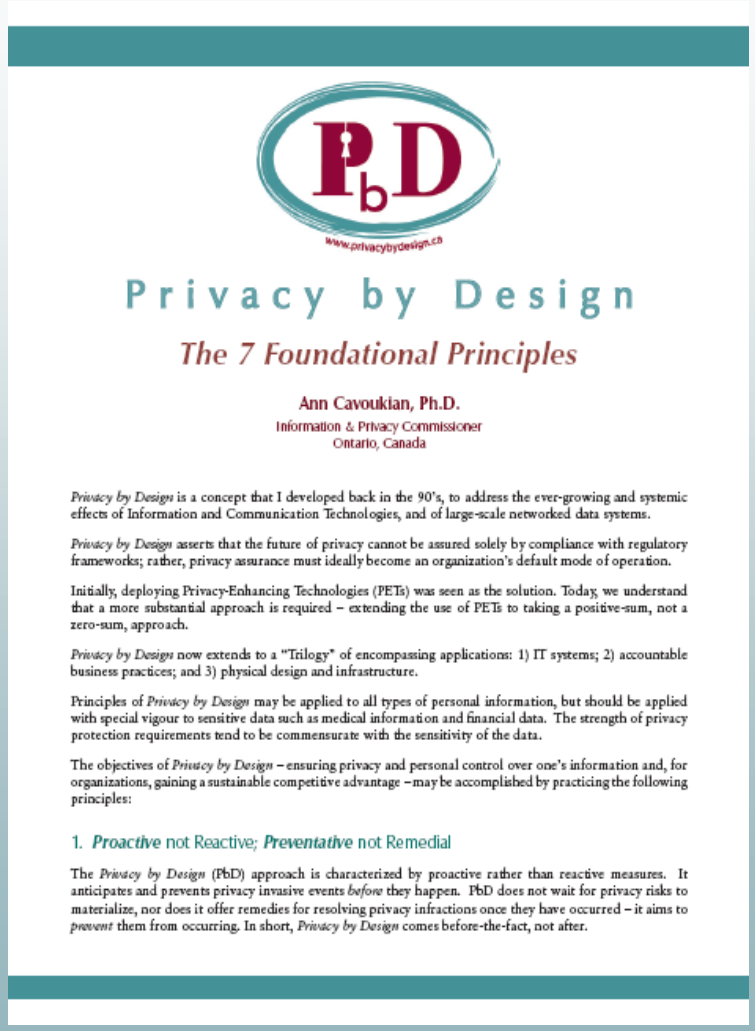
http://en.wikipedia.org/wiki/Unsafe_at_Any_Speed

Why Not:

"Privacy by Design (PBD)"

Privacy by Design: The 7 Foundational Principles

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



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.

www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

INFORMATION INTEGRITY SOLUTIONS

United Kingdom Information Commissioner

2008 Conference

- Building executive support
- Wider use of privacy impact assessments
- Consistent standards for public and private sectors
- Promoting use/research privacy enhancing technology
- More rigorous compliance and enforcement mechanisms

INFORMATION INTEGRITY SOLUTIONS

Regulators expecting more…

Ten Data Protection Commissioners tell Google "…unacceptable to roll out a product that unilaterally renders personal information public, with the intention of repairing problems later as they arise"

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Pamela Jones Harbour (FTC Commissioner) describes Google's approach as "throw it up against the wall and see if it sticks, and if not, we can always pull it back."

EUROPEAN DATA PROTECTION SUPERVISOR
LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES
The European guardian of personal data protection
Le gardien européen de la protection des données personnelles

Peter Hustinx (EDPS) – operationalise privacy by design, including more 'privacy by default' settings

INFORMATION INTEGRITY SOLUTIONS

And some more views on PbD

Harriet Pearson – IBM

- Technology design and technology to support privacy
- Business processes, people, accountability
- Products and customer facing services

- US Department of Commerce
  - PbD needs to be developed carefully to foster not inhibit innovation, cautious about making it law, rather governments can support research, lead by example, focus on technology neutrality

INFORMATION INTEGRITY SOLUTIONS

PbD – towards ‘and’ not ‘or’ privacy solutions

A philosophy

Building privacy in from the start

Building privacy into technology, infrastructure and at all levels

A set of tools

A work in progress

INFORMATION INTEGRITY SOLUTIONS

A practitioner's perspective on PbD

Experience shows that privacy won't just happen

Recognise that good privacy needs a holistic approach:

- Base decisions on early privacy impact assessment
- Reflect social and cultural norms
- Effective/appropriate law and ensure Legal compliance
- Design at every level, not just technology or boxes & wires
  - layered response: processes, people, governance, 'safety net'
- Mix & match – strengthen other protections if there are legal or technology constraints

One is "... by Design".

The other is not.

Both fail on "Privacy".

