

# YOU ARE WHERE YOU'VE BEEN

## Location Technologies' Deep Privacy Impact

**Roger Clarke**

Xamax Consultancy, Canberra

**Visiting Professor – Cyberspace Law & Policy Centre @ UNSW**

and at ANU and the Uni. of Hong Kong  
Chair, Australian Privacy Foundation

<http://www.anu.edu.au/Roger.Clarke/....>  
..../DV/YAWYB {.html,.ppt}

Location Privacy Seminar – UNSW – 23 July 2008

Copyright  
1988-2008



# Prologue – 30 Anonymous Days in Spain

# Prologue – 30 Anonymous Days in Spain

- Air-Travel by identified credit-card tx, and Passport presentation at every border-crossing (2)
- Car-Hire by identified credit-card tx and passport
- Passport at every Casa Rurale and Hotel (14)
- Major Purchases (accomm., petrol, sustenance) by identified credit-card or debit-card tx (28)
- Cash Withdrawals by identified debit-card tx (1)
- AP (Autovia Peage) (20)
- Mobile phone (continuous)

# You Are Where You've Been

## AGENDA

- **Intellectual and Analytical Tools**
  - Location and Tracking
  - Identity, Entity and Nymity
  - Privacy and Dataveillance
- **Location and Tracking Technologies**
  - Handhelds
  - Motor Vehicles
  - Human Bodies
- **Threats**
- **Controls**

# Concepts of Location and Tracking

- **Location** – knowing the whereabouts of something, in relation to known reference points

# Concepts of Location and Tracking

- **Location** – knowing the whereabouts of something, in relation to known reference points

Physical Space, Network Space, Intellectual Space, ...

# Concepts of Location and Tracking

- **Location** – knowing the whereabouts of something, in relation to known reference points

Physical Space, Network Space, Intellectual Space, ...

Precision, Accuracy, Reliability, Timeliness, ...

# Concepts of Location and Tracking

- **Location** – knowing the whereabouts of something, in relation to known reference points

Physical Space, Network Space, Intellectual Space, ...

Precision, Accuracy, Reliability, Timeliness, ...

- **Tracking** – knowing the sequence of locations of something over a period of time

# Concepts of Location and Tracking

- **Location** – knowing the whereabouts of something, in relation to known reference points

Physical Space, Network Space, Intellectual Space, ...

Precision, Accuracy, Reliability, Timeliness, ...

- **Tracking** – knowing the sequence of locations of something over a period of time
  - **Real-Time-Tracking**

# Concepts of Location and Tracking

- **Location** – knowing the whereabouts of something, in relation to known reference points

Physical Space, Network Space, Intellectual Space, ...

Precision, Accuracy, Reliability, Timeliness, ...

- **Tracking** – knowing the sequence of locations of something over a period of time
  - **Real-Time-Tracking**
    - **Retrospective Tracking**

# Concepts of Location and Tracking

- **Location** – knowing the whereabouts of something, in relation to known reference points

Physical Space, Network Space, Intellectual Space, ...

Precision, Accuracy, Reliability, Timeliness, ...

- **Tracking** – knowing the sequence of locations of something over a period of time
  - **Real-Time-Tracking**
    - **Retrospective Tracking**
    - **Predictive Tracking**

