UNSW
THE UNIVERSITY OF NEW SOUTH WALES
SYDNEY • AUSTRALIA

cse

INFORMATION
INTEGRITY
SOLUTIONS

Malcolm Crompton

Trust & user centric ID management at the human level: implications for systems design

CSE Seminar
University of New South Wales

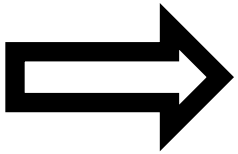
Sydney
3 June 2009

“If you have nothing to hide, you have nothing to fear”

John Major, UK PM
“A Cautionary Tale for a New Age of Surveillance”, NY Times, 7 Oct 2001

So, what’s the problem?

Case study: Australia's failed Access Card



Lost community trust because of:

- Hidden agendas – lack of transparency
- Centralisation of very sensitive information
- Inadequate governance and accountability
- De facto compulsory despite claims

The old website:

www.accesscard.gov.au

Fears over smart card as privacy breaches revealed

Public servant snoops

Tanya Giles and Peter Mickelburough

Sun-Herald, 14 Oct 2006

HUNDREDS of public servants have been caught spying on the private information of citizens in federal and state government agencies.

Most of the 1000-plus victims were never told details of their private lives, including personal, financial, health, police and emergency records, had been invaded.

A *Herald Sun* survey of 15 key federal and state departments and agencies, which hold up to 100 million secret files on individuals, found 650 public servants were sacked or sanctioned for snooping on their clients in the past year.

The revelation comes as Canberra pushes ahead with controversial plans to replace 17 health and welfare cards with a single smart card.

The *Herald Sun* found confidential files were breached at VicRoads, Victoria Police, Corrections Victoria, Centrelink, Medicare, the tax office and the Emergency Services Telecommunications Authority.

The breaches occurred despite strict policies designed to protect private information.

The *Herald Sun* investigation found Medicare investigated 23 breaches in 2005-06, referring one case of alleged fraud and theft to federal police.

Thirteen Medicare workers remain under investigation, four have been sacked, five have resigned and one has been counselled.

Medicare spokesman Peter Sexton said Medicare was beefing up security, including audits and tighter controls on access to records.

Other new privacy intrusion cases included VicRoads, which holds 7.5 million files.

VicRoads probed 21 complaints in 2005-06, leading to two resignations and two reprimands.

VicRoads spokeswoman Kara O'Dwyer said all staff were warned not to use, release, disclose or study people's files for unofficial reasons.

Victoria Police has acted against 19 staff after high-profile leaks of more than 800 files from its LEAP database.

Fourteen police were fined, three were put on good behaviour bonds, three were demoted and one was reprimanded.

Other privacy breaches last year included:

FIVE staff at the Department of Human Services counselled over "inadvertent" breaches.

THREE corrections staff who looked at records of inmates and a prison officer whistleblower.

ONE allegation against a WorkCover employee that could not be substantiated.

The tax office last month sanctioned 24 staff for privacy breaches. Four were sacked, 12 resigned, two were fined and six had their pay cut or were demoted.

Two were prosecuted under the Tax Act, with one sentenced to community service and the other fined.

The worst offender was Centrelink, which last month admitted 111 staff were sacked or had resigned for looking at welfare recipients' files.

Centrelink has disciplined 585 staff for wrongly accessing customer records on 790 occasions since 2004.

Labor's human services spokesman, Kelvin Thomson, said the breaches should ring alarm bells for Australians.

Mr Thomson said Human Services Minister Joe Hockey, who is responsible for Centrelink and the smart card, must show how he would protect privacy.

Mr Hockey said rigorous controls to ensure maximum privacy were being developed for the smart card.

INFORMATION INTEGRITY SOLUTIONS

Trust

"The ongoing debate about data privacy needs to evolve into a dialogue about consumer trust …

"The Yankelovich *Consumer Trust Report* clearly pointed out the need for a new approach. 'The state of mistrust is not a new problem, but it is one that can no longer be ignored,' Wood said. 'According to our findings, 80% of consumers believe American businesses are too concerned about making a profit and not concerned enough about their responsibilities …'

"Distrust has a potentially devastating impact on profitability … Almost half (45%) of the respondents say there is at least one retail business that they trusted at one time but no longer trust. Of those people, nearly all (94%) say they spent less money with that company, resulting in an average 87% decrease in spending by that group."

