



THE UNIVERSITY OF
WESTERN AUSTRALIA



WAIMR Laboratory for Genetic Epidemiology



Western Australian Institute for Medical Research

THE TRUST DIMENSION

Malcolm Crompton

Proof of ID Required? Getting Identity Management Right

Genomics Directions: Bioethics & Beyond
Public Lecture

Perth
16 November 2004



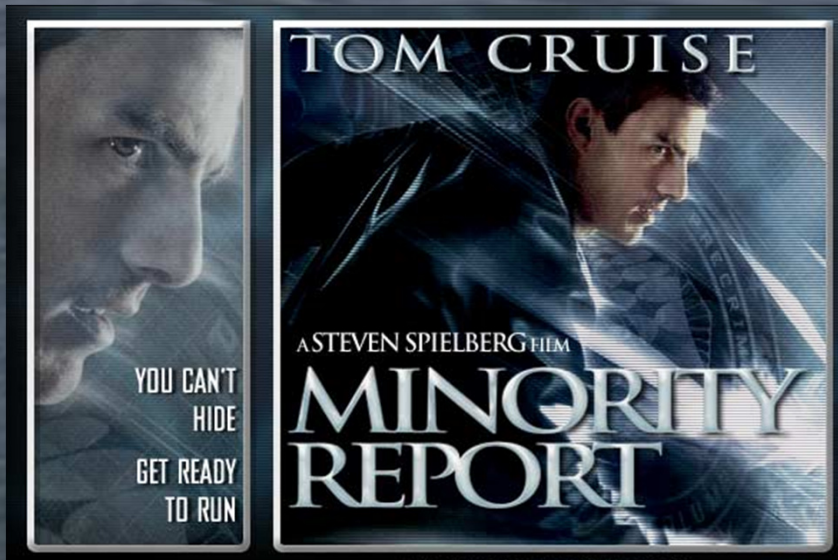
Privacy is about:

- context
- control
- freedom of choice
- identity integrity
- TRUST

ID management is also about trust & control

- Individuals don't know who they can trust with their information
- Organisations / governments want to know who they can trust
- Individuals have a right to have control over their identity and information

Is total ID management just science fiction?



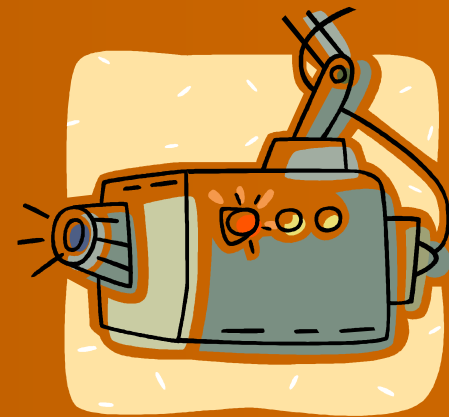
← Eye Scan

DNA Scan



Or possibly an emerging reality:

- Employee thumbprint system in bars/cafés (*SMH Radar*, 17 March 2004)
- US School cafeteria fingerprint
- Iceland DNA project
- Total Information Awareness (TIA) project



Identity management: the next big push for government and business

Response to:

- identity fraud
- identity theft or identity takeover
- border control and traveller identification
- individual convenience
- better customer service for individuals
- more and more complex IT networks



Commonwealth

- IMSC/CIOC/AWG: e-authentication
- Customs: SmartGate
- Customs: Advance Passenger Info
- DIMIA: Extend use of biometrics
- DFAT: biometric passport
- AEC&HIC: match Electoral Roll/Medicare
- Common POI framework
- AGD: Whole-of-Government ID Fraud process
- Centrelink: voice verification?