# Concepts of Location and Tracking

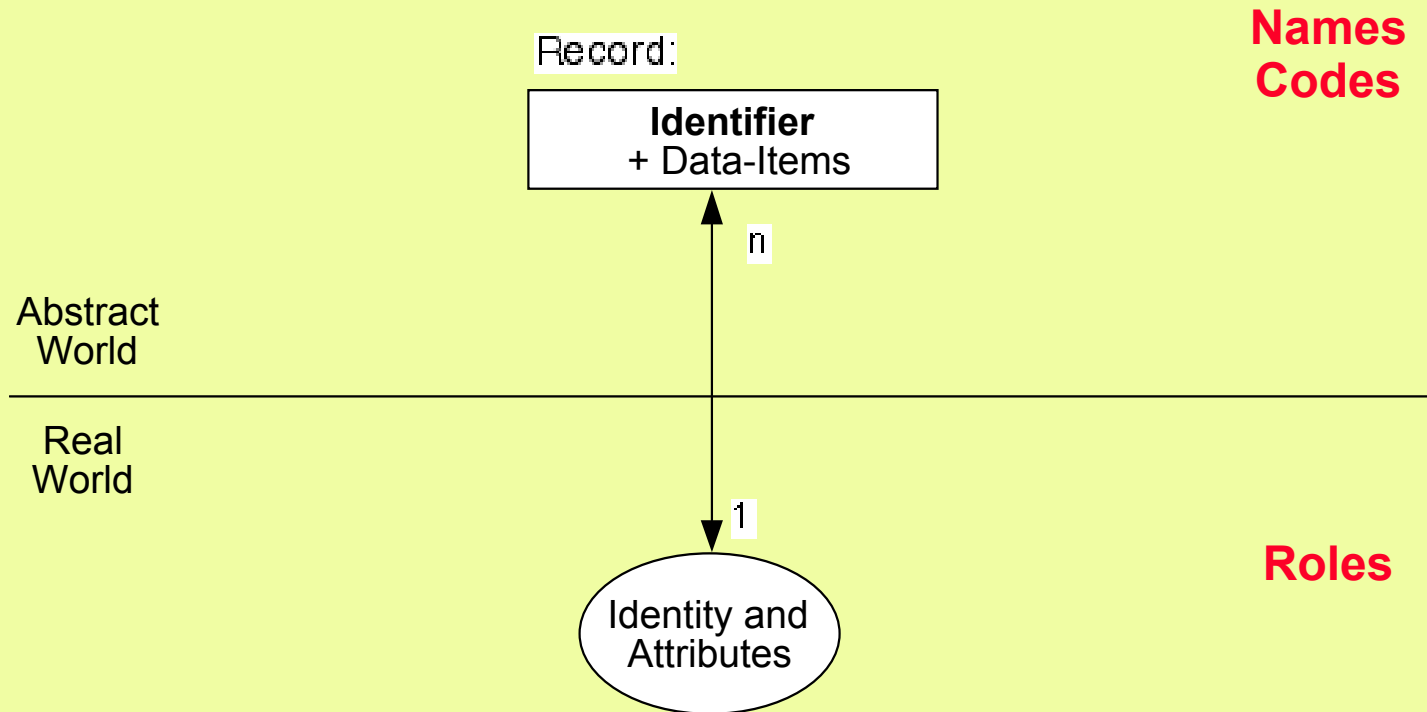
- **Location** – knowing the whereabouts of something, in relation to known reference points

Physical Space, Network Space, Intellectual Space, ...

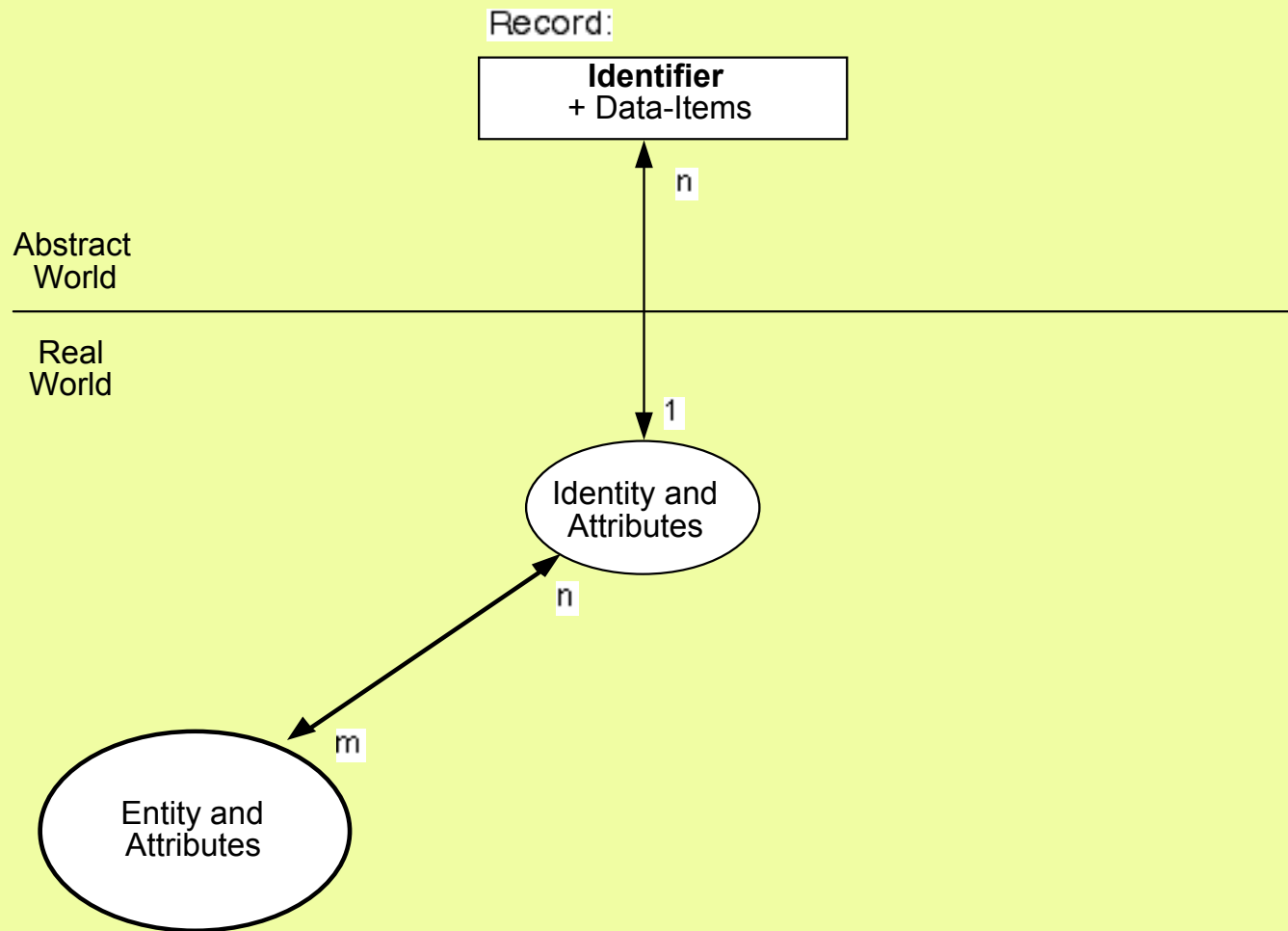
Precision, Accuracy, Reliability, Timeliness, ...

