Location and Tracking of Mobile Devices

Roger Clarke
Xamax Consultancy, Canberra
Visiting Professor in Cyberspace Law & Policy, UNSW, Sydney
Visiting Professor in Computer Science, ANU, Canberra
Research conducted with
Ass Prof Katina Michael, Uni of Wollongong

http://www.rogerclarke.com/DV/LTMD-1401 {.html, .pdf}

University of Southampton
27 January 2014

Location and Tracking of Mobile Devices Agenda

1. Mobile Technologies
   - Devices
   - Communications
2. Surveillance
3. Location Technologies
4. Privacy Impacts
5. Natural Controls
6. Regulatory Framework

Relevant Device Characteristics

- Conveniently Portable by a human
- Emits Signals that:
  - enable another device to compute the location of the device (and hence of the person)
  - are sufficiently distinctive that the device is reliably identifiable at least among those in the vicinity, and hence the device's (and hence the person's) successive locations can be detected, and combined into a trail

Mobile Devices

- **Nomadic / Untethered Portables - Clam Form-Factor**
- **Mobiles / Smartphones – Small One-Hand-Helds**
- **Larger Handhelds**
  PDAs, games machines, music-players, 'converged' / multi-function devices, ...
  Tablets esp. iPad but now many followers
- **Other 'Form Factors'**
  Credit-cards, RFID tags, Toll-Payment tags, Passports, ...
- **Wearable Computing Devices**
  Watches, finger-rings, spectacles, key-rings, glasses, necklaces, bracelets, anklets, body-piercings, chip implants

Wireless Comms

- **Wide Area Networks – Satellite** (Geosynch; Low-Orbit)
  GS is Large footprint, very high latency (c. 2 secs)
- **Wide Area Networks –** IEEE **802.16 (WiMAX)**, 802.20 (MobileFi) (3-10 km per cell, high-capacity per user, but a local monopoly?), and proprietary options such as **iBurst**
- **Wide Area Networks – Cellular** (50m to 10km cell-radius, with increasing capacity per user, particularly 3G onwards)
  1G – Analogue Cellular, e.g. AMPS, TACS
  2G – Digital Cellular, e.g. GSM, CDMA
  3G – GSM/GPRS/EDGE, CDMA2000, UMTS/HSPA
  4G – LTE, deployed / deploying
- **Local Area Networks – 'WiFi'** (10-100 m radius) primarily IEEE **802.11x, where x=a,b,g,n**
- **Personal Area Networks** (1-10 metres) – **Bluetooth**, Infra-red?
- **Contactless Cards / RFID Tags / NFC Chips** (1-10cm radius)

2. Surveillance

- The systematic investigation or monitoring of the actions or communications of one or more persons
- The economics of surveillance has been greatly changed by technological developments since the mid-20th century
- Monitoring is of digital personae rather than physical individuals, which can be automated

Forms of Surveillance

- **Communications** Surveillance
- **Dataveillance**
- **Location and Tracking** Surveillance
- **Behavioural** Surveillance
- **Body** Surveillance
  ['Überveillance' Type 1]
- **Omnipresent / Omniscient** Surveillance
  ['Überveillance' Type 2]

Ways to Categorise Surveillance

1. Of What?
2. For Whom?
3. By Whom?
4. Why?
5. How?
6. Where?
7. When?

Ways to Categorise 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) Dataveillance (retrospective, real-time, predictive) Communications / Experience Personal / Mass Surveillance
(6)	Where?	Physical, Virtual, Intellectual
(7)	When?	Once, Recurrent, Scattered, Continuous

The Inevitability of A Surveillance Explosion

- **Earlier Forms of Surveillance**:
  - Labour-Intensive
  - Time-Consuming
  - Expensive

=> Economic Disincentive Against Wide Use

- **Modern Forms of Surveillance**:
  - Automated
  - Cheaper
  - More Reliable

=> The Economic Disincentive Has Been Overcome

3. Concepts of Location and Tracking

- **Location**
  An entity's relationship to known reference points, within a defined space, at a defined point in time
  - Physical Space ('Geo-Location')
  - Network Space
  - Intellectual Space
- Precision, Accuracy, Reliability, Timeliness, ...
- **Tracking**
  The sequence of locations over a period of time

Categories of Tracking

- **Retrospective Tracking**
  Successive locations indicate direction of movement
  Enables retrospective inferencing and action, re:
  - behaviour
  - intention
  - associations
- **Real-Time Monitoring**
  Successive locations indicate direction of movement
  Enables real-time inferencing and prompt action
- **Predictive Tracking**
  Extrapolation from the direction of movement
  Enables real-time inferencing and anticipatory action

Location and Tracking – Data Networks

- The primary identifier is generally IP-Address, which may be assigned short-term or permanently
- The router has access to a 'MAC-Id', which is a device entifier, e.g. processor-id or NIC Id
- Device entifiers may or may not be tightly linked with the individual(s) who use the device
- But Multi-Functional Handsets connect with not only Wifi networks but also cellular networks ...