Private Sector

- NOIE: e-authentication

- Bankers: Fraud taskforce

- Macquarie Bank: info brochure

- PSMA: G-NAF

- DEST: CHESSN

- Cross-agency data matching

- Document verification service

- ACPR ID Crime Policing Strategy

- AFP: Identity Crime Task Force

- CrimTrac National DNA DB

- ACPR: ID Crime Working Party

- AUSTRAC: Cost of ID Fraud Report

- ACC: Identity Protection Registers (prev ID Fraud Register)

- Unique Health Identifier

- NEVDIS

- Baycorp

- FCS OnLine

- VIC: Victoria Online portal

State

- SA: ID theft amendments (awaiting assent)

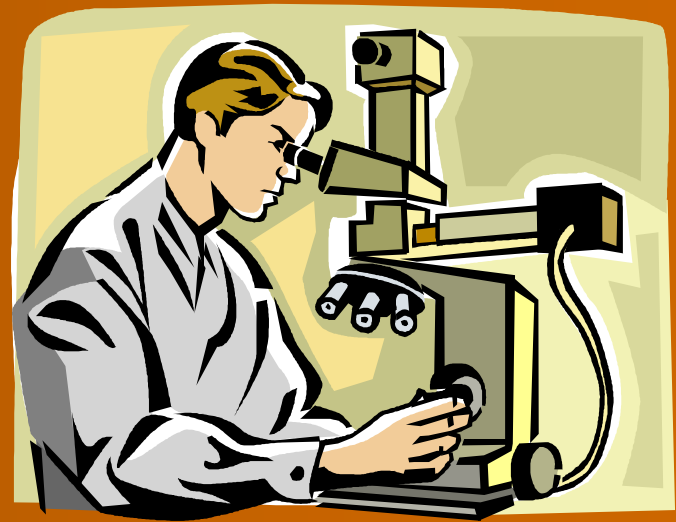
- ACT: Smartcard proposal (2000) ?

- QLD: Smartcard driver licence

Authentication and Identification initiatives In Australia

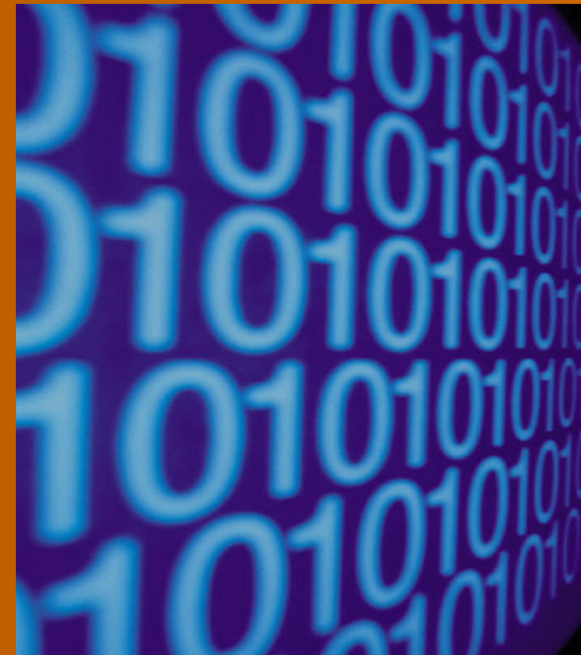
Recent “Red Herring” Solutions

- One number per person
 - Australia Card
- Some biometrics: same body = same person. Can that go wrong?
- Mass data matching projects abandoned after privacy criticism
 - (e.g. US: Total Information Awareness; MATRIX;
Canada: cradle to grave database proposal)



One number per person leads to total surveillance

- Same person with the same number, easy to “zip together” personal information
- Do we want info from banks, libraries, video shops, and takeaway food outlets zipped together with government identifiers?
- If it can be zipped together, it will be – eventually