- **Tracking** – knowing the sequence of locations of something over a period of time
  - **Real-Time-Tracking**
    - **Retrospective Tracking**
      - **Predictive Tracking**
        - **Associative Tracking**

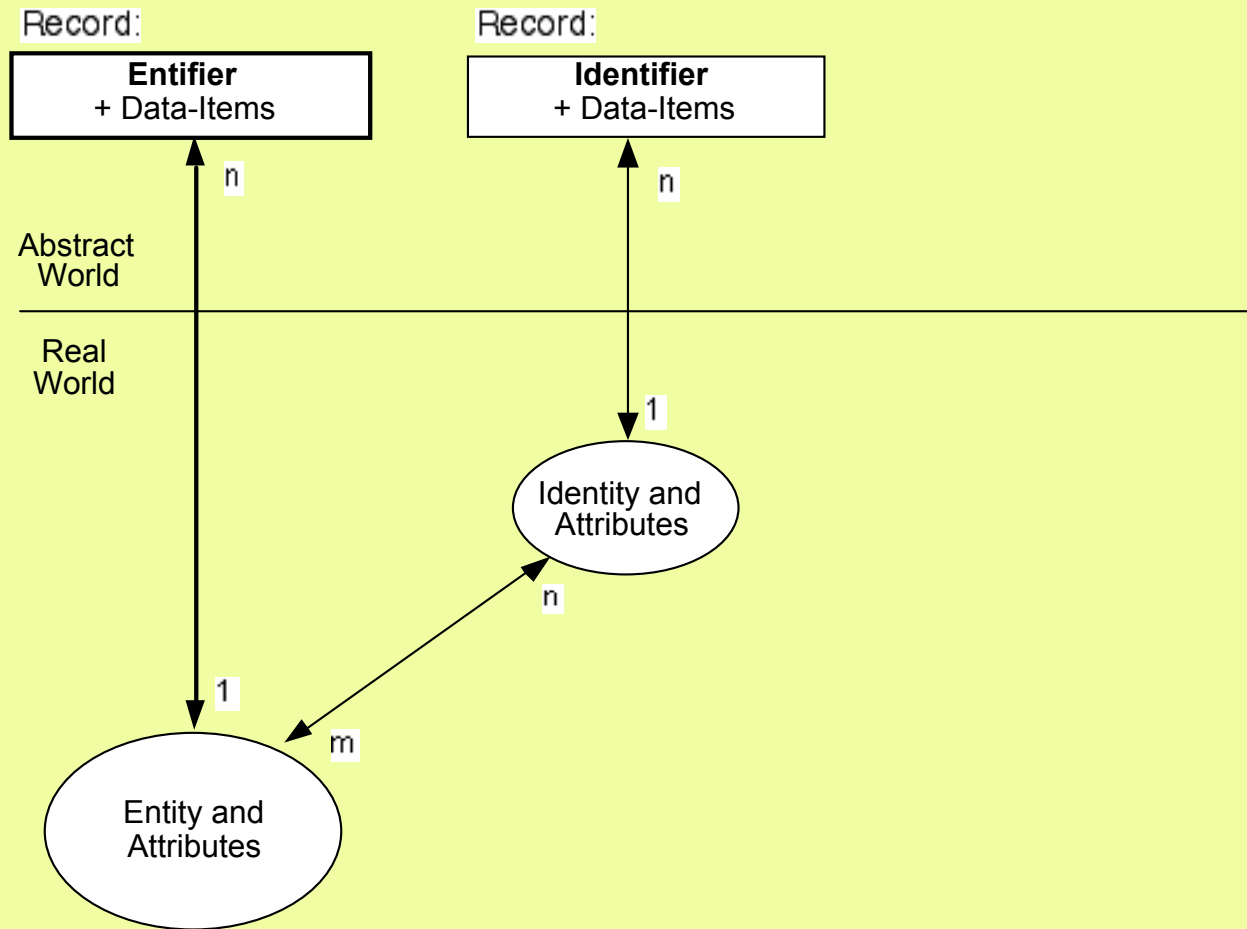
# Identity and Identifier



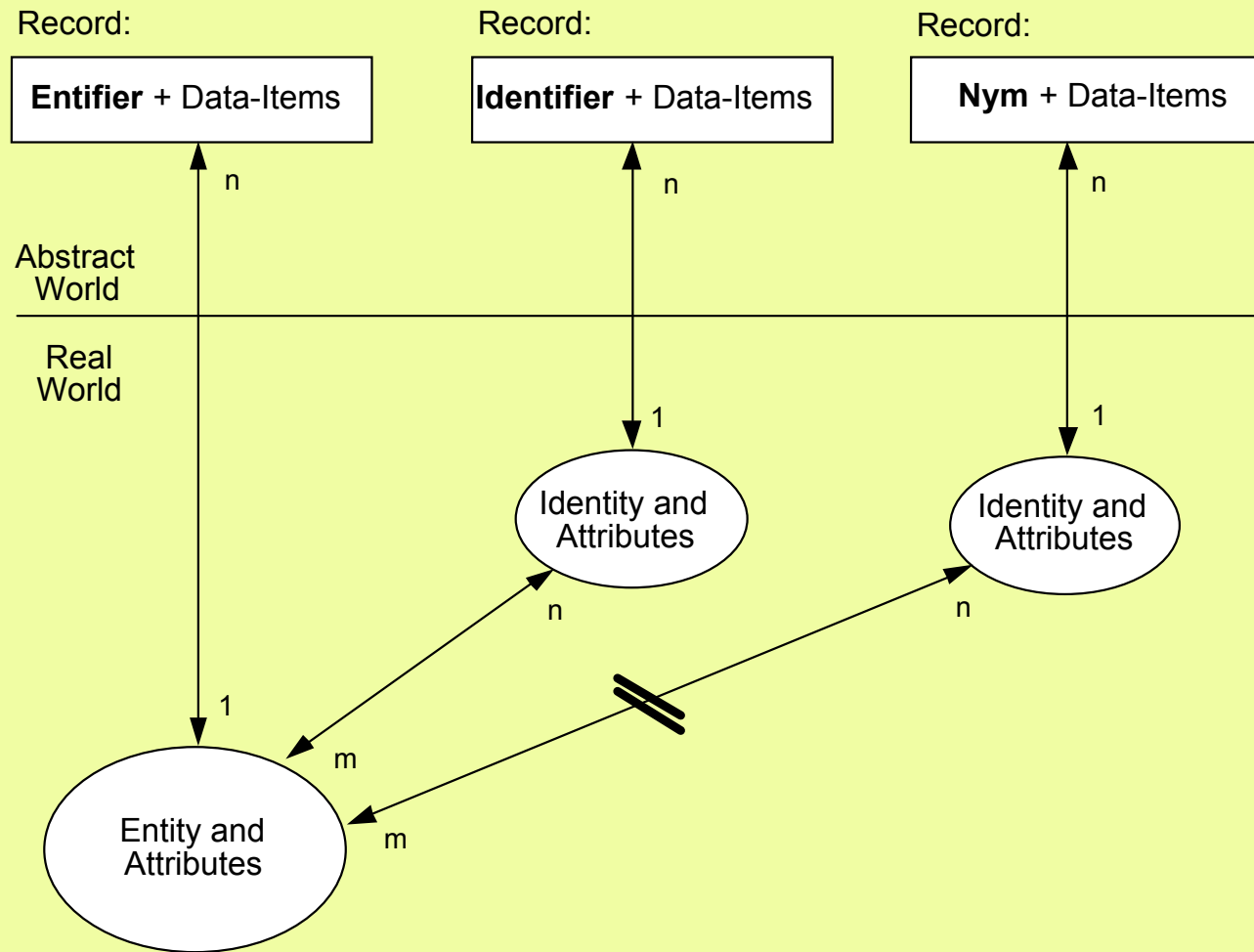
# The Entity/ies underlying an Identity



# Entity and Entifier



# Nymity



# Privacy

The interest that individuals have  
in sustaining a 'personal space',  
free from interference  
by other people and organisations

# Privacy

The interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations

## Dimensions of Privacy

- The Physical Person
- Personal Behaviour
- Personal Communications
- Personal Data

## Why is Privacy ?

- Physical Needs
- Psychological Needs
- Social / Sociological Needs
- Economic Needs
- Political Needs
- The Philosophical Level

## Why is Privacy ?

- Physical Needs
- Psychological Needs
- Social / Sociological Needs
- Economic Needs
- Political Needs
- The Philosophical Level

Highly Person-Dependent – Highly Context-Dependent

# Privacy Protection

- Privacy often conflicts with other interests:
  - other interests of the same person
  - interests of another person
  - interests of a group or community
  - interests of an organisation
  - interests of society as a whole