Location and Tracking – Cellular Networks

Location is Inherent to the Technology

- Insufficient capacity to broadcast all traffic in all cells
- The network needs to know the cell each mobile is in
- Mobiles send registration messages to base-station(s)
- Even if nominally switched off or placed on standby

Location and Tracking – Cellular Networks

Location is Inherent to the Technology

- Insufficient capacity to broadcast all traffic in all cells
- The network needs to know the cell each mobile is in
- Mobiles send registration messages to base-station(s)
- Even if nominally switched off or placed on standby

What's Being Tracked?

- The SIM-card, an identifier of the device
- The mobile-phone id, an entifier of the device
- The person the SIM-card and/or mobile-phone is registered to (and may be required by law to be so)
- Most handsets have one SIM-card, and one user

The Practicability of Location and Tracking in Cellular Networks

- **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 (√)

The Precision of Device Location

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

Device Location – Accuracy and Reliability

- **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 Primary Geolocation Technologies

Technology	Acquirer	Process	Data Quality
Cell Location	Base-Station	Device registers with the base-station 10 times per second	50-100m or several hundred metres
Directional Analysis	Base-Station	Receivers have a known arc and range	Sector within Cell, with errors
Triangulation	Base-Station	Multiple base-stations per Cell enable location within the intersection of their Sectors	Multilateral space within Cell (e.g. a triangle), with errors
Signal Analysis	Base-Station	TDOA (Time Difference of Arrival, aka multi-lateration) RSSI (Received Signal Strength Indicator) AOA (Angle of Arrival)	Small space within Cell, with errors
Proximity to a particular Wifi Router	Any Message Recipient	Commercial services gather and maintain databases of recorded location of Wifi Routers	10m claimed 50-100m measured with errors
GPS	The Device	Device detects satellite signals, Device self-reports its coordinates	7-8m claimed 20-100m measured availability and speed issues, with errors

http://www.rogerclarke.com/DV/LTMD.html

Mobile Device Signatures (MDS)

- Device-signal characteristics may be sufficiently distinctive that each device in the vicinity can be distinguished from the others
- Service sold to shopping-precinct owners and shops, to detect congestion-points, routes taken, dwell-times, repeat-visits, conversion-rates, 'where shops' data, etc.
- Linkable with sales data, CCTV images
- All data is accumulated by the service-provider
- In clear breach of the intent of both electronic interception and data protection laws

http://www.pathintelligence.com

Location-Based Services

- Services to **the Device-User – Direct**
  - Navigation to a defined location
  - Discovery of nearby facilities
- Services to **the Device-User – Indirect**
  - Search-and-Rescue
- Services to **Government Agencies**
  - Personal Surveillance
  - Mass Surveillance / Dragnet / Data-Trawl
- Services to **Corporations**
  - Advertising / Marketing
  - Insurance / Car-Hire

Additional Location and Tracking Scenarios

- Arresting a crook
- Investigating the proximity of suspect to crime-scene
- Targeting an enemy or a competitor

- Being targeted by an enemy or a competitor
- Being found by a fan, stalker, abusive ex-partner
- Having your association with a person discovered
- Being accused of association with another person
- Being targeted by a marketer ...
- ... who knows a great deal about you
- Being monitored by your partner, or your next date

4. Privacy Impacts

Privacy

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

Privacy Dimensions

- Privacy of the Physical Person
- Privacy of Personal Data
- Privacy of Personal Communications
- Privacy of Personal Behaviour
- Privacy of Personal Experience

http://www.rogerclarke.com/DV/Intro.html#Priv (1997)
http://www.rogerclarke.com/DV/SMTD.html#PSMP (2013)

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 is a process of finding appropriate balances between privacy and multiple competing interests

Privacy Factors in Location and Tracking

- Sensitivity of the Data
- Intensive Collection resulting in rich data-sets
- Automatable Collection leads to automated detection of, and punishment for, minor infringements that hitherto have gone unpunished
- Automated mining and correlation enables inferencing about multiple individuals and networks
- Wrong Inferences from inaccurate data
- Spurious Inferences from happenstance