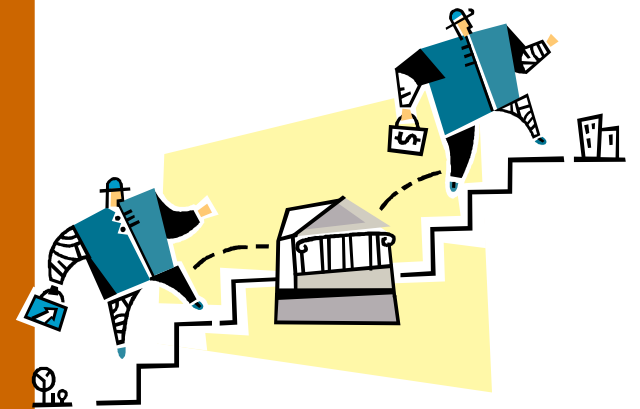
Major Privacy Problems



- Fort Knox Problems
- Identity theft is a self-defeating consequence of increased identification
- People may change behaviour
(to avoid situations that might be misunderstood by watchers, e.g. talking to people with strong political views, or of certain ethnic backgrounds)
- No EOI documents means no engagement in society – EOI documents become the condition of citizenry

Success feels like:

- Individuals feel trusted by the government agencies and organisations they deal with
- Agencies and organisations trust the individuals they deal with
- Individuals have control over who knows about them, and how much they know
- Just the right amount of personal information is handled:
 - only the minimum necessary to authenticate identity, complete the transaction



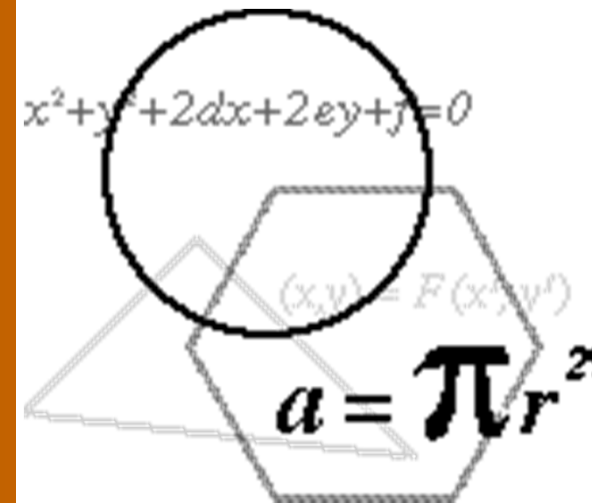
BUT HOW ? A MULTI-LAYERED APPROACH

- Create trust – open, vigorous debate
- There are good ID management solutions
 - use them
- Use technology that can identify people without creating a ‘honey pot’ for all the information about a person
- Extra ‘costs’ are the key
 - Never forget economics



Law + Technology + Market + Transparency + Accountability

- Law = promise; enforcement
- Technology = delivers promise
- Market = public debate; people don't buy; nobody makes
- T+A = proof of promise kept
= governance, audit, complaints
- Combined = something like the previous balance achieved from 'practical obscurity'



Good ID management: PITs v PETs

- Multiple identities allowed
- Only authenticate when necessary & what's necessary
 - is it ID which really needs to be authenticated or something else?
- Individuals retain control
- Unique identifiers specific to application
- Identifiers carry no other information
- Data Silos
- De-identification




Biometrics too good to be true?

- Too much or irrelevant information?
 - DNA can carry information about ethnic origin, health, family etc
 - Speech recognition may carry information about accent or cultural background
- Link between a person and the biometric may be unbreakable, even when it needs to be?
- If the system is hacked will the identifier be compromised?
- Reconstruction, or 'reverse engineering' from biometric identifier?
 - (e.g. picture of fingerprint may allow construction of forged fingerprint)



Privacy Enhancing Technologies (PETs) ?

Building in trust, permission & control ...

- Iris recognition technology & application specific biometric templates
- 'Drug records in blink of an eye', *AFR*, 9 Mar 2004
- Biometric encryption
- IBM – **idemix**  : pseudonymity for e-transactions
- P3P; EPAL; Distributed Identity; Combinations;
PRIME

The Big Picture

Strong push for identity management

Get it wrong – society significantly worse off

Get it right – trust & control

The debate must start now, before it's too late

Privacy – a fundamental human right

www.privacy.gov.au/news/speeches/sp1_04p.pdf



THE TRUST DIMENSION

Malcolm Crompton

+61 407 014 450

mcrompton@trustdimension.com