

Freedom and Privacy: Positive and Negative Effects of Mobile and Internet Applications

Roger Clarke

Xamax Consultancy Pty Ltd, Canberra
Visiting Professor in Computer Science, ANU
and in Cyberspace Law & Policy, UNSW
Long-Term Privacy Advocate, esp. Aust. Privacy Foundation

**Interdisciplinary Conf. on 'Privacy and Freedom'
Bielefeld University – 4-5 May 2015**

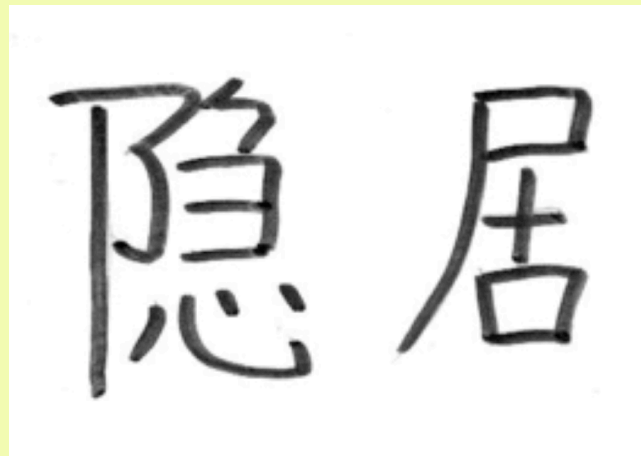
<http://www.rogerclarke.com/DV/Biel15> {.html, .pdf}

Copyright
2015



Privacy

The interest that individuals have in sustaining
a 'personal space' free from interference
by other people and organisations
(Morison 1973)



Justification – Longstanding

Privacy is a shield for individual autonomy

Justification – Alternative

Privacy

{protects the contexts that support (Dorota / Liberalism) OR
defends against dominance over (Andrew / Republicanism)}

each person's

{physical, psychological, political}

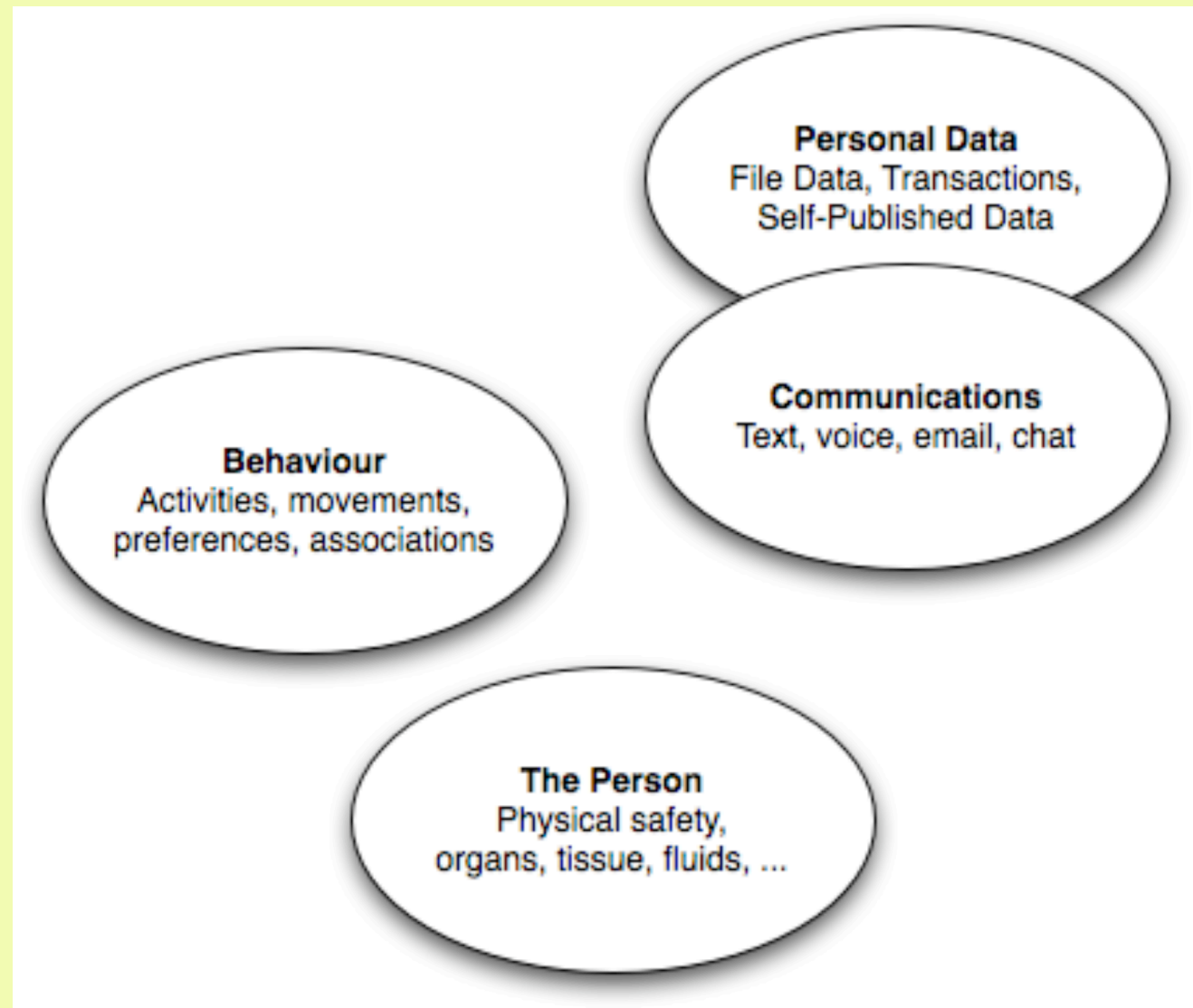
{independence, self-governance, self-determination}