Craig Rogers, Yankelovich Partners, Press Release on *The State of Consumer Trust Report* 8 June 2004

INFORMATION INTEGRITY SOLUTIONS

The trust deficit – Impact

We avoid engagement

We defend – minimise or falsify our responses

We call for more law regardless of impact

Opportunities missed to develop close relationships

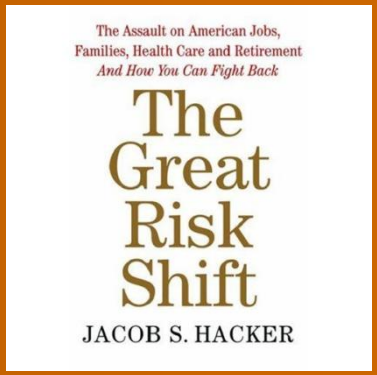
Solutions go on the scrap heap

New security vulnerabilities – more information collected than needed creates the ID fraud honey pot

INFORMATION INTEGRITY SOLUTIONS

The Trust Deficit; the great risk shift: Cloud as next instalment?

- We've been doing it for decades
  - A significant contributor to the Global Financial Crisis
  - The life blood of many online service models
  - Separates risk taker from risk bearer
- Will Cloud to add to this risk, asking end user to discover which company did what; which jurisdiction …
- THE common thread to all discussions
- Self regulate or wait to have it imposed?



INFORMATION INTEGRITY SOLUTIONS

Survey after survey shows the impact

- Research into Community attitudes towards Privacy in Australia 2007, 2004 & 2001, OPC Australia
- "Poll: Americans fear ID theft but try to protect themselves", CNN Money, 18 July 2005
- *Attitudes and Behaviors of Online Consumers: A Study of Five Cities* (Sydney, Singapore, Bangalore, Seoul, New York), NUS, 2003-04
- *The New e-Government Equation: Ease, Engagement, Privacy and Protection*, Hart-Teeter Research in US, 2003
- *Privacy and data-sharing: The way forward for public services*, UK Cabinet Office, 2002
- TRUSTe-TNS 2008 Study: Consumer Attitudes about Behavioral Targeting

What can we do about it?

www.trustguide.org.uk

Trustguide: Final Report

October 2006

Hazel Lacohée
BT Group Chief Technology Office, Research & Venturing
hazel.v.lacohee@bt.com

Stephen Crane
HP Labs
stephen.crane@hp.com

Andy Phippen
University of Plymouth, Network Research Group
andy@jack.see.plymouth.ac.uk

sciencewise

In association with
knowledge west http://www.knowledgewest.org.uk
www.network-research-group.org

Guidelines

TG.1: Education – Enabling better informed risk decision making

TG.2: Experimentation – learning through doing

TG.3: Restitution Measures – provide a positive impact on personal perceived risk

TG.4: Guarantees – Provide assurance and improve confidence in whether to enter into a transaction

TG.5: Control – Increased transparency brings increased confidence

TG.6: Openness – honesty signifies and engenders trust

www.trustguide.org.uk

INFORMATION INTEGRITY SOLUTIONS

Hence “Layered Defence”

Privacy ► Control ► Trust ► Risk ► Accountability

Education

Law

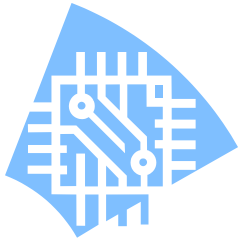
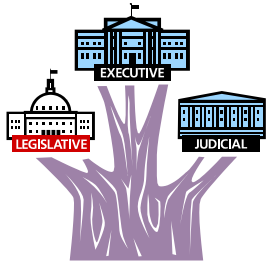
Technology

Governance

Safety Net

We can reduce the Trust Deficit



INFORMATION INTEGRITY SOLUTIONS

Layered Defence tools

Education on managing risks – citizen users and staff

Law – maybe more, where risks particularly high (eg specific use and disclosure limitations, criminal penalties, special measures to ensure review before critical changes made); NOT just compliance;

