PARLIAMENT *of* AUSTRALIA
PARLIAMENTARY LIBRARY

INFORMATION, ANALYSIS
AND ADVICE FOR THE PARLIAMENT

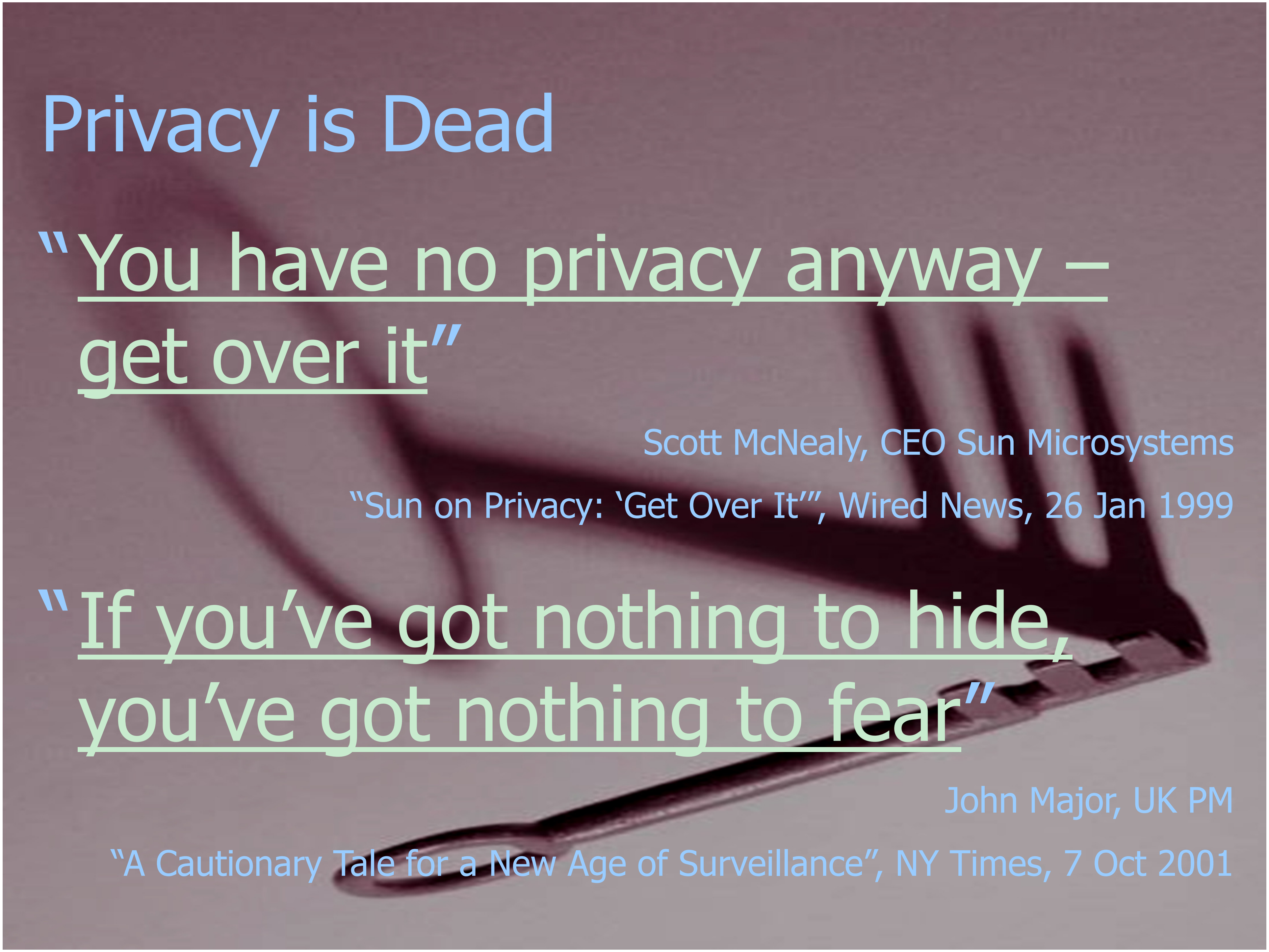
THE TRUST DIMENSION

Malcolm Crompton

Proof of Identity Required? Getting Identity Management Right

A seminar in the Vital Issues Program
for the Parliamentary Library, Parliament of Australia

