INFORMATION INTEGRITY SOLUTIONS

PREVENTION. CARE. RECOVERY.

Te Kaporeihana Āwhina Hunga Whara

The Cone of Silence – Data Protection and Privacy

What every in-house lawyer should know

Malcolm Crompton – Managing Director, IIS

Mary Ahern – Senior Solicitor, ACC

Corporate Lawyers Association of New Zealand

Napier, 16 May 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 and strategy, privacy impact assessments and audits, regulator, customer and stakeholder engagement, identity management, privacy training.....

The Department of Internal Affairs
Te Tari Taiwhenua

Australia Post

Google

Australian Government

CommonwealthBank

ACC
PREVENTION. CARE. RECOVERY.

NSW GOVERNMENT

Microsoft

INFORMATION INTEGRITY SOLUTIONS

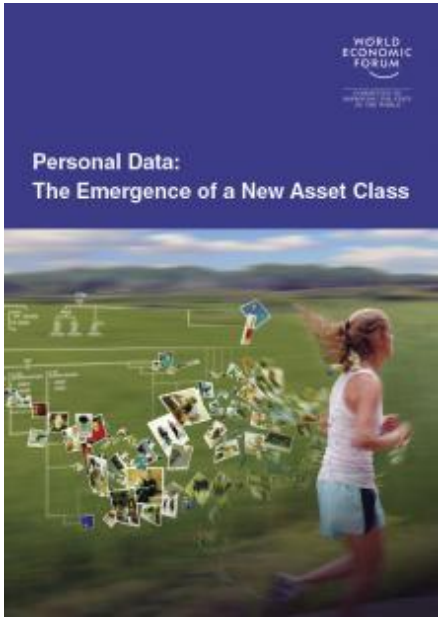
Outline

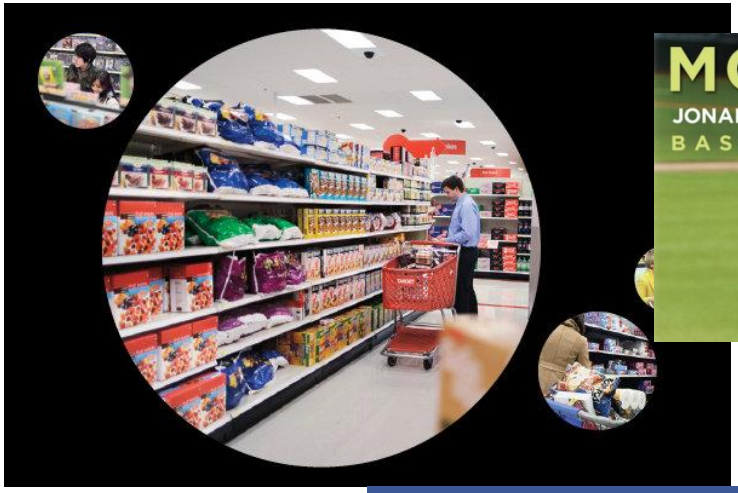
- Data as asset and liability
- Summary of ACC Review
- ACC – Facts and challenges
- ACC – The way forward
- Implications for in-house lawyers
- Key takeaways
- Questions

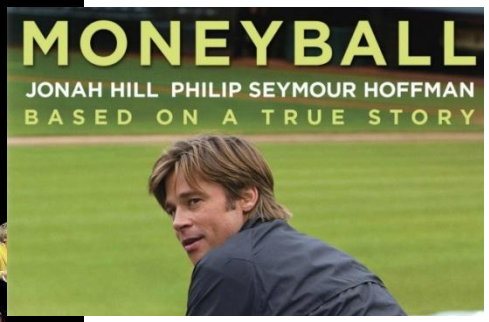
Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Data as asset







ACXIOM

Real Analytics for facebook

"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 … Stakeholders will need to embrace the uncertainty, ambiguity and risk of an emerging ecosystem."* – World Economic Forum (2011)