Location Surveillance Risks

- **Retrospective Use**:
  - Suspicion-generation
  - Mapping of Social Networks
  - Guilt by Proximity
    Revival and extension of consorting crimes
  - Behavioural S | | Comms S | | Dataveillance
- **Real-Time Use**: Plausible criminalisation based on identity, location, video footage (and comms?)
- **Predictive Use**: Plausible criminalisation based on intention inferred from observed behaviour

Chilling Effects of Location and Tracking

- Chilling Effects on:
  - Terrorism
  - Crime
  - Sociopathic Behaviour
  - Breach of Conditions for Remand, Parole
  - 'Anti-Social Behaviour'
- Chilling Effects on:
  - 'Anti-Social Behaviour'
  - Creative Behaviour
  - Dissidence
  - Travel
  - Association
- Denial of:
  - Service
  - Travel
  - Identity

5. Natural Controls

- **Technological Limitations**
- **Physical Danger**
- **Economics**. But:
  - Benefits exist, and Costs have plummeted
  - Disbenefits are borne by others
- **Reputation / Public Opinion**. But:
  - Projected as being 'for customer convenience'
  - Media primarily republishes organisations' Media Releases, and concentration span is short
- **Activism** (complaints, boycotts, demonstrations, civil disobedience, physical and cyber-attacks). But:
  - Imbalance of power

6. Regulatory Forms

Forms: / Actors:	**Formal Regulation** ('Government')	**Co-Regulation**	**Industry Self-Regulation**	**Organisational Self-Regulation** ('Governance')
The State	**Determines What and How**	**Negotiates What and How**	Influences What	Has Limited Influence
Industry Assocn	Influences What and How	**Negotiates What and How**	**Determines What and How**	Influences What and How
Corporations	Contribute to Industry Assocn	Contribute to Industry Assocn	Contribute to Industry Assocn	**Determine What and How**
Other Stakeholders	May or May Not Have Some Influence	May or May Not Have Some Influence	May or May Not Have Some Influence	May or May Not Have Some Influence
	Statutes, Delegated Legislation	Statutory Codes & Standards	Industry Codes & Standards	Customer Charters

Clarke & Bennett Moses
http://www.rogerclarke.com/SOS/Drones-PS.html#R

Organisational Self-Regulation

- The Mythologies of 'Business Ethics' and 'Corporate Social Responsibility' (CSR)
- Self-Restraint, e.g. a Customer Charter
  - Strategic
  - Tactical

Nonesuch

Industry Self-Regulation

- Industry Codes
  Aspirational window-dressing
- Industry Standards
  Effectively non-existent
- No Commitments
- No Enforcement

"Wolves self-regulate for the good of themselves and the pack, not the deer"

Co-Regulation

- Statutory Framework
- Statutory Code(s) negotiated among Stakeholders
- Statutory Standards negotiated among Stakeholders
- Education, Business Process Design, Complaints Processes, Back-Ended by Damages Provisions and Criminal Sanctions

BUT:

- The public is seldom represented and empowered
- The Agency is subject to regulatory capture
- Enforcement is commonly lacking

Nonesuch

Formal Regulation

- **Consumer Protection Laws**
  - Permit unconscionable Terms of Service
- **Data Protection Laws**
  - IT advances have rendered existing laws obsolete
  - Parliaments fail to provide effective protections
- **Data Communications Laws**
  - Telecomms Interception provisions unenforced
- **Privacy Supervisory Agencies**
  - Most are toothless
  - All are Government appointments
  - All are dependent on Government funding

Contemporary Regulation of Surveillance

Tort

- Interference with Real Estate (Trespass, Nuisance)
- Interference with the Person (Trespass, Obstruction, False Imprisonment, Assault, AVOs / PSIOs)
- Interference with Emotional State (Stalking, Negligence)
- Deceitful Behaviour (Misrepresentation, Deceit, Passing-Off)

Surveillance Statutes

- Telecomms (postal, TIAA, computer offences)
- Aural/Visual Surv Devices (Clth, State, Territory)
- Pornography, Anti-Voyeurism

Other Statutes (Copyright, Trademarks, Media Law, Human Rights, Privacy)

http://www.rogerclarke.com/DV/POVSRA.html
http://www.rogerclarke.com/DV/MSR.html
http://www.rogerclarke.com/SOS/Drones-BP.html

APF's Meta-Principles for Privacy Protection

1. Evaluation
2. Consultation
3. Transparency
4. Justification
5. Proportionality
6. Mitigation
7. Controls
8. Audit

The Regulation of Visual Surveillance
APF's Principles

1. Justification
2. Proportionality
3. Openness
4. Access Security
5. Controlled Use
6. Controlled Disclosure
7. Controlled Publication
8. Cyclical Destruction
9. Review
10. Withdrawal

Technical Protections
Privacy Enhancing Technologies (PETs)

