

# Can We Productise Secure eWorking Environments?

**Roger Clarke**

Xamax Consultancy Pty Ltd, Canberra

Visiting Professor, UNSW Law

Visiting Professor, Computer Science, ANU

<http://www.rogerclarke.com/DV/SeWE16> {.html, .ppt}

**IFIP Summer School on Privacy & Identity Management**

Karlstad SE – 24 August 2016

**This is a PET Rescue Mission**

**Can we get PETs out of the Laboratory?**

- There are squillions of small products under the 'Privacy-Enhancing Technology' umbrella
- The adoption levels are dismally low  
Honourable exceptions: above all SSL / TLS, but also Tor, Ghostery, ...
- We need to understand the impediments
- And we need to address the deficiencies
- **So that the people who need them, use them**

## Rescue PETs

# Productise Secure eWorking Environments

## Summary

# How 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

# The Workshop Format

0. Introduction to Topic and Purpose  
Segment Structure: Outline then Responses
  1. The Contexts of Insecurity
  2. Needs
  3. Segmentation
  4. Risk Assessment
  5. Tools
  6. Design
  7. Architecture
  8. Test Applications
  9. Implementation – Demand-Side
  10. Implementation – Supply-Side
99. Summary of Outcomes

# 1. The Contexts of Insecurity

## a. Network Infrastructure and Architecture

- **The Internet has been subverted into 'the world's largest surveillance network'**  
Tim Berners-Lee (the Web), Vint Cerf (TCP / IP),  
Brewster Kahle (the Internet Archive)
- **We need to 're-decentralise the Web'**

<http://www.theinquirer.net/inquirer/news/2460894/sir-tim-berners-lee-internet-has-become-world-s-largest-surveillance-network>

Decentralized Web Summit – 8-9 June 2016  
<http://www.decentralizedweb.net/>



# Internet Architecture Board

[Home](#) [About](#) [Activities](#) [Documents](#) [Liaisons](#) [Appeals](#)

[← Reappointment of Lars Eggert as IRTF Chair](#)

[IAB Seeks Feedback on ICANN Technical Liaison Group Candidates](#)

## IAB Statement on Internet Confidentiality

Posted on November  
14, 2014 by cindy

The IAB urges protocol designers to design for confidential operation by default. We strongly encourage developers to include encryption in their implementations, and to make them encrypted by default. We similarly encourage network and service operators to deploy encryption where it is not yet deployed, and we urge firewall policy administrators to permit encrypted traffic.

[https://www.iab.org/2014/11/14/  
iab-statement-on-internet-confidentiality/](https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/)  
<https://tools.ietf.org/html/rfc6973> (Privacy)  
<https://tools.ietf.org/html/rfc7624> (Surveillance)

Copyright  
2016



# The Contexts of Insecurity

## b. Consumer Devices – 'Insecure by Design'

- Massively bug-ridden software ('buffer overflows')
- Insecure default settings
- Backdoors, incl. Auto-Updates
- Un-sandboxed Applications
- http Extensions / AJAX / HTML5
- Web-Server malbehaviour
- Unencrypted communications
- Unauthenticated communication-partners





HTML



- Support for:
  - multi-media streaming
  - open channels as well as sessions
  - geolocation
- **A way to subvert sandboxing**
- **A way to subvert user control, by inverting the Web from pull to push**
- **A way to access local data and devices (e.g. cameras, microphones), giving rise to "A Pandora's box of tracking in the Internet"**

# The Contexts of Insecurity

## c. Authoritarian Governments (throughout the 'Free World' as well)

- Kneejerk reactions to terrorism
- Warrantless access to data
- Exemptions from 'computer crimes' legislation
- The Ephemerality of human communications has been undermined by reduction to digital form
- Digital communications are subjected to '[meta-?]data retention' requirements
- Location-detection, tracking, stalking, pursuit, interdiction, inference of intentions, inference of associations on the basis of co-location

# The Contexts of Insecurity

## d. Authoritarian Corporations

- Onerous Consumer Terms, acquisition of vast amounts of personal data, exploitation, trafficking
- Location-detection, tracking, plus profiling, enabling behaviour manipulation
- Productisation processes that serve
  - Corporations' economic interests
  - Individuals' hedonic interests only
- Replacement of general-purpose computing by limited 'appliances' with use supplier-controlled
- Local autonomy out, cloud-based services in
- 'Internet of Things' as monitoring tools

# Attacks

## By Whom?

### Principals

Opportunists

Hactivists

Vigilantes

Organised Crime

Unfriends

Corporations

Nation-States

### Agents

Mercenaries

Private Military

Corporations

## And Why?

### Politics

Protest against Action

Revenge

Espionage

Social Control

### Economics

Financial Gain

Financial Harm

### Social/Cultural Factors

Lust

Challenge

Dispute

Celebration

# 1. The Contexts of Insecurity

## Discussion Primers

Are important contextual factors omitted / misrepresented / exaggerated?