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

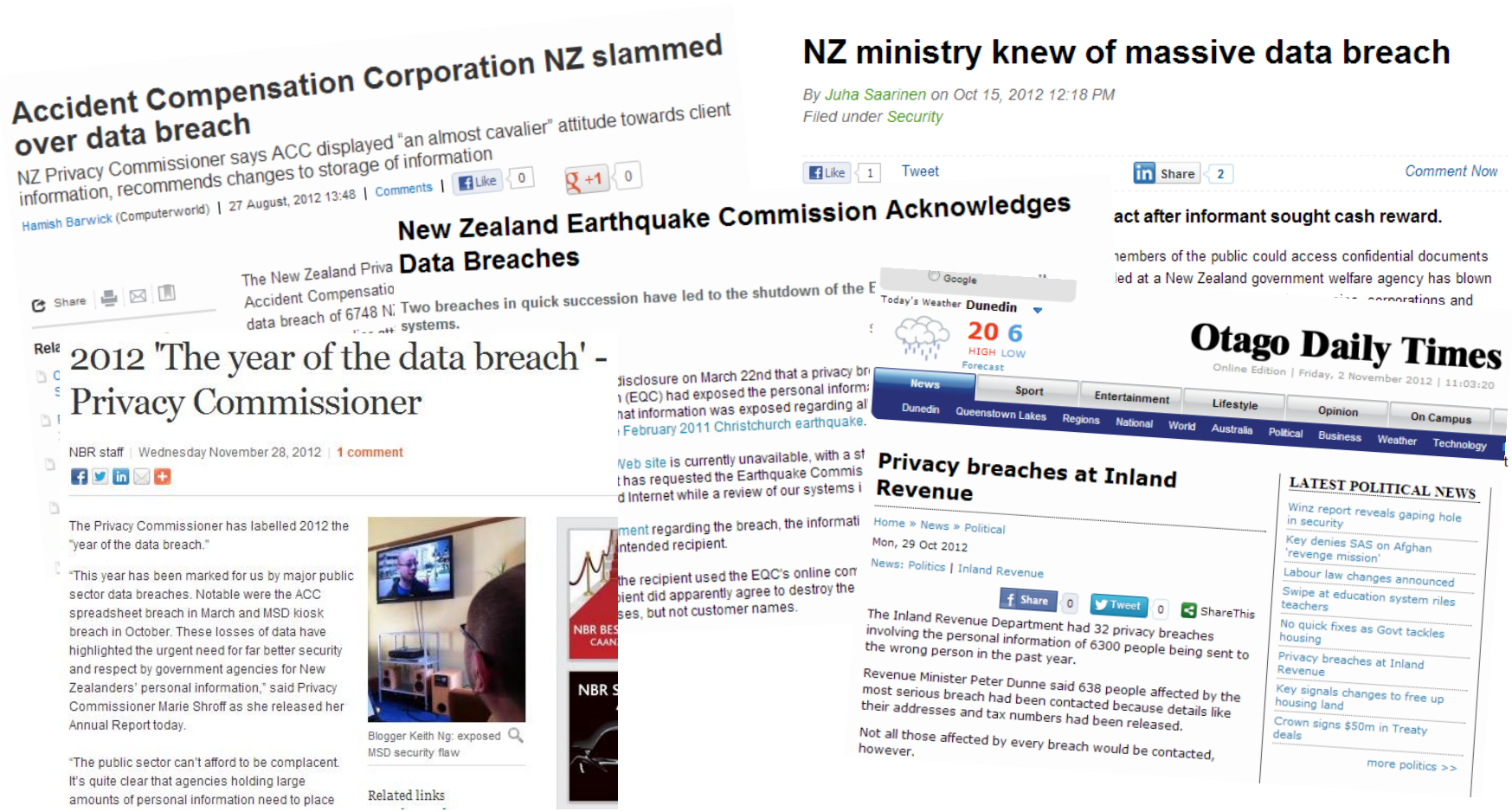
Data as liability

- Data may be vulnerable to external parties, who act for fun and/or profit
  - **52%** of attacks involved some form of **hacking**
  - **76%** of network intrusions exploited **weak or stolen credentials**
  - **71%** of attacks targeted user devices
  - **66%** of data breaches took months to discover

