The Shape of PETs 2.0

Roger Clarke
Xamax Consultancy Pty Ltd, Canberra
Visiting Professor, UNSW Law
Visiting Professor, Computer Science, ANU

http://www.rogerclarke.com/DV/PETs2S {.html, .pdf}

Doctoral College 2050: Privacy and Trust for Mobile Users
Technische Universität Darmstadt
28 November 2016

The Shape of PETs 2.0
Agenda

- PETs
- Failure Factors and the Remedies
  - Conception
  - Requirements
  - Architecture
  - Design
  - Dissemination
  - Understanding
  - Adoption
  - Use
- A Test-Case: Consents and Denials

PITs and PETs

- **PITs** – Privacy-Invasive Technologies

http://www.rogerclarke.com/DV/PITsPETs.html
http://www.rogerclarke.com/DV/Biel15-DuD.html#P

Forms of Interference with Human Behaviour

- Chilling Effect of surveillance / 'self-discipline'
- Reminders of the existence of surveillance
- Targeted messages (direct communications, custom-ads)
- Internet Access Restrictions
- Meetings, Interviews with authoritarian institutions
- Travel restrictions, e.g. no-fly lists
- Real-Time Interdiction on the move
  e.g. en route to a relevant event
- Denial of liberty, through arrest, detention, charge, remand in custody, and prosecution incl. with crimes that are incapable of being defended against

PITs and PETs

- **PITs** – Privacy-Invasive Technologies
- **PETs** – Privacy-Enhancing Technologies
  A long line of work since 1995
  - **Counter-PITs**, incl. protections for data in storage and in transit, authentication, ...
  - **Savage PETs**
    for Persistent Anonymity

  - **Gentle PETs**
    for Protected Pseudonymity, and hence accountability as well as freedom

PET Successes

- **Focus** on 'Technology for Privacy'
- **Venues**

  PET Workshops and Symposia, 2000-
  https://petsymposium.org/2016/links.php

  Symposia on Usable Privacy and Security (SOUPS), 2005-
  https://cups.cs.cmu.edu/soups
- **Publications** – thousands, generic and specific
- **Citations** – tens of thousands
- **Products**

PET Products

Catalogues

https://www.**epic**.org/privacy/tools.html
https://**prism-break**.org/en/
https://ssd.**eff**.org/en/index
https://www.**bestvpn**.com/blog/49728/ultimate-privacy-guide
https://www.**privacytools**.io/
http://www.rogerclarke.com/DV/UPETs-1405.html#Cat

An Alternative Categorisation of PETs

1. Communications
2. Traffic Management
3. Data Management

Categories of PETs – 1. Communications

- **Email and Instant Messaging / Chat**
  e.g. Protonmail, Tutanota, Hushmail, Fastmail, Wickr?
- **Handsets**
  e.g. Silent Circle BlackPhone
- **Browsers**
  e.g. Stripped Chrome, WhiteHat Aviator, Opera/VPN
- **Search-Engines**
  e.g. DuckDuckGo, Ixquick/Startpage
- **Encryption**
  e.g. HTTPS Everywhere
- **Social Media Services**
  e.g. Diaspora

Categories of PETs

2. Traffic Management

- **End-Point Authentication,**
  e.g. VPNs
- **End-Point Obfuscation**
  Proxy-Servers, VPNs, ToR
- **Firewalls, Malware Filters, Cleansers**
- **Meshnets**
- **Privacy-Enhancing Software Agents**

3. Data Management

- **Stored Data Encryption**
  e.g. Veracrypt
- **Secure Data Deletion**
- **Secure Dropbox**
  e.g. SecureDrop, Podzy

PET Adoption Levels

- SSL / TLS
  - Adblockers
  - Malware Filters
    - Proxy-Servers
    - VPNs
      - ... ?