INFORMATION INTEGRITY SOLUTIONS

PbD could have helped…

- Photocopiers storing copy of what is scanned – ID documents, company secrets – US Congress, Federal Trade Commission "Concerned"
- Airport body scanners that are less intrusive, limiting vision of travellers in the raw or capture & storage of images
- UK ID card – massive stakes, central database, a detailed trail of use and 50,000 people having a look – canned

INFORMATION INTEGRITY SOLUTIONS

Case study: Electronic health Records

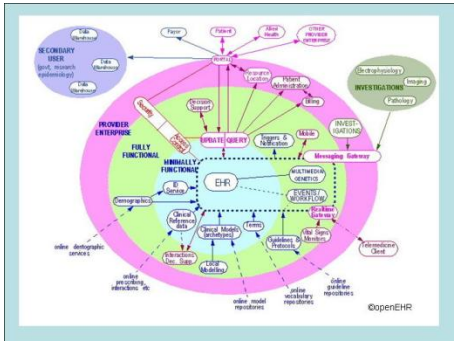
- Individual Health Identifier (IHI) – like it or not, you're getting one
- IHI – like it or not – practitioners and others can use
- Next stage – Electronic Health Records using IHI
- A good start – Nicola Roxon promises Personally Controlled Electronic Health Records for All Australians (Budget 2010)

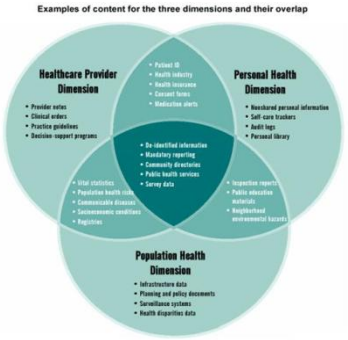
INFORMATION INTEGRITY SOLUTIONS

The EHR PbD story so far

A long gestation starting late 1990s – Not a PbD approach as such but great endeavours on privacy from the word go – the result??

PbD element	Australia's indicative scorecard: Work in progress …
Proactive privacy approach	✔ Still concerns after 10+ years
Early privacy impact assessment	✔ Yes but slow to publish; more 'holistic' still needed
Reflect social and cultural norms	✔ & ✘ Privacy norms in the picture but some overridden
Law and legal compliance	✔ & ✘ IHI law and regs have made a start; more to come
Design decisions	
• Technology	✔ & ✘ Data trail associated with IHI
• People & Processes	✔ & ✘ Control of access to IHI at practice level
• Governance	✔ & ✘ Compliance regime in hot contention
• Safety net	✔ & ✘ May need review





INFORMATION INTEGRITY SOLUTIONS

PbD for genuinely personally controlled EHR

- Good answers to complex issues such as
  - Central or distributed storage of records
  - Consumer control over access to whole/part of a record
  - Agreed processes for 'break glass' emergency
  - Role-based authentication & authorisation at individual provider level
  - Trustworthy security
  - Clear & credible accountability & compliance processes
  - The right law with real teeth with credible enforcement

PRIME
Privacy and Identity Management for Europe

PrimeLife

INFORMATION INTEGRITY SOLUTIONS

Identity management

- The old way: Digital God
  - Brings you into digital existence
  - Takes you out of digital existence
  - Watches every move in between …
- A better way
  - User centric; user controlled
  - Government and others investigating probabilistic, reputation based approaches
  - Rely on ID assertions last

INFORMATION INTEGRITY SOLUTIONS

PbD – Queensland example

New QLD Licence with Smartcard technology

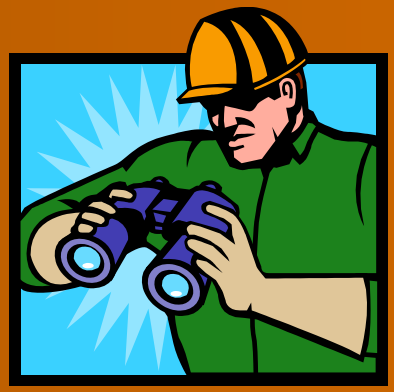
PbD elements include:

- Early consideration of privacy: Govt. Committee, PIAs
- Design of chip
- Surrounding processes including who gets access to what

INFORMATION INTEGRITY SOLUTIONS

NQDL – things to watch

- Early days – full rollout 2011



- Will privacy promises be kept?

- Address on card could go to enhance privacy?

- Potential for more government departments to read securely stored information – change process?

[Play full screen version of movie that is online at the following page of the Microsoft End to End Trust pages:

www.microsoft.com/mscorp/twc/endtoendtrust/vision/eid.aspx]

INFORMATION INTEGRITY SOLUTIONS

PbD - its doable

- Don’t settle for any thing less for yourself
- Don’t settle for anything less from others

INFORMATION
INTEGRITY
SOLUTIONS

Malcolm Crompton
Managing Director

53 Balfour Street
Chippendale NSW 2008
Australia

+61 407 014 450

MCrompton@iispartners.com
www.iispartners.com