Source: Verizon, '2013 Data Breach Investigations Report' **(2013)**

INFORMATION INTEGRITY SOLUTIONS

In New Zealand



Accident Compensation Corporation NZ slammed over data breach

NZ Privacy Commissioner says ACC displayed "an almost cavalier" attitude towards client information, recommends changes to storage of information

Hamish Barwick (Computerworld) | 27 August, 2012 13:48 | Comments | Like 0 +1 0

The New Zealand Priva
Accident Compensatio
data breach of 6748 N

New Zealand Earthquake Commission Acknowledges Data Breaches

Two breaches in quick succession have led to the shutdown of the E
systems.

disclosure on March 22nd that a privacy br
(EQC) had exposed the personal inform
hat information was exposed regarding al
February 2011 Christchurch earthquake.

Web site is currently unavailable, with a st
has requested the Earthquake Commis
d Internet while a review of our systems i

ment regarding the breach, the informati
ntended recipient.

he recipient used the EQC's online com
ient did apparently agree to destroy the
es, but not customer names.

NZ ministry knew of massive data breach

By Juha Saarinen on Oct 15, 2012 12:18 PM
Filed under Security

Like 1 Tweet Share 2 Comment Now

act after informant sought cash reward.

embers of the public could access confidential documents
ed at a New Zealand government welfare agency has blown
corporations and

2012 'The year of the data breach' - Privacy Commissioner

NBR staff | Wednesday November 28, 2012 | 1 comment

The Privacy Commissioner has labelled 2012 the "year of the data breach."

"This year has been marked for us by major public sector data breaches. Notable were the ACC spreadsheet breach in March and MSD kiosk breach in October. These losses of data have highlighted the urgent need for far better security and respect by government agencies for New Zealanders' personal information," said Privacy Commissioner Marie Shroff as she released her Annual Report today.

"The public sector can't afford to be complacent. It's quite clear that agencies holding large amounts of personal information need to place

Blogger Keith Ng: exposed MSD security flaw

Related links

Google
Today's Weather Dunedin
20 6
HIGH LOW
Forecast

Otago Daily Times
Online Edition | Friday, 2 November 2012 | 11:03:20

News Sport Entertainment Lifestyle Opinion On Campus
Dunedin Queenstown Lakes Regions National World Australia Political Business Weather Technology

Privacy breaches at Inland Revenue

Home » News » Political
Mon, 29 Oct 2012
News: Politics | Inland Revenue

Share 0 Tweet 0 ShareThis

The Inland Revenue Department had 32 privacy breaches involving the personal information of 6300 people being sent to the wrong person in the past year.

Revenue Minister Peter Dunne said 638 people affected by the most serious breach had been contacted because details like their addresses and tax numbers had been released.

Not all those affected by every breach would be contacted, however.

LATEST POLITICAL NEWS

Winz report reveals gaping hole in security
Key denies SAS on Afghan 'revenge mission'
Labour law changes announced
Swipe at education system riles teachers
No quick fixes as Govt tackles housing
Privacy breaches at Inland Revenue
Key signals changes to free up housing land
Crown signs $50m in Treaty deals