# Privacy Protection

- Privacy often conflicts with other interests:
  - other interests of the same person
  - interests of another person
  - interests of a group or community
  - interests of an organisation
  - interests of society as a whole
- Privacy Protection is a process of finding appropriate balances between privacy and multiple competing interests

# Vehicles for Privacy Protection

- Categories of Measures:
  - Legal
  - Organisational
  - Technical

# Vehicles for Privacy Protection

- Categories of Measures:
  - Legal
  - Organisational
  - Technical
- Secrecy
- Data Silo'ing
- Identity Silo'ing
- Nymity

# The Vacuousness of Data Protection Laws

- FIPs ('Fair Information Practices') were designed for 'administrative convenience'
- OECD Guidelines were designed to protect businesses from inconsistent national laws
- Exceptions, Exemptions, Loop-Holes
- Over-Rides and Small-Print Authorisations
- 1980 Provisions for 1970s Computing
- A Privacy Commissioner whose duty is to protect government and business, not privacy

# Vignettes of Location and Tracking Technologies

## V1 Handhelds

- Computers
- Phones

## V2 Motor Vehicles (specifically ANPR)

## V3 Human Bodies

- Tightly-Associated RFID Tags
- Embedded Chips

# V1 Handhelds

- **Personal Digital Assistants (PDAs)**  
for computing on the move – for business or personal use, and for text, sound, image and/or video
  - Wifi/IEEE 802.11x / WiMax/802.16x / iBurst
- **Mobile Phones**  
for voice-calls from any location within range of a transceiver connected to the relevant wireless network
  - Analogue
  - Early Digital, e.g. GSM, CDMA
  - ‘Third Generation’/3G Digital  
e.g. GSM/GPRS, CDMA2000, UMTS/HSPA

## Location and Tracking of PDAs

- The primary identifier is generally the IP-Address, which is commonly assigned short-term
- The 'router' may also have access to a device identifier, such as a processor-id or NIC Id
- Device identifiers are not tightly linked with the individuals who use each device
- But Multi-Functional Handsets connect with not only Wifi networks but also cellular networks ...
- And Networks will converge over the next decade

# Location and Tracking of Mobiles

- **Inherent**

There is insufficient capacity to broadcast all traffic in all cells

The network needs to know the cell each mobile is in

Mobiles transmit registration messages to base-station(s)

They do so when nominally switched off or placed on standby

- **What is being tracked:**

- The SIM-card, an identifier
- The mobile-phone id, an identifier
- The SIM-card and/or mobile-phone may be registered to a human identity (and may be required by law to be so)
- **The vast majority of handsets are used for long periods with a single SIM-card installed, and by a single**

**person**

# The Practicability of Location and Tracking

- **Location** is intrinsic to network operation (✓)
- **Tracking** is feasible, because the handset sends a stream of messages (✓)
- **Real-Time Tracking** is feasible if the data-stream is intense and latency is low (✓)
- **Retrospective Tracking** is feasible if the series of locations is logged (✓), and the log is retained (✓)
- **Predictive Tracking** is feasible if the data-stream is intense and latency is low (✓)
- **Associative Tracking** is feasible if data-streams are intense and precision is high (✓)

# The Precision of Handset Location

- **Intrinsically, the Cell-Size:**
  - 1km-10km radius for Mobile non-CBD
  - 100m radius for Wifi & CBD Mobile
- **Potentially much more fine-grained:**
  - Directional Analysis
  - Differential Signal Analysis
  - Triangulation
  - Self-Reporting of GPS coordinates

# The Accuracy and Reliability of Handset Location

- **Directional Analysis**  
The Case of the Cabramatta Murder Conviction
- **Differential Signal Analysis**  
A Wide Array of Error-Factors
- **Triangulation**  
Multiple Transceivers  
Multiple Error-Factors
- **Self-Reporting of GPS coordinates**  
Highly situation-dependent, and unknown  
Dependent on US largesse, 'operational requirements'

# The Case of the Cabramatta Murder Conviction

- In 1994, a NSW MP, John Newman, was murdered
- In 2001, Phuong Ngo was convicted, sentenced to life in prison, 'never to be released', and is 'in solitary' in a maximum-security prison
- In July 2008, after further pressure (from an ANU law academic and Four Corners), the NSW Chief Justice commissioned a formal review

# The Case of the Cabramatta Murder Conviction

- In 1994, a NSW MP, John Newman, was murdered
- In 2001, Phuong Ngo was convicted, sentenced to life in prison, 'never to be released', and is 'in solitary' in a maximum-security prison
- In July 2008, after further pressure (from an ANU law academic and Four Corners), the NSW Chief Justice commissioned a formal review
- The conviction depended heavily on mobile-phone location evidence
- This made assumptions about the precision of directional analysis
- The evidence went unchallenged
- It appears to have been materially misleading