Why Privacy ?

- **Physical Needs**
Personal Safety, Physical Integrity
- **Psychological Needs**
Intellectual Integrity, Self-Determination, Self-Actualisation
- **Social / Sociological Needs**
Behaviour, Association, without Continual Observation
- **Economic Needs**
Innovation through 'Different-Thinking' 'outside-the-square'
- **Political Needs**
Innovation through Debate, Non-Conformance, Deviance
- **Spiritual Needs, Human Dignity**

Four Privacy Dimensions

(cf. Kinds,
Aspects,
Realms,
Spheres,
Types ...)



Now Five Privacy Dimensions



Privacy Dimensions as Human Rights

Experience
Reading, viewing,
interacting, associating
ICCPR 18, 19, 22

Personal Data
File Data, Transactions,
Self-Published Data
ICCPR 17.1

Behaviour
Activities, movements,
preferences, associations
ICCPR 12,17,18,19,21,22

Communications
Text, voice, email, chat
ICCPR 17.1

The Person
Physical safety,
organs, tissue, fluids, ...
ICCPR 6, 7, 8, 9, 10, 11

IT's Negative Impacts (Privacy-Invasive Technologies – The PITs)

Copyright
2015



<http://www.rogerclarke.com/DV/PITsPETs.html>

IT's Negative Impacts (Privacy-Invasive Technologies – The PITs) Privacy of Personal Data

- Data Collection
- Data Expropriation
- Data Consolidation
- Organisation Consolidation
- Data Exploitation

IT's Negative Impacts

Privacy of Personal Communications

- Metadata Retention and Access
- Content Interception, Message-Storage Access
 - Fixed-Line Telephony
 - Mobile Telephony
 - Fixed-Line Internet Access
 - Mobile Internet Access
- Use may be:
 - Real-Time
 - Retrospective
 - Predictive

IT's Negative Impacts

Privacy of Personal Communications

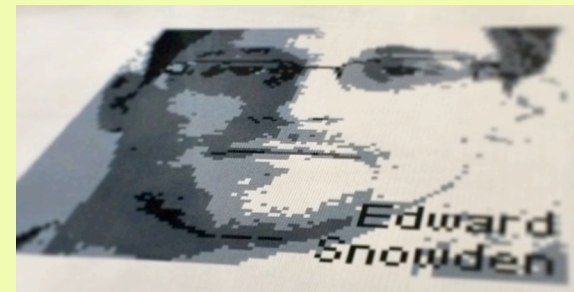
- Metadata Retention and Access
- Content Interception, Message-Storage Access
 - Fixed-Line Telephony
 - Mobile Telephony
 - Fixed-Line Internet Access
 - Mobile Internet Access
- Use may be:
 - Real-Time
 - Retrospective
 - Predictive

Echelon

PRISM

...