more politics >>

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Cost of breaches

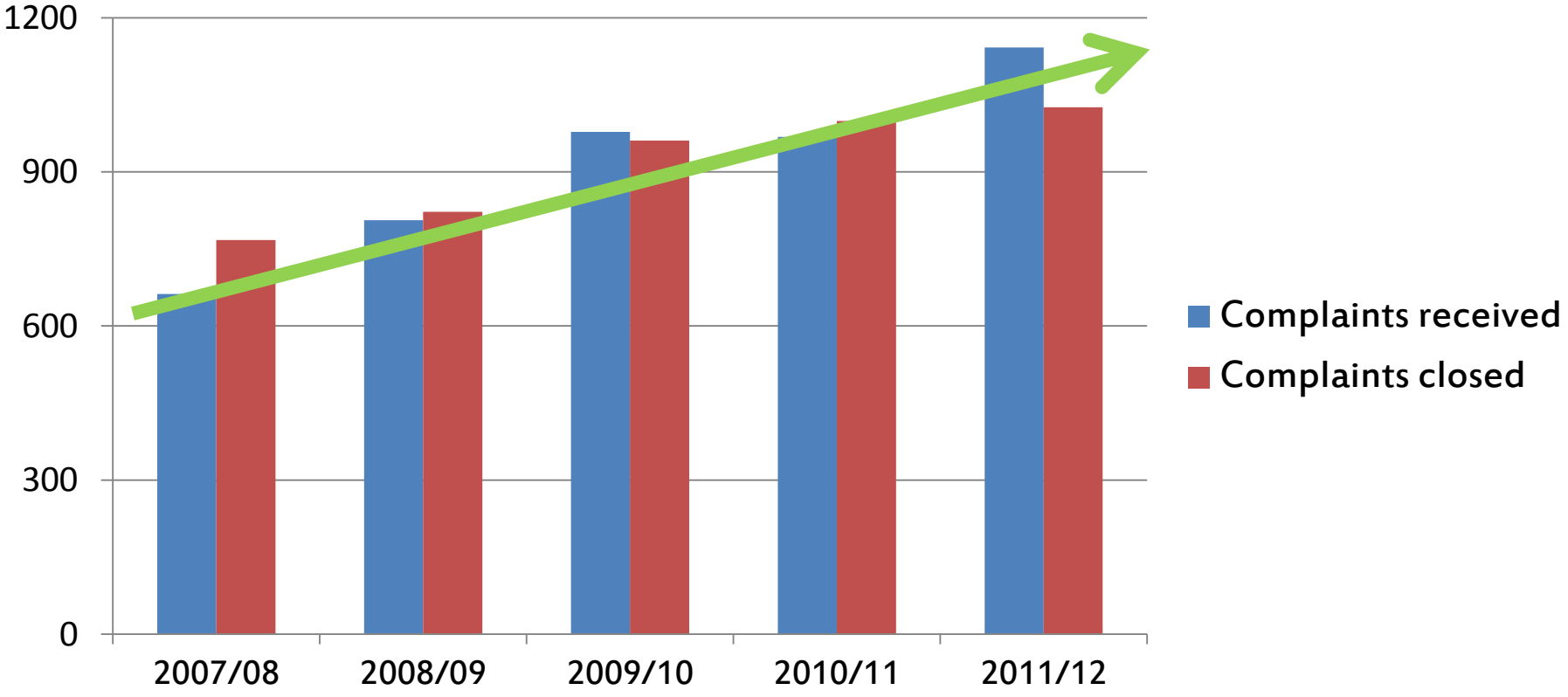
- Cost to organisations
  - Aus – $2.3M per org ($138 per record)
  - Intangibles – reputation and trust

- Financial costs reduced by:
  - External consulting support ($45 per record)
  - CISO and overall data protection strategy ($35 per record)
- Cost to *individuals*
  - Fraud; time, money and effort to resolve the issue

Source: Ponemon Institute, "2011 Cost of Data Breach Study: Australia' (2012)

INFORMATION INTEGRITY SOLUTIONS

It could happen to anyone



Source: Privacy Commissioner (NZ), 'Annual Report 2012' (2012)

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Privacy matters

- The people have spoken:
  - **67%** – Concerned or very concerned with privacy, the highest level recorded and up from 47% in 2001
  - **92%** – "It's extremely important that government agencies properly protect the information I give them"
  - **88%** - "Businesses should be punished if they misuse people's personal information"