Canberra
4 August 2004



Privacy is Dead

"You have no privacy anyway – get over it"

Scott McNealy, CEO Sun Microsystems

"Sun on Privacy: 'Get Over It'", Wired News, 26 Jan 1999

"If you've got nothing to hide, you've got nothing to fear"

John Major, UK PM

"A Cautionary Tale for a New Age of Surveillance", NY Times, 7 Oct 2001

The concept of Privacy

‘the right to be let alone’

1888, Judge Cooley

- Without privacy, every decision is observed, and in a sense forced by the public gaze, not the moral code of the individual.

THE TRUST DIMENSION

“A man without privacy is a man without dignity; the fear that Big Brother is watching and listening threatens the freedom of the individual no less than the prison bars”

Professor Zelman Cowen, 1969
“The Private Man”, ABC Boyer Lectures

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

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

Some very recent recent initiatives

"Once we have the health card in place, we can add Medicare details, tax file number, driver's licence and police data … all aspects of social security …"

"Advance Australia Card"
The Bulletin, 1 June 2004

"Initially, the card, containing an electronic chip, … will only be used to store emergency contact details. … The extent of the information to be stored is yet to be determined."

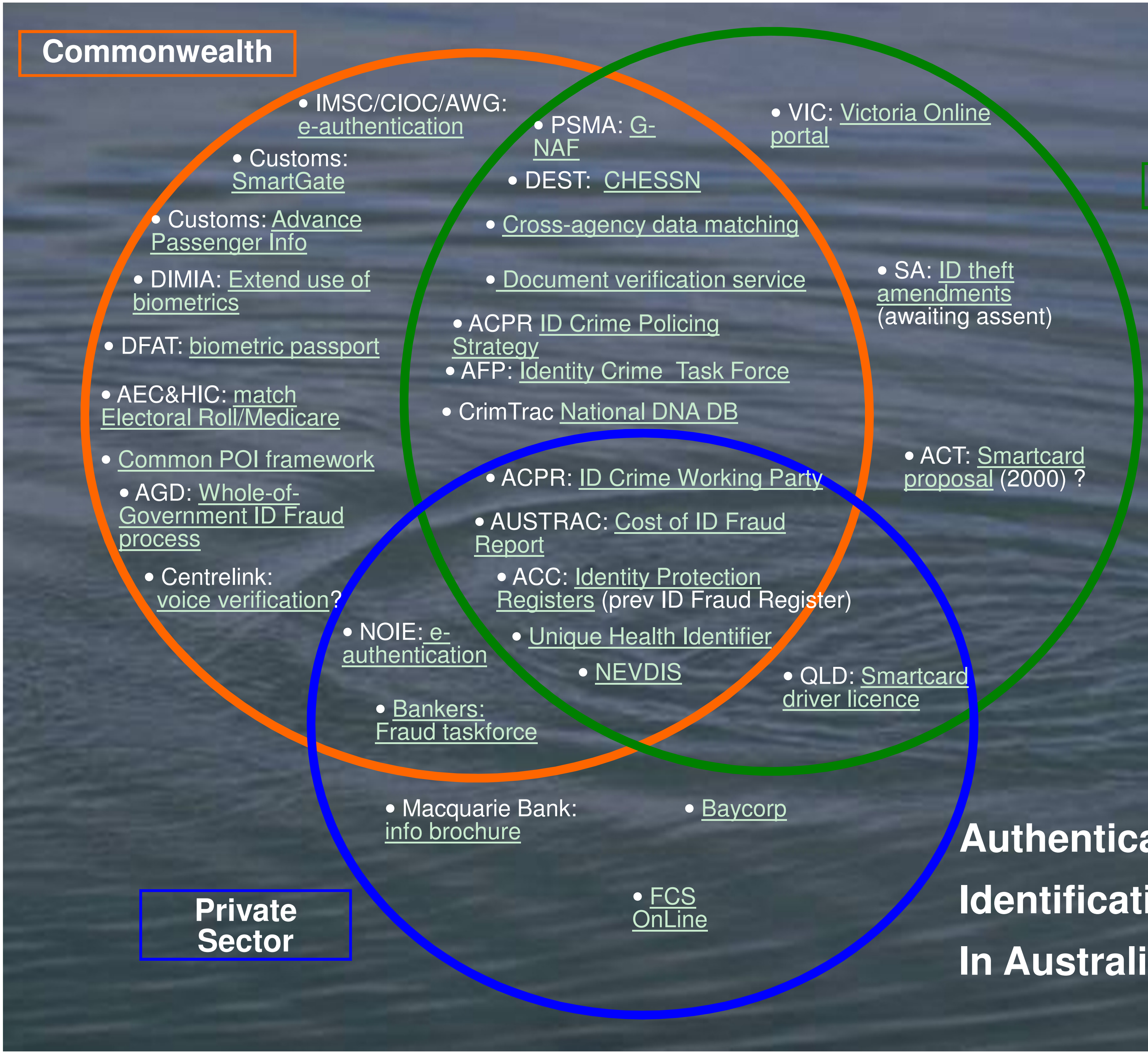
"Main parties rush to back Medicare smartcard"
AFR, 25 June 2004