- a. Network Infrastructure and Architecture?
- b. Consumer Devices – 'Insecure by Design'?
- c. Authoritarian Governments?
- d. Authoritarian Corporations?

Are any attacker categories or motives omitted?

## 2. Needs

- Generic Functional Requirements
  - Security in particular
- 'Non-Functional' Requirements

# Generic Functional Requirements

- Accessibility of data, traffic and social networks by authorised people
- Inaccessibility of data, traffic and social networks by unauthorised people
- Integrity of data, traffic and social networks
- Non-Detectability of traffic
- Plausible Deniability of actions

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

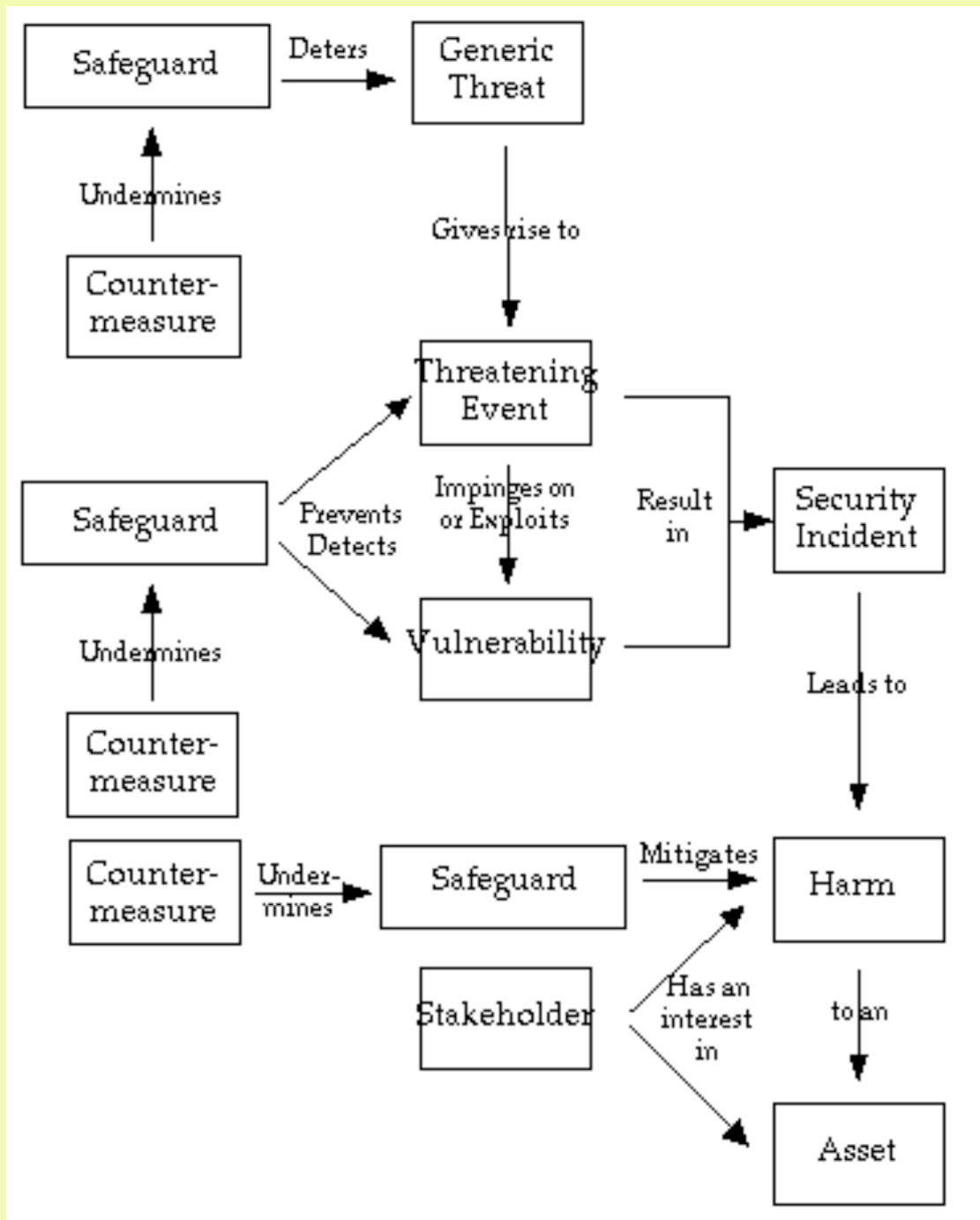
# The Conventional Security Model

## Key Concepts

- A **Threat** is a circumstance that could result in Harm
  - A **Threatening Event** is an instance of a generic Threat
  - A Threat may be natural, accidental or intentional
    - An intentional Threatening Event is an **Attack**
    - A party that creates an Intentional Threat is an **Attacker**
- A **Vulnerability** is a susceptibility to a Threat
- **Harm** is any kind of deleterious consequence to an **Asset**
- A **Safeguard** is a measure to counter a Threat
- A **Countermeasure** is an action to circumvent a Safeguard



# The Conventional Security Model



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

Copyright  
2016



# Conventional IT and Data Security Safeguards

## The Physical Site

- Physical Access Control (locks, guards, ...)
- Smoke Detectors, UPS, ...

## Hardware

- Parity-checking, read-after-write
- Backup and Recovery

## Network

- Channel encryption
- Firewalls
- Intrusion Detection

## Software

- Authentication of data, of value, of (id)entity, and/or of attributes
- Access Control, Authorisations

## Liveware

- **Human Procedures**  
Control Totals, Reconciliations
- **Organisation**  
Respy / Authy, Separation of duties

## Legal Measures

- Duty Statements, Terms of Use, Contractual Commitments

# The Absolute-Minimum Security Safeguards for Small Business – and for People?

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

# Absolute-Minimum InfoSec Safeguards

## 2. ACCESS CONTROL, including:

- user-accounts allocated to individuals for their, & only their, personal use
- privileges limited to only the software, functions and data that are required for that person's work
- tight control over super-user accounts, to reduce the opportunity for abuse of access privileges

## 3. MALWARE DETECTION AND ERADICATION

(Malware is used here as a generic, encompassing viruses, worms, spyware, bots, rootkits, etc. – <http://rogerclarke.com/II/RCMal.html>)