Source: UMR Research, 'Individual privacy and personal information' (2012)

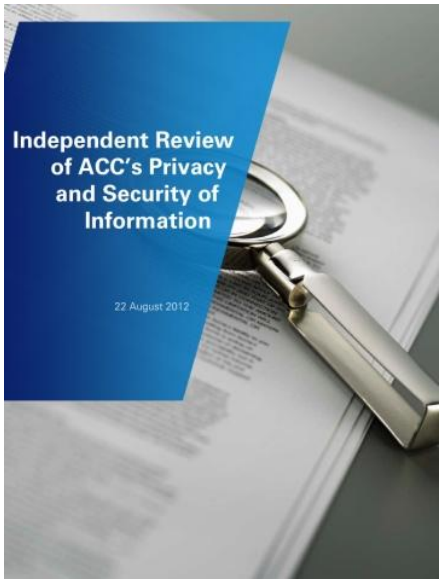
- The experts have spoken…

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

ACC Review

- **Findings:** breach was a genuine error, but arose in the context of systemic weaknesses in ACC's business as usual
  - Technology and business practice – multiple monitors and spreadsheets
  - Culture – inconsistent respect for personal information
  - Privacy management – lack of accountability
- Privacy is a **whole-of-business concern**



Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

ACC Review

- Framework for good privacy management

Response

- Crisis management
- Established a dedicated toll-free service and response team
- Called all clients in released list to advise of the breach and confirmed in writing with an apology, within 5 days

Breach / Related

PREVENTION. CARE. RECOVERY.
Te Kaporeihana Āwhina Hunga Whara

POLITICS

Scorn poured on ACC privac

Phil Kitchin
INVESTIGATIONS EDITOR

FAMILY NOTICES, NEWS

Rape Crisis centre anxiety over ACC's error

by Sophie Rishworth

WOMEN have been calling the Gisborne Rape Crisis Centre, anxious that their details are now in the public domain after ACC acknowledged a

counsellors or doctors," she said.
The Rape Crisis Centre in Gisborne has about 50 women on their ra
who have been victi
abuse

ACC to send mountain of apologies

unit, the sensitive claims unit.
The recipient of the information spoke to *The Dominion Post* after repeatedly raisi
issues of systemic privacy f
by ACC in handling
lected, used
claimants'

of those clients but ACC had failed to protect those clients' privacy, e said.
ACC yesterday invited clients king a settlement or compen- to write to the corporation's y officer and said the issue e dealt with on a case by is.

SLOPPY PRIVACY PROTECTION, SAYS CLIENT

A man who was paid $12,
ACC for breaching his pri
later sent sensitive inform
the corporation relating
investigations.
Even after being ordere

people still have privacy rights yet
care less."
ongly sent

the privacy commissioner upheld in 2007."
He said it had taken him nearly five
ars to settle that breach and he
veral other privacy

ACC apologises to thousands of clients

By AMELIA ROMANOS

WELLINGTON: ACC has apologised for an error that led to information about thousands of claimants being emailed to an

The organisation said the client would not respond to its request for the information to be returned and, until yesterday, the client would not confirm that it had any confidential informa-

calls yesterday from clients concerned about the data breach.
The news was deeply upsetting. Maintaining trust in ACC was vital, because of the information the corporation held

INSIGHT

Apology meaningless

There's an old saying that it's too late to be sorry. ACC needs to remember that.

Chief executive Ralph Stewart yesterday apologised for the latest gaffe by his staff and said they would be calling or writing to

But it wasn't until the c Fairfax journalist that AC the situation seriously.