"Imagine a world where the government knows how and where you travel, what your spending habits are, your medical history and your daily habits. … Then imagine all this information and more can also be accessed by corrupt officials."

"The longer term fear of this is that it will gradually shift the relationship between the government and the people," Prof Malbon warned.

"Smart card 'threatens privacy'" [re Queensland Driver's Licence Smartcard]
The Age, 10 July 2004

Authentication and Identification initiatives In Australia



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?

- 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

State

- VIC: Victoria Online portal
- SA: ID theft amendments (awaiting assent)
- ACT: Smartcard proposal (2000) ?

- ACPR: ID Crime Working Party
- AUSTRAC: Cost of ID Fraud Report
- ACC: Identity Protection Registers (prev ID Fraud Register)
- Unique Health Identifier
- NEVDIS

- NOIE: e-authentication
- Bankers: Fraud taskforce

- QLD: Smartcard driver licence

Private Sector

- Macquarie Bank: info brochure
- Baycorp
- FCS OnLine

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**

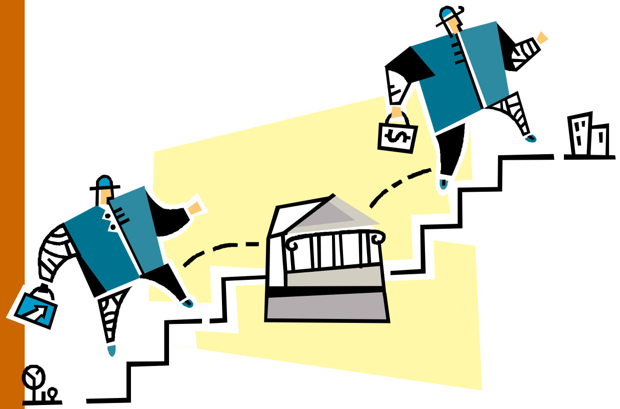
Major Privacy Problems

- 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



GETTING ID MANAGEMENT RIGHT A MULTI-LAYERED APPROACH

We must have this debate now

- 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 worth it in the long run
- Good ID management will
  - Build trust between individuals government & business
  - Increase individual control over own identity

THE TRUST DIMENSION

Law + Technology + Market + Transparency + Accountability

- Law = promise; enforcement
- Technology = delivers promise
- Market = people don’t buy; nobody makes
- T+A = proof of promise kept
- Combined = total cost too high, except in extremes (High Court; or worth a massive tech attack; or ...)

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

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