- on all inbound traffic; and
- periodically on all storage devices

## 4. PATCHING PROCEDURES

To ensure the frequent application of all security-relevant updates and patches to all systems software and application software

# 'Non-Functional' Requirements

- **Awareness** - why would I need one of those?
- **Comprehensibility** - it does what?
- **Ease of Discovery, Acquisition, Installation and Familiarisation** - how do I get it on my device(s)?
- **Cohesiveness** - do the elements work together?
- **Integration** - is it compatible with my device(s), software?
- **Usability** - can I utilise its features without difficulty?
- **Adaptability** - can I get it to fit to my needs?
- **Convenience** - does it interfere much with my activities?

## 2. Needs Discussion Primers

Are there better models of functional requirements?

Are there better models of non-functional requirements?

## 3. Segmentation

### Diversity of Risk-Generating Activities

- Inbound Communications
- Outbound Communications
- Contact-List / Social Network Management
- Location and Location-Trail Management
- Research (documents viewed, search-terms used)

# Diverse Categories of 'Persons-at-Risk'

## 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

## 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



# Diverse Categories of 'Persons-at-Risk'

## 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**

## 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

# Possible Security Profiles

- **Low Security / High Convenience**  
'**Carefree** social media' ... social ephemera, trivia  
<http://www.rogerclarke.com/EC/SSACS.html#App2>
- **Medium Security / Medium Convenience**  
'**Careful** social media', e.g. 'enterprise' purposes, and where subject to privacy and/or security concerns  
<http://www.rogerclarke.com/EC/SSACS.html#App3>
- **High Security / Low Convenience**  
**Undercover** operatives, corporate takeover analysts, researchers handling delicate data, diplomats, ...  
**Persons-at-Risk** (protected witness, whistle-blower)  
<http://www.rogerclarke.com/EC/SSACS.html#App4>

# Absolute-Minimum InfoSec Safeguards

## A Less *Ad Hoc* Approach

- Stratify into Market Segments
  - For each Market Segment:
    - Conduct a generic Risk Assessment
    - Establish a generic Risk Management Strategy
    - Articulate Strategy into a Management Plan
- ? A Possible Segmentation Basis:  
'Carefree' / Careful/Normal Business / 'Exposed'

### 3. Segmentation Discussion Primers

Are there better ways to distinguish user-segments?