Failures of a Technical Nature

- Requirements Elicitation short-changed / omitted resulting in a poor fit to potential users' needs
- Design casual
- Architecture not considered
- Compatibility with the Mainstream not a priority
- Compatibility with other PETs not a priority

Failures of an Economic Nature

- Inventions, not Innovations
- Unworkable Business Models
- Lack of use of appropriate Channels to Market

Failures of a Socio-Technical Nature

- **Awareness** Why would I need one of those?
- **Comprehensibility** It does what?
- **Ease of Discovery, Acquisition, Installation, and Configuration** How do I get it on my device(s)?
- **Learnability** Can I work out how to use it?
- **Cohesiveness** Do the elements work together?
- **Integration** Is it compatible with what I use?
- **Usability** Can I utilise its features easily?
- **Adaptability** Can I get it to fit to my needs?
- **Convenience** Does it interfere with my activities?

PET Symposia and SOUPS
The Missing Topics

- Architecture for PETs
- Innovation (as distinct from Invention)
- Articulation
- Integration among PETs
- Integration with systems and applications software
- Relevance to people
- Feedforward into practice
- Adoption
- Impediments to adoption
- Measures to overcome impediments to adoption

https://petsymposium.org/2016/links.php
https://cups.cs.cmu.edu/soups/

Drivers for Adoption

Demand-Side

- Focus on User-Segments
- Understand Needs
- Conduct Risk Assessmt
- Design to address Needs
- Design for Usability
- Provide explanations, examples, training
- Use channels suitable for each user-segment
- Sell via opinion leaders

Architecture

- Design-In:
  - Modularity
  - Substitutability
  - Interoperability
  - Portability
  - Decentralised Control
  - FOSS
- Provide integrated Suites not standalone Tools
- Embed in Users' Working Environments

Supply-Side

- Deliver through key suppliers
  - Devices, OS
  - IAPs

http://www.rogerclarke.com/DV/UPETs-1405.html
http://www.rogerclarke.com/DV/SeWE16.html

Generic Needs
(1) 'Functional Requirements'

Beyond 'Confidentiality, Integrity and Availability' (CIA):

- **Accessibility** by authorised people of (a) data, (b) traffic and (c) social networks
- **Inaccessibility** by unauthorised people of (a) data, (b) traffic and (c) social networks
- **Integrity** of (a) data, (b) traffic, (c) social networks

- **Unlinkability** of sessions
- **Non-Detectability** of traffic
- **Plausible Deniability** of actions

The Key Things to Obfuscate and Falsify

Data

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

Messages

Re a person's communications

Identities

Re visibility of the identity under which a person performs acts

Locations

Re visibility of the location at which a person performs acts

Social Networks

Re the associations that a person has with others

(1) Functional Requirements
Mandatories: Baseline Security Safeguards

1. Physical Safeguards
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

http://www.xamax.com.au/EC/ISInfo.pdf

Generic Needs
(2) 'Non-Functional' Requirements

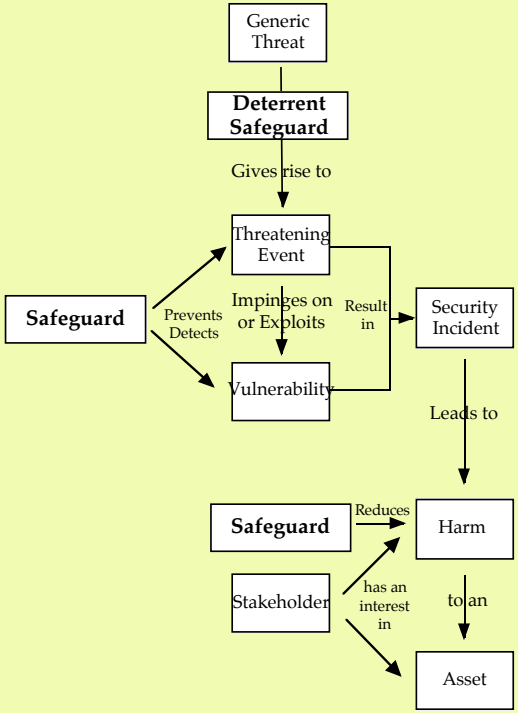
- **Awareness** It has an apparent fit to a known need
- **Comprehensibility** Its function is apparent
- **Ease of Discovery, Acquisition, Installation, and Configuration** It's easy to get it installed
- **Learnability** It's easy to work out how to use it
- **Cohesiveness** The elements work together
- **Integration** It's compatible with the mainstream
- **Usability** Its features can be easily applied
- **Adaptability** It can be configured to fit my needs
- **Convenience** It only interferes minimally