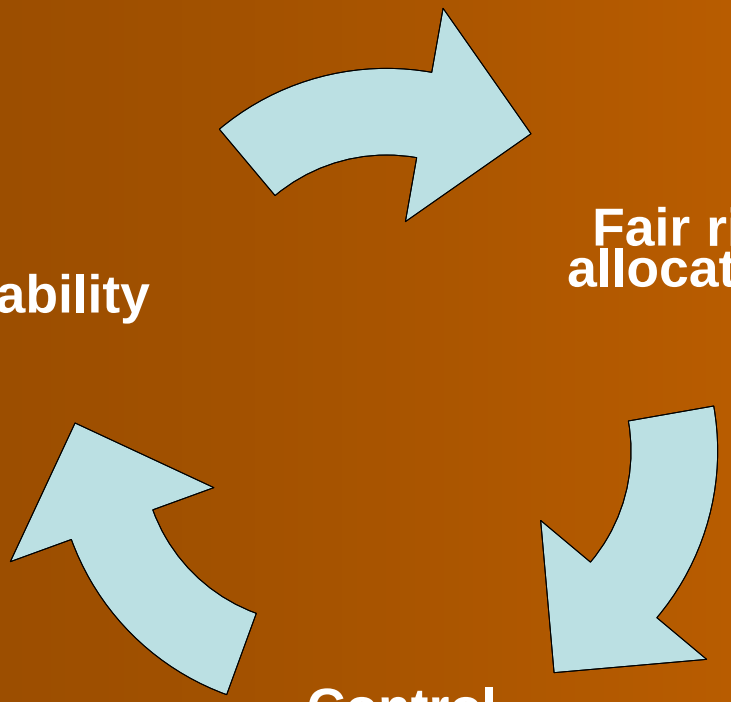
Technology – design limits information collected, what can be connected and who can see what;

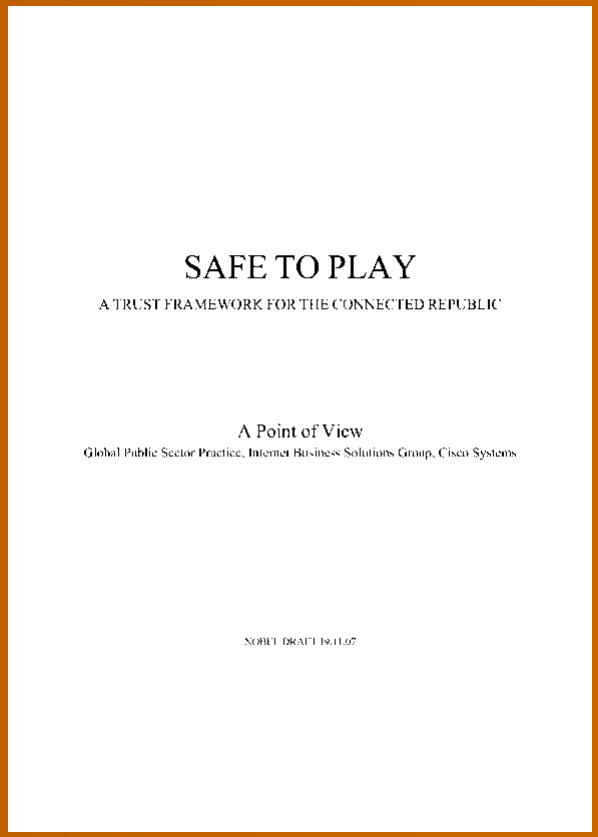
Governance – including transparency and accountability;

Safety mechanisms for citizens when failure or mistakes occur.

INFORMATION INTEGRITY SOLUTIONS

Three dynamically related elements the key




SAFE TO PLAY

A TRUST FRAMEWORK FOR THE CONNECTED REPUBLIC

A Point of View

Global Public Sector Practice, Internet Business Solutions Group, Cisco Systems

NOBET DRAFT 19.11.07

www.TheConnectedRepublic.org

Now www.iispartners.com/Publications/index.html

INFORMATION INTEGRITY SOLUTIONS

Culture & History also important

Why are many of the countries based on Anglo cultures so fussed about IDM?

Take Scandinavia

- Citizens appear more willing to trust government with their identity
- High levels of trust through history of openness – FOI & stronger accountability?

"Use Cases for Identity Management in E-Government"

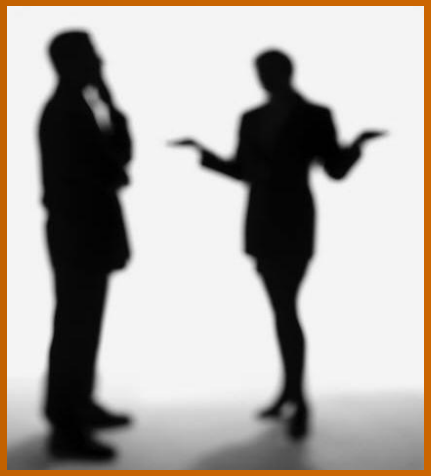
Robin McKenzie, Malcolm Crompton, Colin Wallis, *IEEE Security and Privacy*, vol. 6, no. 2, pp. 51-57, Mar/Apr, 2008