# Location and Tracking Technologies

## V2 Motor Vehicles

- Vehicles can be monitored in various ways, e.g.
  - Manual Inspection of VINs, registration plates
  - Passive RFID-tags passing control-points
  - On-Board Transmitters, with self-reporting of GPS-based or other coordinates
- **Vehicle Registration Data** can be monitored:
  - Cameras were wet chemistry, are now digital
  - Extraction was manual, is now automated

# Automated Number Plate Recognition (ANPR)



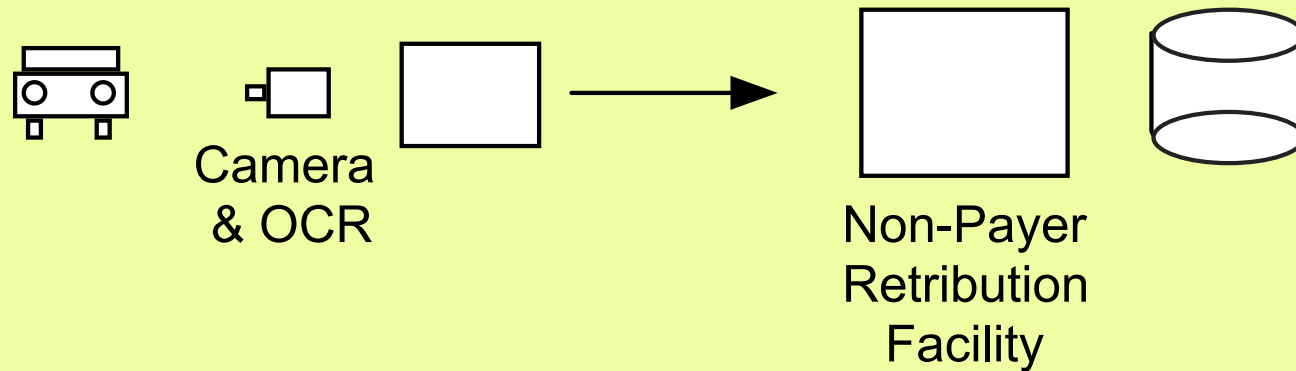
# Automated Number Plate Recognition (ANPR)

- **A Digital Camera**  
Captures an image of a motor vehicle's 'number' plate
- **Software**  
Extracts the registration data (numbers, letters, perhaps other data such as colour and jurisdiction identifiers)
- **(Maybe) List(s) of Numbers Being Sought**  
So that the extracted data can be compared with it
- **Transmission Facilities**  
Send the extracted data and perhaps other data elsewhere

# ANPR for (1) User-Pays Charging

- Transport infrastructure can be paid for centrally, or by the users of the resources
- It's attractive to extract revenue for:
  - on-street parking
  - use of space in garages and parking stations
  - use of toll-roads
  - use of congested areas such as inner-cities
- Reliable and inexpensive payment is needed
- Controls are needed over non-payers

# User-Pays Control Mechanism



# Privacy Threats in User-Pays Road Transport

- Denial of Anonymous Travel (no cash booths, no or inconvenient non-identified payment)
- Error
- Re the Registration Data:
  - Indiscriminate Collection (i.e. all vehicles not just non-payers)
  - Retention not Early Destruction
  - Availability for Exploitation
  - Availability for Disclosure