A spokeswoman said tl had done more to inve Stewart said the breach

POLITICS

ACC manager 'failed to do enough' about breach

Official knew about huge privacy slip-up for three months before chiefs found out

by Adam Bennett and Amelia Romanos

Senior ACC manager Philip Murch knew of a potentially major breach of the privacy of more than 6000 claim-

meeting with the
during a r
claimant in
He sent
to her the
return the

Mr Stewart said he did not k
whether Mr Murch had let his imm
superiors know about the pote
became aware

NEWS

Call to compensate clients

WELLINGTON — The Accident Compensation Corporation is being called on to compensate thousands of people whose claim details were inadvertently emailed to an ACC client

review, those that succeed and those that don't."
Wellington's Rape Crisis agency manager, Natalie Gousmett, many of its clients are in the

- Technology and process changes- ongoing, cont..

Some ideas not so workable

- Refusing to courier files

Stress to staff causing

- oversensitivity about releasing information

The challenges

Retrieving information

- The good – prompt return
  - Same day interim injunction
- the bad - Five months to get court orders
- the perplexing

Volume of information

On a daily basis, ACC

- Operates across 48 locations
- Sends 25,000 letters to claimants, levy payers and health providers
- Answers over 24,000 calls
- Processes up to 7,500 claims

On an annual basis, ACC

- Handles 1.6 million claims
- Purchases $1.7 billion health and disability services
- Engages 20,000 individual registered providers

The way forward

- Technology changes
- Culture changes
- A long game

INFORMATION INTEGRITY SOLUTIONS

Implications for in-house lawyers

- Organisational role
- Expertise
  - Understanding Privacy by Design
- Risk management
  - Privacy Impact Assessments
  - Contracted service providers
  - Assurance and review
  - Managing data breaches

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Organisational role

- Know what your role is and how privacy fits into it
- Buy into the organisation's culture, governance structure and strategic vision
- Be familiar with the organisation's information handling practices
- **Raise awareness:**
  - Privacy is an important issue
  - You can make a difference

INFORMATION INTEGRITY SOLUTIONS

Expertise

- Keep up-to-date with latest privacy developments:
  - Privacy law reform in NZ
  - International developments – eg, APEC, US, EU
  - Technologies – eg, Big Data, Internet of Things
- Understand the most widely endorsed approach to fostering organisational privacy: **Privacy by Design**

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Privacy by Design

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

Risk management

Privacy Impact Assessment

- Identify and manage privacy risks and opportunities
- Features of PIA:
  - Prospective – looking at the future privacy impacts
  - Iterative – conducting analysis and feeding back into the design process
  - Risk & opportunity management – for both org and individuals
- See Privacy Commissioner's PIA Handbook

Building trust and innovative privacy solutions

INFORMATION INTEGRITY SOLUTIONS

Risk management

Contracted service providers

- Be careful when engaging CSPs:
  - Read terms carefully and clarify ambiguous provisions
  - Find out where and how the data will be stored
  - Find out CSP's arrangements with third-party subcontractors
  - Clarify rights of access, correction and deletion
  - Determine liability – what happens when things go wrong
  - Determine accountability – 'corrective', 'detective' and 'preventative'
  - Enforce