http://doi.ieeecomputersociety.org/10.1109/MSP.2008.51

Identity Management …

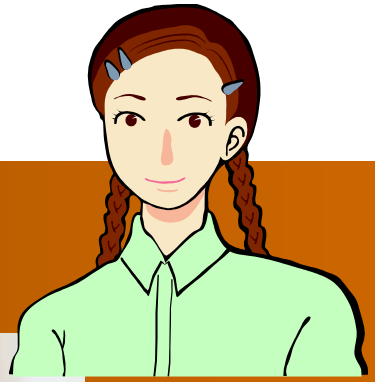
INFORMATION INTEGRITY SOLUTIONS

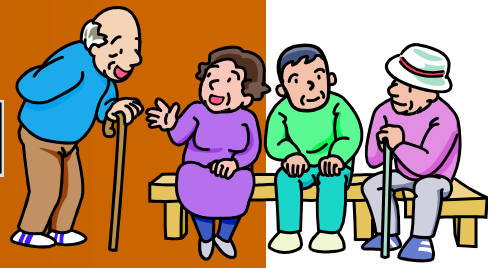
“Managing” “identity”: problem or solution?



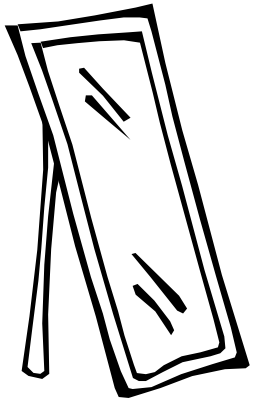
INFORMATION
INTEGRITY
SOLUTIONS

Identity?





... a very personal concept



INFORMATION INTEGRITY SOLUTIONS

“Managing” “identity”:
Whose risks are you managing?
What’s your concern?

- Identity fraud, identity theft, identity takeover?
- Border control?
- Traveller identification?
- The bottom line?

INFORMATION INTEGRITY SOLUTIONS

ID Mgt – Key Issues

- ID & the security check, especially online, is the first engagement with the customer
  - Is it a hand shake or a pat down in your organisation?
- What is in it for individuals?
  - How to handle customer data so that customers feel well treated not exploited?
- Recognise customers in control of further use of data (eg AML for CRM), not the institutions
- PPP!

INFORMATION INTEGRITY SOLUTIONS

Good ID management

Convergent thinking:

- ***The Identity Project: an assessment of the UK Identity Cards Bill & its implications***
  LSE, June 2005
  http://identityproject.lse.ac.uk/identityreport.pdf
- ***Microsoft Laws of Identity***
  Kim Cameron, May 2005
  http://msdn.microsoft.com/en-us/library/ms996456.aspx
- ***Proof of ID Required***
  Malcolm Crompton, March 2004
  www.privacy.gov.au/news/speeches/sp1_04p.pdf

INFORMATION INTEGRITY SOLUTIONS

Good ID management (cont)

Convergent thinking:

- ***Privacy & Identity Management for Europe (PRIME) & PrimeLife***
  www.prime-project.eu, www.primelife.eu
- ***The Higgins Trust Framework***
  Eclipse Foundation
  www.eclipse.org/higgins/
- ***The Identity Metasystem: Towards a Privacy-Compliant Solution to the Challenges of Digital Identity***
  Microsoft Corporation, Oct 2006
  www.identityblog.com/wp-content/resources/Identity_Metasystem_EU_Privacy.pdf

INFORMATION INTEGRITY SOLUTIONS

Good ID mgt: PITs *v* PETs

The most essential elements:

- Individuals control the use and disclosure of personal information about them unless specified in law
- Multiple authenticated electronic identities
- Registration empathetic and responsive
- Identity credentials revocable
- Identity numbers invisible outside the identity management system
- Competition between Operators and Technologies
- Consistent User Experience