User Interface Design for Privacy

EU-funded studies, oriented to the EU Directive:

- Patrick et al. (2002)
  (Chapter 12 of van Blarkom, Borking & Olk's 'Handbook of Privacy and Privacy-Enhancing Technologies')
- Privacy and Identity Management for Europe
  (**PRIME**, 2006-08)
  https://www.prime-project.eu/
- **PrimeLife** (2009-11)
  'Bringing sustainable privacy and identity management to future networks and services'
  http://primelife.ercim.eu/

The Conventional Security Model



http://www.rogerclarke.com/EC/PBAR.html#App1

4. Risk Assessment (RA)

Analyse

(1) Define the Objectives and Constraints

(2) Identify the relevant Stakeholders, Assets, Values and categories of Harm

(3) Analyse Threats and Vulnerabilities

(4) Identify existing Safeguards

(5) Identify and Prioritise the Residual Risks

http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

The Categories of 'Persons-at-Risk' are Diverse

Social Contexts

- Celebrities and notorieties at risk of extortion, kidnap, burglary
- Short-term celebrities such as lottery-winners, victims of crime
- Victims of domestic violence
- Victims of harassment, stalking
- Individuals subject to significant discriminatory behaviour
- People seeking to leave a former association, e.g. ex-gang-members

Political Contexts

- Whistleblowers
- Dissidents
- Human Rights Activists

Organisational Contexts

- Corporate executives
- Government executives
- Undercover operatives
- Law enforcement and prison staff
- Mental health care prof'ls, counsellors

Legal Contexts

- Judges, lawyers and jurors, particularly in highly-charged cases
- Witnesses, especially people in protected witness programs
- Ex-prisoners re-integrating with society

http://www.rogerclarke.com/EC/eHlthRes.html#PAR

http://geekfeminism.wikia.com/wiki/Who_is_harmed_by_a_%22Real_Names%22_policy%3F

Threat 'Models'

Victims of Domestic Violence

Discovery by a specific organisation and any informants of:

- individual identity
- the source documents / content / items of information
- the individuals to whom the d / c / i have been passed
- the individual's current location
- the individual's future locations

Whistleblowers

Discovery by a specific individual and any informants of:

- current location
- future locations

Protest Organisers

Discovery by 'the government' of:

- individual identity
- the movement's social network
- the movement's plans and logistical arrangements
- denial of service by 'the government'

Indicative Risk Assessment for a Whistleblower

Asset – Freedom

Harm – Denial of Freedom

Threats – Discovery of:

- Disclosure of suppressed information / documents
- Identities of persons involved in the disclosure
- Their Location
- Sufficient grounds to act

Vulnerabilities – Exposure of:

- Disclosure
- Identities
- Human entities underlying the relevant Identities
- Location of those persons

Security Safeguards re:

- Disclosures
- Actions, dates and times, physical and net locations,
- Identities
- Entities
- Locations

http://www.rogerclarke.com/DV/UPETs-1405.html#Tab3
https://freedom.press/encryption-works (Lee 2013)

4. Risk Assessment (RA) then Risk Mngt Planning

Analyse

(1) Define the Objectives and Constraints
(2) Identify the relevant Stakeholders, Assets, Values and categories of Harm
(3) Analyse Threats and Vulnerabilities
(4) Identify existing Safeguards
(5) Identify and Prioritise the Residual Risks

Design

(1) Postulate / articulate alternative Designs
(2) Evaluate the alternatives against the Objectives and Constraints
(3) Select a Design (or adapt / refine the alternatives to achieve an acceptable Design)