- **Avoidance**
  - Don't use such devices
  - Don't use offending software / services
- **Obfuscation**
  - Understand and use preferences
  - Suppress location
  - Consolidate digital personae
- **Falsification**
  - Falsify location
  - Project many digital personae

Location and Tracking of Mobile Devices
Agenda

1. Mobile Technologies
   - Devices
   - Communications
2. Surveillance
3. Location Technologies
4. Privacy Impacts
5. Natural Controls
6. Regulatory Framework

Location and Tracking of Mobile Devices

Roger Clarke

Xamax Consultancy, Canberra
Visiting Professor in Cyberspace Law & Policy, UNSW, Sydney
Visiting Professor in Computer Science, ANU, Canberra

Research conducted with

Ass Prof Katina Michael, Uni of Wollongong

http://www.rogerclarke.com/II/LTMD-1401 {.html, .pdf}

University of Southampton
27 January 2014

Drill-Down Slides

The Vulnerability Aspect

- **The Environment**
  - Physical Surroundings
  - Organisational Context
  - Social Engineering
- **The Device**
  - Hardware, Systems Software
  - Applications
  - Server-Driven Apps (ActiveX, Java, AJAX)
  - The Device's Functions: Known, Unknown, Hidden
  - Software Installation
  - Software Activation
- **Communications**
  - Transaction Partners
  - Data Transmission
- **Intrusions**
  - Malware Vectors
  - Malware Payloads
  - Hacking, incl. Backdoors, Botnets

Threat Aspects – Second-Party

- **Situations of Threat**
  - Banks
  - Telcos / Mobile Phone Providers
  - Toll-Road eTag Providers
  - Intermediaries
  - Devices
- **Safeguards**
  - Terms of Contract
  - Risk Allocation
  - Enforceability
  - Consumer Rights

Threat Aspects – Third-Party, Within the System (Who else can get at you, where, and how?)

- **Points-of-Trans'n Physical**
  - Observation
  - Coercion
- **Points-of-Trans'n Electronic**
  - Rogue Devices
  - Rogue Transactions
  - Keystroke Loggers
  - Private Key Reapers
- **Comms Network**
  - Interception
  - Decryption
  - Man-in-the-Middle Attacks
- **Points-of-Processing**
  - Rogue Employee
  - Rogue Company
  - Error

Threat Aspects – Third-Party, Within the Device

- **Physical Intrusion**
- **Social Engineering**
  - Confidence Tricks
  - Phishing
- **Masquerade**
- **Abuse of Privilege**
  - Hardware
  - Software
  - Data
- **Electronic Intrusion**
  - Interception
  - Cracking / 'Hacking'
    - Bugs
    - Trojans
    - Backdoors
    - Masquerade
  - Distributed Denial of Service (DDOS)
  - Infiltration by Software with a Payload

Key Threat / Vulnerability Combinations re Mobile Payments

- **Unauthorised Conduct of Transactions**
- **Interference with Legitimate Transactions**
- **Acquisition of Identity Authenticators**

  e.g. Cr-Card Details (card-number as identifier, plus the associated identity authenticators)

  e.g. Username (identifier) plus Password/PIN/Passphrase/Private Signing Key (id authenticator)

  e.g. Biometrics capture and comparison

4. What Do We Do About It?

- Consumers
- Organisations
  - Corporate Devices
  - BYOD

The Status of Consumer Protection

- **EFT Code of Conduct** – phasing out
  http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/EFT-Code-as-amended-from-1-July-2012.pdf
- **ePayments Code** – phasing in c. 30 March 2013
  http://www.asic.gov.au/asic/asic.nsf/byheadline/ePayments-Code?openDocument
- Soft regulation of such things as receipts, risk apportionment, complaints, privacy, ...
- The banks have sought to weaken the protections (In NZ they succeeded, but were beaten back by the tide of public opinion, and withdrew the changes)
- The Code's provisions apply to contactless-card transactions – but with a lot of 'buts'

The Absolute-Minimum Security Safeguards

1. Physical Safeuguards
2. Access Control
3. Malware Detection and Eradication
4. Patching Procedures
5. Firewalls
6. Incident Management Processes
7. Logging
8. Backup and Recovery Plans, Procedures
9. Training
10. Responsibility

Beyond the Absolute-Minimum Safeguards

Risk Asssessment, leading to at least some of:

11. Data Communications Encryption
12. Data Storage Encryption
13. Vulnerability Testing
14. Standard Operating Environments
15. Application Whitelisting
16. Device Authentication and Authorisation
17. Use of Virtual Private Networks
18. Intrusion Detection and Prevention
19. User Authentication
20. Firewall Configurations, Outbound