# Privacy-Sensitive Architectures are Feasible

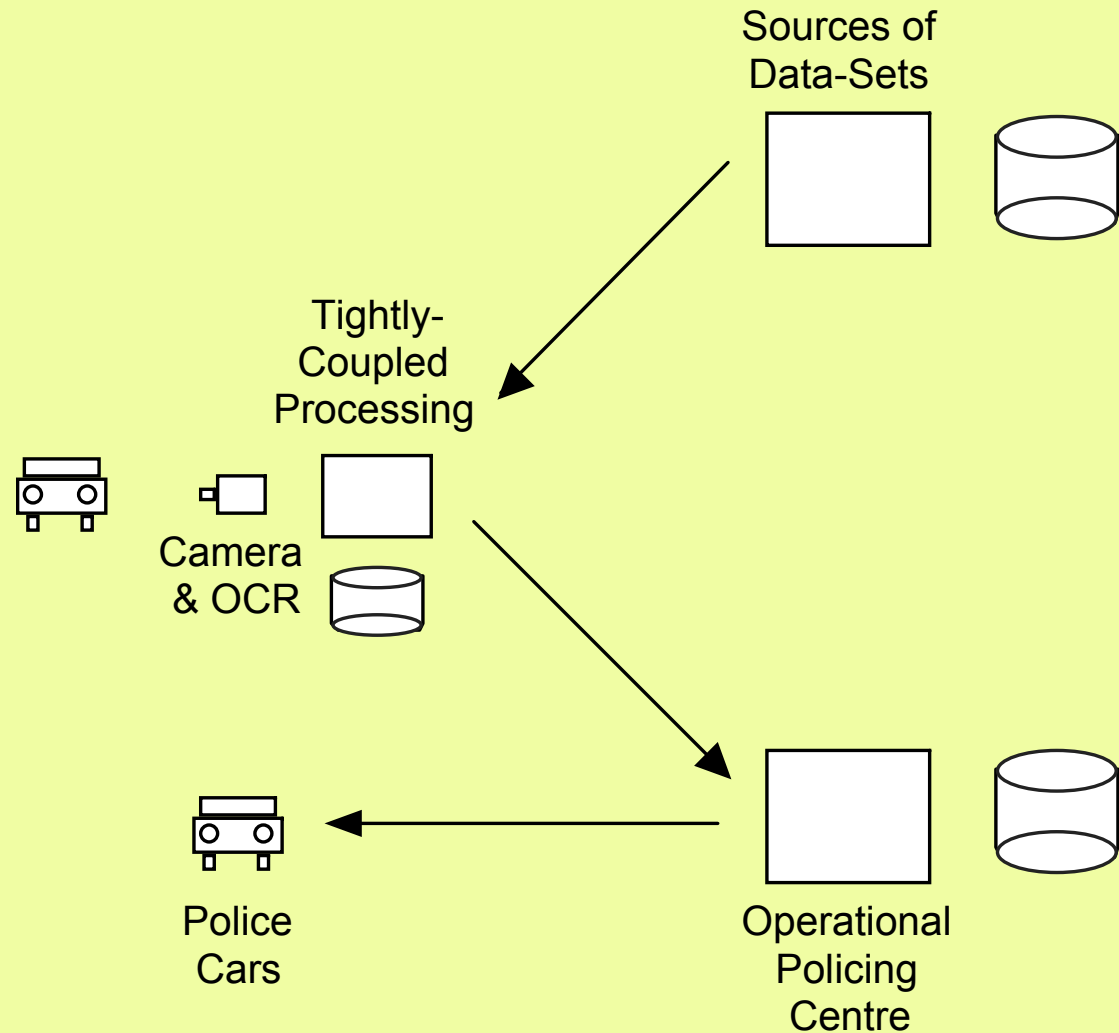
- A simple example:
  - Vehicle Registration Data could be retained for the duration of the trip only
  - The payment tag could be issued, electronically, with a Receipt Number
  - The operator could store the facility usage data that gave rise to the charge in combination with the Receipt Number, not the Registration Data

**But Privacy-Sensitive Architectures  
are not implemented**

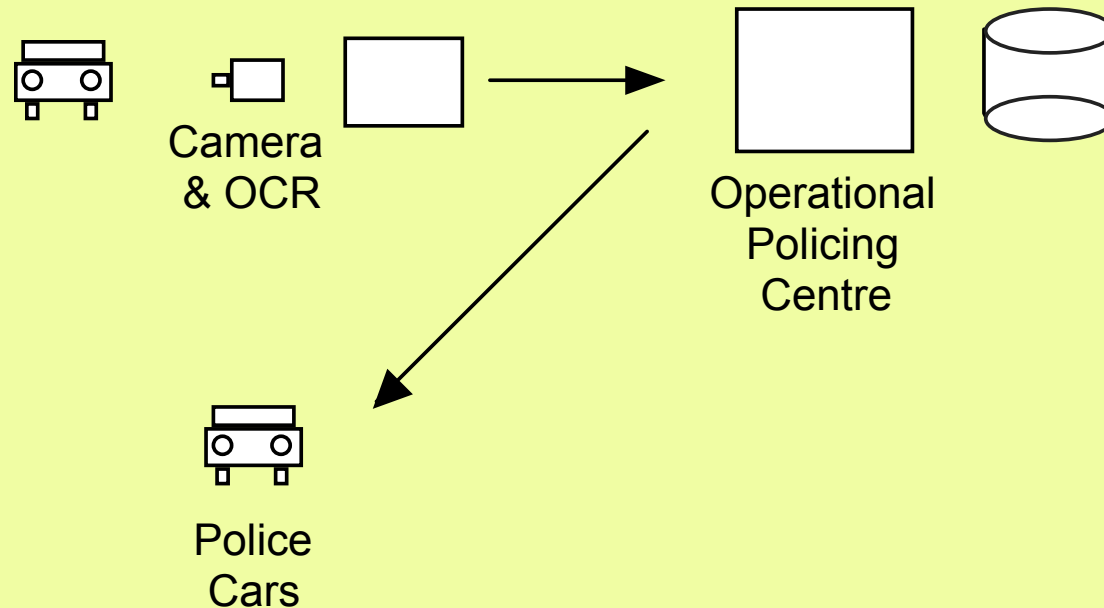
## ANPR for (2) Law Enforcement

- √ **Traffic Administration.** Detection and interception of Unregistered Vehicles, and of Vehicles owned by people whose driving licences are currently suspended
- √ **Traffic Law Enforcement.** Detection and prosecution of Offences, e.g.
  - √ running red lights
  - √ driving at a point-in-time speed in exceed of the speed limit
  - ? driving at an average speed in excess of the speed limit
- ? **Public Safety.** Deterrence of unsafe practices (e.g. speeding, driving unregistered vehicles, driving unlicensed)
- ?? **Criminal Law Enforcement.** Detection and interception of vehicles reported stolen, or associated with 'wanted people'