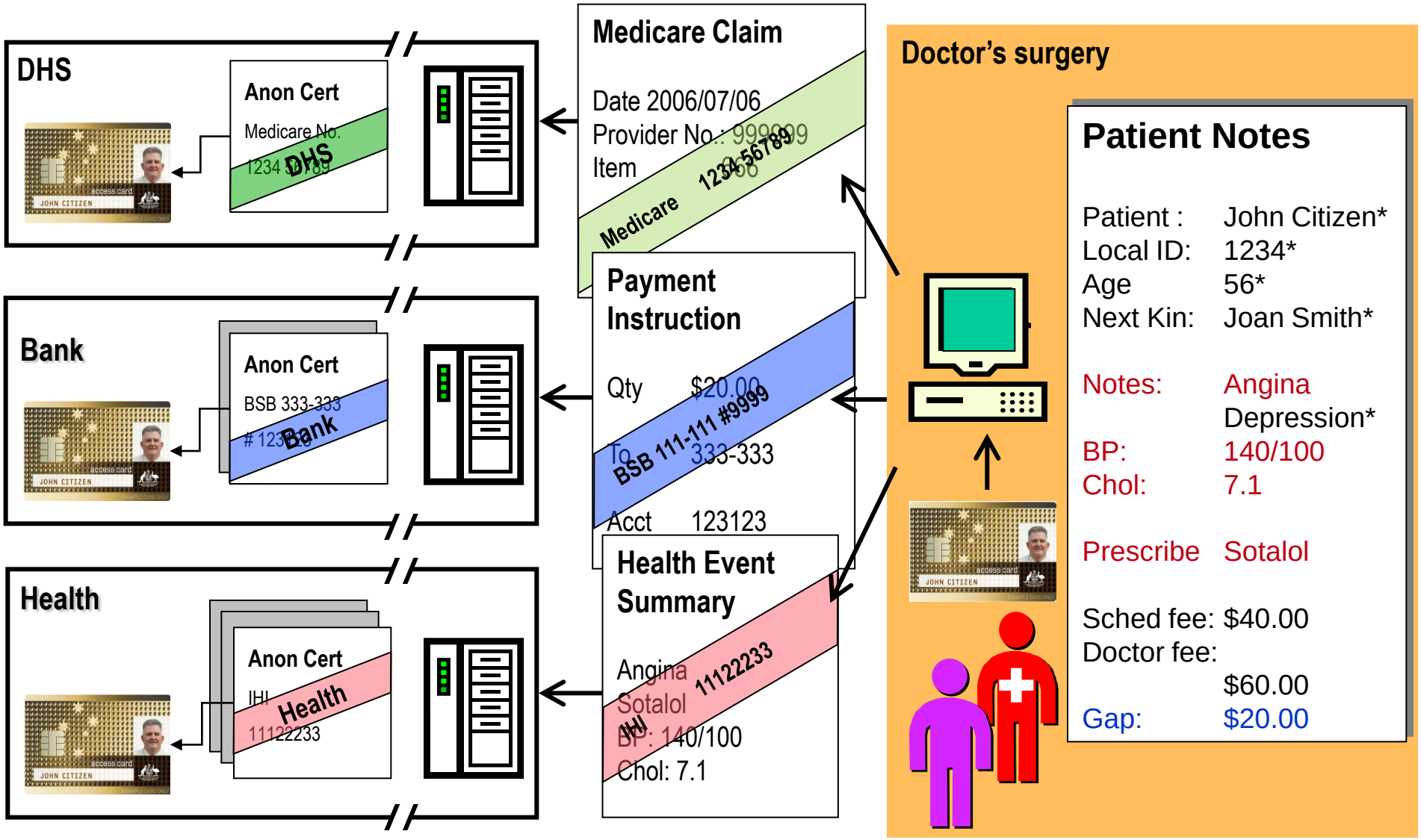
INFORMATION INTEGRITY SOLUTIONS

Privacy Enhancing Technologies (PETs) ?

Building in trust, permission & control …

- Iris recognition technology & application specific biometric templates
- Biometric encryption
- IBM – idemix : pseudonymity for e-transactions
- Credentica: purchased by Microsoft 2008
- Highly secure, privacy preserving Multi-app Smartcard technology emerging, eg Lockstep

Lockstep de-identification



INFORMATION INTEGRITY SOLUTIONS

Identity management – the future

User centric becoming mainstream

- Decentralisation in identity brokering – OpenID
- Identity selectors – Cardspace, Higgins
- Microsoft – Credentica purchase
- Cooperation and interoperability

User centric good stories emerging

Austria

New Zealand State Services Commission

Australian Government Online Services Portal

- User control
- Pseudonymous identity provider

INFORMATION INTEGRITY SOLUTIONS

Implications for global cooperation & research

- Is it ‘privacy’ or something else?
  - Redefining & measuring privacy?
- Current governance framework doesn’t work
  - What is the new paradigm?
- How to beyond the legal & conceptual divide between civil law (the State owns your identity) & common law (you do)?
  - Use advances in User Centric eID from EU FP6 & 7 + other advanced thinking to deliver a widely credible eID ‘on the ground’
    - Australia as a test bed for all Common Law...?
  - Move from there to a global ‘inter-op’?
    - Not just about technology; links to first 2 points

It’s all about TRUST

Is the ID management in your business up to it?

User Centric ID management: it’s coming

INFORMATION
INTEGRITY
SOLUTIONS

Malcolm Crompton
Managing Director

53 Balfour Street
Chippendale NSW 2008
Australia

+61 407 014 450

MCrompton@iispartners.com
www.iispartners.com