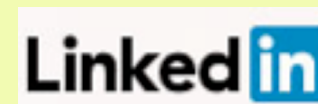
Five Eyes



IT's Negative Impacts

Privacy of Personal Communications

- Metadata Retention and Access
- Content Interception, Message-Storage Access
 - Fixed-Line Telephony
 - Mobile Telephony
 - Fixed-Line Internet Access
 - Mobile Internet Access
- Use may be:
 - Real-Time
 - Retrospective
 - Predictive



IT's Negative Impacts

Privacy of Personal Behaviour

- **Visual Surveillance of Spaces**
CCTV, wearcams, PoV cameras, ICV, drones, etc.
- **Visual Surveillance of Traffic Corridors**
Automated Number-Plate Recognition (ANPR)
- **Mapping of Physical Social Networks**
Analysis of the intersections among individuals' tracks, and inferencing about encounters
- **Mapping of Electronic Social Networks**
Analysis of message metadata and / or content

IT's Negative Impacts

Privacy of Personal Experience

- **Recording of Content Sought**
Web-searches
- **Recording of Metadata of Content Accessed**
Web-logs
- **Recording of Content Read and Viewed**
Web-logs, Web-caches, e-books
- **Mapping of Intellectual Networks**
Analysis of search-terms and metadata
and of content accessed, read and viewed
- **Inferences from Behaviour Surveillance**

IT's Negative Impacts

Enabling Technologies – (Id)entification

Identity Requirements

Pre-Registration, production of
Identity Authenticators

- Telephony connections
- Internet connections
- Mobile Handsets
- Internet Services

Biometric Entifiers

Device-Id – IMEI, IMSI

Device-Id Transmission

Message-Headers, IPv6 address

Electronic Identification

Cookies, web-bugs, ...

Transport tickets

Toll-road tags

Vehicle microchips

Human microchips

Ubiquitous / Pervasive /

Ambient /

Net of Things? /

Net of People?

IT's Negative Impacts

Enabling Technologies – Location and Tracking

Modes

Capture of Current Location
Real-Time Location Tracking
Retrospective Tracking
Predictive Tracking
Co-Locational Inferencing

Physical Means

ANPR
'Facial recognition' CCTV?

Electronic Means

Cookies, web-bugs
Transport tickets
Toll-road tags
Vehicle microchips
Human microchips
Net of Things, People

IT's Negative Impacts – Enabling Technologies

Interference with Human Behaviour

- **'Self-Discipline' / 'Chilling Effect'**
- Reminders of the existence of surveillance
- **Targeted Messages** – direct, and 'advertisements'
- Internet Access Restrictions
- Meetings and Interviews with authorities' agents
- **Travel Restrictions**, e.g. no-fly lists
- **Real-Time Interdiction**, e.g. en route to an event
- Denial of Liberty
Arrest, detention, charge, remand in custody,
prosecution incl. with non-defensible crimes

IT's Positive Impacts

Q: What about Privacy Enhancing Technologies (PETs)?

A1: In Principle, PETs are necessary but not sufficient

Legal and organisational measures are essential,
as complements to technical measures

A2: In Practice, PETs are immature

PET Coding is okay; but PET Design remains poor

PETs

Tech Categories

Device-Management Tools

- CD/USB Based OS
- Disk/File Encryption
- Disk/File Erasing Programs
- Password Vaults

Traffic-Related Tools

- Anonymizers, Virtual Private Networks (VPNs), Proxy Servers
- Firewalls
- Antivirus
- Mesh Networks
- Publishing

Email-Related Tools

- Email Encryption
- Alternative Email Accounts
- Anonymous Remailers

Web-Related Tools

- Web Browser Ad-ons
- Cookie/Cache/History Cleaners
- Search Engines
- Social Networking

Other Comms-Related Tools

- Secure Instant Messaging
- VoIP/Video Messaging
- Temporary Mobile Phones
- Mobile Privacy

Other Commerce-Related Tools

- Alternative Currencies

Impediments to PET Adoption

- **(Un)Awareness**
Why would I need one of those?
- **(In)Comprehensibility**
It does what?
- **(Un)Installability**
How do I get it on my device(s)?
- **(Un)Usability**
How do I get it to do what I need?
- **(In)Convenience**
Does it interfere with my activities?