INFORMATION INTEGRITY SOLUTIONS

Risk management

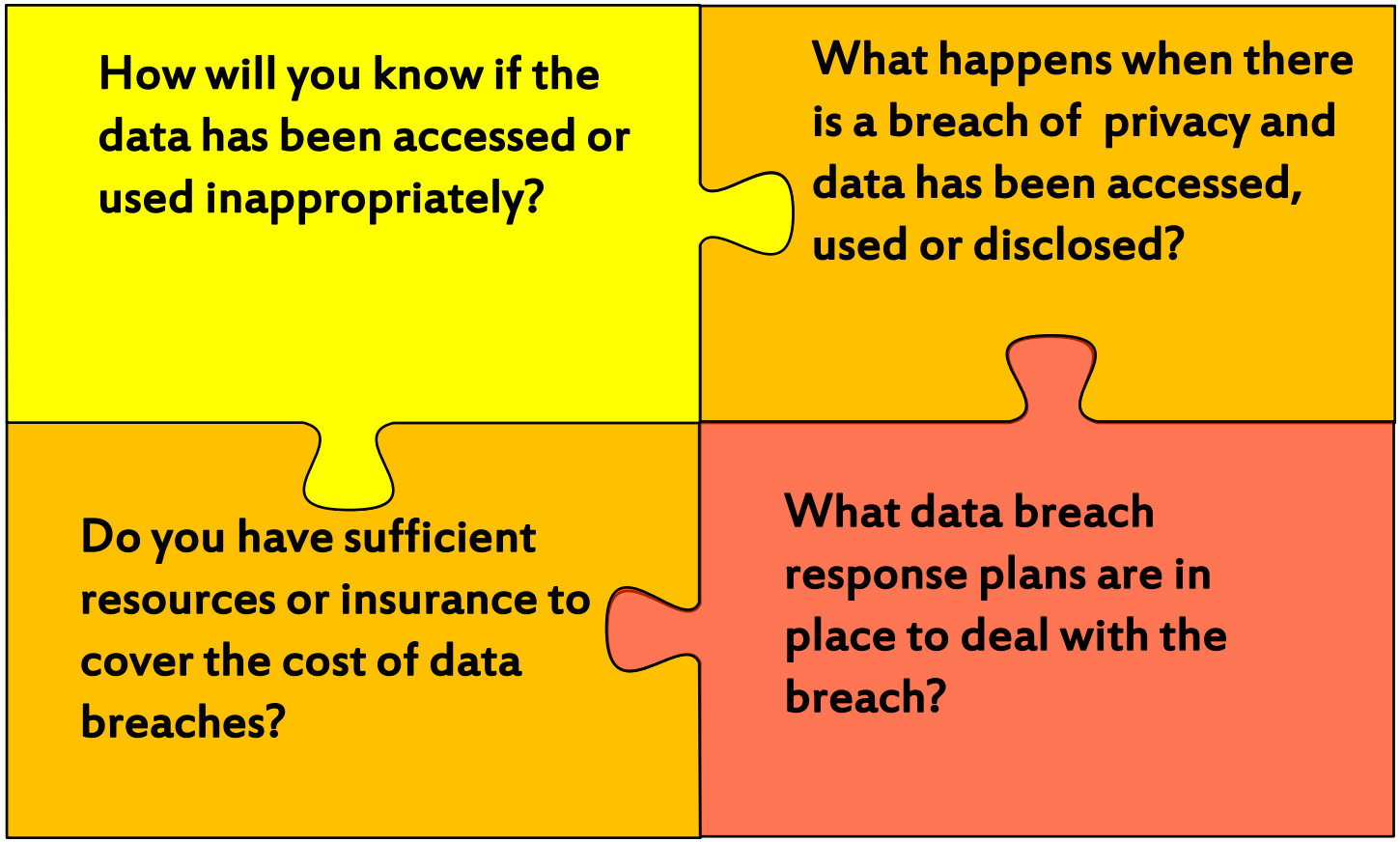
Assurance and review

- Monitor compliance with privacy and security policy
- Periodically review new risks and adequacy of existing measures
- Update policies and procedures when required

INFORMATION INTEGRITY SOLUTIONS

Risk management

Managing data breaches



INFORMATION INTEGRITY SOLUTIONS

Risk management

Managing data breaches

1. Contain breach and do a preliminary assessment
2. Appoint a response leader (internal or external)
3. Evaluate risks associated with the breach
4. Consider notification to affected individuals and/or the Privacy Commissioner
5. Review incident and take action to prevent future breaches

INFORMATION INTEGRITY SOLUTIONS

Key takeaways

- Be wise, be prepared – it could happen to you
- Good privacy is *not just* about stopping data breaches
- Getting data management and privacy right requires a whole-of-business response
  - Addressing governance and risk issues
  - Strong leadership required

Building trust and innovative privacy solutions

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