# Appropriate 'Blacklist in Camera' Architecture



# ANPR for (3) Mass Surveillance



- Indiscriminate collection
- Long retention
- Data Mining to generate suspicions
- **All Australian Police Forces are adopting this approach, and are being aided and abetted by the Clth**

# ANPR Quality

- Alliances of purveyors and purchasers suggest that registration data extraction is accurate and reliable
- But:
  - Very little evidence is publicly available
  - There appear to have been no independent tests
  - Many factors reduce reliability, incl. the state of the registration plates, of the camera lens and of the light-path
  - The extraction is by its nature 'fuzzy', and confidence thresholds have to be set
- **Reliable extraction of the registration data may be as low as 70% even under favourable conditions**

# Location and Tracking Technologies

## V3 Human Bodies

- Location and Tracking requires a chip-set and an associated transceiver, antenna and power-source
- The most relevant technology/ies:
  - contactless smartcards
  - radio-frequency identification (RFID)
  - near field communications (NFC)
- Carriers – 'plastic cards', 'RFID tags', handsets
- Alternative Carrier 'Form-Factors':
  - **Adornments** – wrist-watches, brooches, belt-buckles, body-piercings (ear, nose, navel, tongue)
  - Tightly-Attached RFID Tags (**Wristlets, Anklets**)
  - **Embedded Chips** (hand, arm, tooth-enamel, gums, ...)

# Chips for Goods Monitoring



# Monitoring of Animal-Attached Chips



# Monitoring of Animal-Embedded Chips



Copyright  
1988-2008

**XAMAX**  
Consultancy  
Pty Ltd

# Continuous Monitoring of Chips

QuickTime™ and a  
TIFF (Uncompressed) decompressor  
are needed to see this picture.



# Categorising Surveillance

- |               |   |
|---------------|---|
| (1) Of What?  | Person, Object, Space   |
| (2) For Whom? | Person, Involved Party, Third Party   |
| (3) By Whom?  | Person, Involved Party, Third Party   |
| (4) Why?      | Wellbeing, Evidence, Deterrence   |
| (5) How?      | Physical (visual, aural, at distance, auto-surveillance)<br>Dataveillance (retrospective, real-time, predictive)<br>Communications / Experience<br>Personal / Mass Surveillance |
| (6) Where?    | Physical, Virtual, Intellectual   |
| (7) When?     | Once, Recurrent, Scattered, Continuous  |

# Voluntary? Consensual? Coerced? Imposed?

- **Voluntary**  
e.g. individuals who are concerned about being kidnapped
- **Consensual**  
e.g. genuinely optional use to locate people within a campus
- **Coerced**  
'an offer you couldn't refuse', e.g. a condition of a job or a promotion
- **Imposed**, e.g.
  - on employees by powerful employers such as the military
  - **on various categories of institutionalised individuals**
    - prisoners on parole
    - **prisoners within low-security facilities**
    - prisoners within conventional gaols
    - people on remand (charged, untried, may be a flight risk)
    - **the frail aged, especially those suffering senile dementia**
    - babies in neo-natal wards
    - unconscious patients during operational procedures

# Potential Impacts of Location and Tracking

- Chilling Effect on:
  - Terrorism
  - Crime
  - Sociopathic Behaviour
- Chilling Effect on:
  - 'Anti-Social Behaviour'
  - Creative Behaviour
  - Dissidence
  - Travel
  - Association
- Denial of:
  - Service
  - Travel
  - Identity

# Counterveillance Principles

1. Independent Evaluation of Technology
2. A Moratorium on Technology Deployments
3. Open Information Flows
4. Justification for Proposed Measures
5. Consultation and Participation
6. Evaluation
7. Design Principles
  1. Balance
  2. Independent Controls
  3. Nymity and Multiple Identity
8. Rollback

# You Are Where You've Been

## AGENDA

- **Intellectual and Analytical Tools**
  - Location and Tracking
  - Identity, Entity and Nymity
  - Privacy and Dataveillance
- **Location and Tracking Technologies**
  - Handhelds
  - Motor Vehicles
  - Human Bodies
- **Threats**
- **Controls**

# YOU ARE WHERE YOU'VE BEEN

## Location Technologies' Deep Privacy Impact

**Roger Clarke**

Xamax Consultancy, Canberra

**Visiting Professor – Cyberspace Law & Policy Centre @ UNSW**  
and at ANU and the Uni. of Hong Kong  
Chair, Australian Privacy Foundation

<http://www.anu.edu.au/Roger.Clarke/....>  
..../DV/YAWYB {.html,.ppt}

Location Privacy Seminar – UNSW – 23 July 2008

Copyright  
1988-2008