Societal Resilience

(1) Precaution / Prevention

Ensure that proposals that embody threats are subject to an appropriate process

Technology Assessment (TA)

Social Impact Assessment

Privacy Impact Assessment

Surveillance Impact Assessment

Meta-Principles for Privacy Protection

Pre-Conditions

1. **Evaluation**
2. Consultation
3. Transparency
4. Justification

Design

5. Proportionality
6. Mitigation
7. Controls

Review

8. Audit

Meta-Principles for Privacy Protection

Pre-Conditions

1. Evaluation
2. Consultation
3. Transparency
4. Justification

Design

5. Proportionality
6. Mitigation
7. Controls

Review

8. Audit

International Principles on
the Application of Human Rights
to Communications Surveillance

<https://en.necessaryandproportionate.org/>

Societal Resilience

(1) Precaution / Prevention

Ensure that proposals that embody threats are subject to an appropriate process

Technology Assessment (TA)
Social Impact Assessment
Privacy Impact Assessment
Surveillance Impact Assessment

(2) Resistance

Agitation, incl. to ensure that the process is applied

Avoidance, Civil Disobedience, Political Speech, Media Coverage, Demonstrations, Court Actions, Sabotage

(3) Robustness

Ignore it, Deride it
Become inured, take the risk
Intentionally transgress,
and dare authorities to act

Societal Resilience Through PETs

1. Basic PETs

To counter Privacy-Invasive Technologies (The PITs)

- **Stored Data Security**
- **Message Security**
Content interception, Traffic surveillance, Location collection
Default encryption of traffic / HTTPS Everywhere
- **Authentication** of senders and recipients of content
- **Peer-to-Peer Architectures**, not client-server architectures
- Avoidance of telecommunications backbones in favour of '**Mesh Networks**' linking peripheral local area networks

Societal Resilience Through PETs

2. Savage PETs

To deliver persistent anonymity

- These have the effect of undermining accountability
e.g. SecureDrop whistleblower protection tool
Tor for Source-Obfuscation

Societal Resilience Through PETs

2. Savage PETs

To deliver persistent anonymity

- These have the effect of undermining accountability
e.g. SecureDrop whistleblower protection tool
Tor for Source-Obfuscation

3. Gentle PETs

To deliver protected pseudonymity

- These (could) enable accountability to co-exist with freedom
- **BUT** they depend on legal, organisational and technical protections, to withstand malbehaviour by natsec agencies

Societal Resilience Through PETs

1. Basic PETs

To counter Privacy-Invasive Technologies (The PITs)

2. Savage PETs

To deliver persistent anonymity

3. Gentle PETs

To deliver protected pseudonymity

4? Counter-Attacking Technologies (CATs?)

5? Assault Technologies (ASSes?)

The Key Things to Obfuscate and Falsify

Data

If a person's stored data could result in some organisation constraining their or another person's freedom or privacy, the content of the stored data may need to be hidden