Do

(1) Plan the implementation
(2) Implement
(3) Review the implementation

http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

(1) Functional Requirements
Additional Security Safeguards for Persons-at-Risk

Risk Asssessment will point 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

http://www.xamax.com.au/EC/ISInfo.pdf

Risk Management Strategies

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

Architectural Features

- **Layering**
  Common, underlying services for all tools
- **Modularity**
  For Tool Substitutability
- **Interface Definitions**
  Protocols for processes, Standards for data
- **Free and Open Source Software (FOSS)**
  'Many hands', 'many eyes'
- **Interoperability**
  Open Protocols, Standards, for cross-device use
- **Portability**
  For use across hardware and systems software
- **Security**
  Features, Settings, Defaults
- **Decentralised Control**
  To avoid ceding power to service-providers

http://www.rogerclarke.com/SOS/OAA-1990.html#MM
http://primelife.ercim.eu/images/stories/deliverables/h1.3.5-requirements_and_concepts_for_idm_throughout_life-public.pdf
http://www.rogerclarke.com/II/COSM-1402.html#COSMF

Characteristics of a Successful Innovation

Relative Advantage
- Perceived to be better than what it supersedes

Compatibility
- Consistent with values, experiences, needs

Complexity
- Not difficult to understand and use

Trialability
- Can be experimented with on a limited basis

Observability
- Its results are visible

Rogers, e.g. http://www.rogerclarke.com/SOS/InnDiff.html

Economic Challenges

What Business Models Work?

A Business Model
is an Answer
to the Question:

Who Pays?

For What?

To Whom?

And Why?

Open ... Models for eBusiness
http://www.rogerclarke.com/EC/Bled04.html

A Key Element of PETs 2.0
A Less-Insecure Web-Browser

1. Install Chromium (not Chrome!!)
2. Strip the following features: ...
3. Set the following Preferences: ...
4. Install the following:
   - CookieMonster
   - BetterPrivacy
   - Ghostery
   - PrivacyBadger
   - ....

Why haven't relevant organisations made this available for one-click download and install??

One Shape That PET 2.0 Will Take

- Locally-installed facilities
- Seamless intermediation between user devices and the Internet Access Provider
  - End-to-end encryption
  - Pseudonymity
  - Unlinkability of sessions
- Minimal need for user expertise
- Minimal need for conscious user actions
- Compatibility with user working environments

comidio TrutzBox

mobile business | AN.ON NEXT GENERATION | Bundesministerium für Bildung und Forschung | AN.ON-next

- **Duration:** 01/2016 – 12/2018
- **Aim:** Create and integrate privacy-enhancing technologies into the internet infrastructure
- **Focus:** Establish PET in the mass market
  - Develop new or adapt existing business models
  - Standardize technologies
  - User study: How do users understand tariff and pricing models?
  - User study: What is the perceived relationship of service feature and accepted prices?
  - How can existing value creation architectures and operational models be adapted?

UR Universität Regensburg | GOETHE UNIVERSITÄT FRANKFURT AM MAIN | Universität Hamburg | TECHNISCHE UNIVERSITÄT DRESDEN | ULD | manitu | JonDonym | comidio

Summary
How to achieve Adoption of Secure eWorking Environments by People who need them

- Focus on one or more relevant **user segments**
- Conduct **risk assessments** for those segments
- Architect and design (or adapt and integrate) **suites of tools** with the relevant features
- **Integrate** those features within targeted user segments' working environments
- Provide clear **explanations, examples, training**
- Identify, and **sell** to, opinion leaders, change agents and change aids

A Test-Case
The User Consent Module

Means of capturing consents and denials
in a form that supports 'policy enforcement'
rather than merely 'policy expression'

Sample Contexts

Health Care Data
Social Media

Consumer-Oriented Social Media
A Possible Set of Priority Features

Not 'The Default is Social'

Not Opt-Out

Consent-Based, incl.:

- Informed
- Freely-Given
- Granular not Bundled
- Settings Management
- Conservative Defaults

Trustworthy Terms

Identity Protections

- Protected Pseudonyms
- Multiple Identities
- Caveats, Social Norms and Reputations

Non-User Protections

- Content
- Social Networks

Location Protections

Trust

Confident reliance by one party about the behaviour of the other parties

- Origins in kinship groups
- Extensible to cultural affinity (i.e. friends)
- Not directly extensible to business relationships
- **Forced reliance is not 'Trust'**

Consent

Concurrence / Authorisation
by one party
with an action
to be taken by another party

Characteristics of Consent

- **Informed**
  - The Scope of the Actions
  - Who may take such Action
  - For what Purpose may it be taken
  - Over what time-period consent applies
- **Freely-given**
- Revocability and Variability
- Legal Capacity
- Physical and Intellectual Capacity
- Delegability

Forms of Consent

- {Express in writing OR
  - Express unrecorded OR
    - Implied OR
      - Inferred}

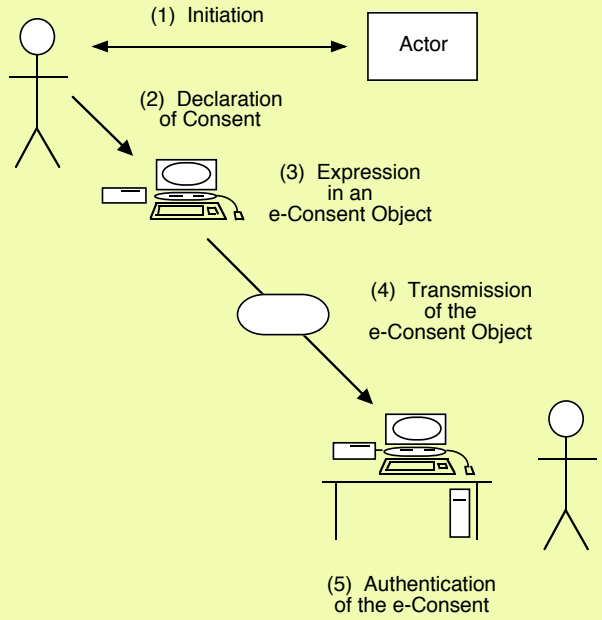
- {Declared [US 'opt-in'] OR
  - Presumed [US 'opt-out'], but
    Subject to the Absence of Express Denial}

e-Consent

Signification by recorded electronic means
of concurrence or otherwise
with an action to be taken by another party

- Recording is essential, to enable authentication
- Recording by electronic means is essential:
  - for practicality and convenience
  - to facilitate automated use
    ('policy enforcement')

The e-Consent Process



(3) Expression of an e-Consent Object

Access to	<data>
by	<one or more entities or identities, or categories thereof>
for	<one or more purposes>
in	<a context>
is	[consented to | denied]
by	<an identity>

http://www.rogerclarke.com/EC/e-C-Cases-020523.pdf
http://www.rogerclarke.com/EC/e-C-Backgrd-Final021201.pdf
http://www.rogerclarke.com/EC/e-C-Impl-Final021201.pdf

Nature of the eConsent Object

- Consent/denial statements, hierarchical/nested
  The first entry may be either a consent or a denial
  Each subsequent entry must be the other category, qualifying the preceding entry
  Examples: a single consent entry; a sequence of a broadly-expressed consent, then a specific denial
- Each entry comprises:
  - Consent/Denial Indicator
  - Declaration of the Data covered
  - Specification of the Authorised Entity
  - Specification of the Purpose of Use
  - Re-Disclosure Conditions

Subtleties in an e-Consent Object

- Specific, Operational Specification of the Domains on which data-items are defined, e.g. which data, which other party or which category of parties, which purpose
- Supplementary Data (e.g. re power of attorney)
- General Consent with Specific Denial (all except ...)
- General Denial with Specific Consent (none except ...)
- A Hierarchy of Consent/Denial/Consent/etc.
- Reliable Date-Time Stamps, to support authentication

The Shape of PETs 2.0
Agenda

- PETs
- Failure Factors and the Remedies
  - Conception
  - Requirements
  - Architecture
  - Design
  - Dissemination
  - Understanding
  - Adoption
  - Use
- A Test-Case: Consents and Denials

The Shape of PETs 2.0

Roger Clarke
Xamax Consultancy Pty Ltd, Canberra
Visiting Professor, UNSW Law
Visiting Professor, Computer Science, ANU

http://www.rogerclarke.com/DV/PETs2S {.html, .pdf}

Doctoral College 2050: Privacy and Trust for Mobile Users
Technische Universität Darmstadt
28 November 2016