Messages

Re a person's communications

Identities

Re the identities under which a person performs acts

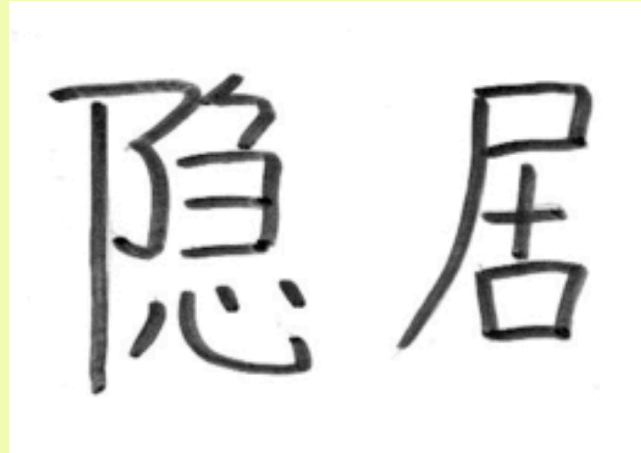
Locations

Re the locations at which a person performs acts

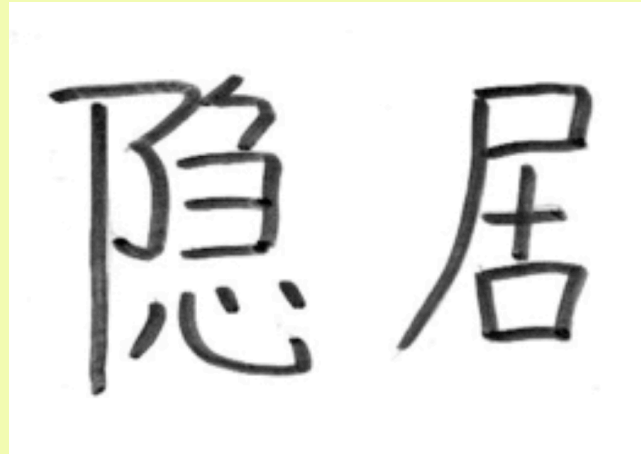
Social Networks

Re the associations that a person has with others

From: 'Hidden Person'



From: 'Hidden Person'



To: Hidden Data
... Messages
... Identities
... Locations
... Social Media

Consumer-Oriented Social Media

- **Distributed Architecture**
Probably P2P (but possibly Client-Server with Obfuscation)
- **Interoperability**
Content and messages can be exchanged between services
- **Portability**
Content and messages can be extracted from one service and loaded into another
- **Consumer-Friendliness**
In Features, and in Terms of Service
- **Privacy-Protectiveness**
In Features, and in Terms of Service

Will You Apply PETs if they are:

- Incomprehensible?
- Unusable?
- Usable?
- Embedded?

‘Privacy By Design’ means what exactly?

Privacy by Default

Freedom and Privacy: Positive and Negative Effects of Mobile and Internet Applications

Roger Clarke

Xamax Consultancy Pty Ltd, Canberra
Visiting Professor in Computer Science, ANU
and in Cyberspace Law & Policy, UNSW
Long-Term Privacy Advocate, esp. Aust. Privacy Foundation

**Interdisciplinary Conf. on 'Privacy and Freedom'
Bielefeld University – 4-5 May 2015**

<http://www.rogerclarke.com/DV/Biel15> {.html, .pdf}

Copyright
2015



Freedom

The scope for a person
to determine their own behaviour
subject only to those constraints
that are necessary to sustain
the freedoms of others,
social and political cohesion, and
economic wellbeing and sustainability

Rights in Support of Freedom

- Positive human rights – to express views, to perform acts, to refrain from acting
- Negative human rights – to be free from unreasonable external constraints on thoughts, words and deeds
- Rights may be 'merely' moral or social
- Rights may be legally protected, by means of:
 - The rule of law
 - Laws that give rise to rights; &
 - Enforcement of those laws

Basis in International Law



- **Rights to Liberty**
Rights to Participation in Political Life
(UDHR 1948 Articles 3-21, ICCPR 1966)
- Rights to Equality
(UDHR 1948 Articles 22-27, ICESCR 1966)
- Rights of Particular Categories of People
e.g. Children, Older People

Self-Determination

- **'Self-Determination of Peoples'**
The capacity of a (voting) populace within a nation-state to determine that country's political, economic, social and cultural activities (ICCPR Article 1)
- **Individual Self-Determination / 'Free Will'**
If individualism were strongly valued, this would be a foundation underlying human rights
- No such internationally-recognised right has been formalised in human rights documents
- A qualified form exists, in the form of Privacy

Privacy

The interest that individuals have in sustaining
a 'personal space' free from interference
by other people and organisations
(Morison 1973)

Privacy is one interest among many.

Privacy protection is an exercise in balance
(just like protection of every other human interest).

There are no 'privacy absolutists'.