Are any key user-segments  
omitted / misrepresented / exaggerated?

## 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

## 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

## 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



# The Absolute-Minimum 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

# Beyond the Absolute-Minimum Safeguards

**Risk Assessment**, 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

## 4. Risk Assessment Discussion Primers

Is there any literature on the risks facing any of the key user-segments?

Are there any known risk management designs for any of the key user-segments?

Is there a grey literature in the corporate and/or government sectors?

## 5. Tools ... commonly called 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, hence accountability as well as freedom



**ELECTRONIC FRONTIER FOUNDATION**  
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

HOME

ABOUT

OUR WORK

DEEPLINKS BLOG

PRESS ROOM











# HTTPS Everywhere


**HTTPS  
Everywhere**

**FAQ**

HTTPS Everywhere is a Firefox, Chrome, and Opera extension that encrypts your communications with many major websites, making your browsing more secure. **Encrypt the web: Install HTTPS Everywhere today.**

From  
SSL/TLS  
to ...

Mobile	
	Android
	iOS
Computer	
	BSD
	GNU/Linux
	OS X
	Windows
Network	
	Routers
	Servers

**PRISM  BREAK** [Protocols](#) [About](#)

---

Opt out of global data surveillance programs like **PRISM**, **XKeyscore** and **Tempora**.

Help make mass surveillance of entire populations uneconomical! We all have a right to privacy, which you can exercise today by encrypting your communications and ending your reliance on proprietary services.



# the official **SECUREDROP** directory

SecureDrop is an open-source whistleblower submission system that media organizations can install to securely accept documents from anonymous sources. It was originally coded by the late Aaron Swartz and is now managed by Freedom of the Press Foundation. For more information, you can go [here](#).

**theguardian**



**SECUREDROP**

A way of sharing stories with us  
Securely & Confidentially

blackphone

Phone

# Introducing PrivatOS 1.1

In the Age of BYOD, privacy is essential to protecting your business infrastructure. PrivatOS 1.1 puts privacy in the hands of you and your enterprise, without any sacrifice to your productivity.



## Silent Text

Automatically encrypt your text messages. Includes Burn functionality, which destroys selected messages.



## Silent Phone

Makes private calls and video conferences more secure with an encrypted peer-to-peer VoIP service that operate worldwide with HD clarity over 3G, 4G or WiFi networks.



## Silent Contacts

Safeguard your contacts and leads by only providing you with access. Silent contact easily imports your address book with automatic encryption and password protection.

# Silent World

Silent World is a calling plan that provides you with enhanced security and flexibility on your mobile device. Simply buy minutes to make or receive calls between Silent Phone and regular mobile and landline numbers. Silent World's crystal-clear VOIP

Copyright  
2016



<https://silentcircle.com/>  
<https://blackphone.ch/silent-suite/>



Power to The People  
Encryption Makes the World Better




ESCAPE THE INTERNET®



## No rest for the Wickr: Turnbull's alternative to 'insecure' SMS

Although he's leading the charge for data retention, Malcolm Turnbull has argued that SMS is "insecure" and he prefers over-the-top messaging services -- services that won't be a part of the new laws.

by **Claire Reilly**  @reillystyley / 3 March 2015, 2:23 pm AEDT

Funnily enough, talk of his use of Wickr has seen a surge in people downloading it. Data from app analytics company App Annie shows the number of downloads in Australia surged in recent days, causing its ranking to go from 546th overall in Apple's App Store early Monday to 76th at time of writing on Tuesday.

<http://www.cnet.com/au/news/turnbull-says-over-the-top-messaging-superior-to-insecure-sms-whatsapp-wickr/>  
<http://www.smh.com.au/digital-life/consumer-security/minister-for-encryption-metadata-avoidance-app-wickr-shoots-to-top-of-charts-after-malcolm-turnbull-revealed-as-a-fan-20150303-13tgxy.html>

Copyright  
2016



# 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

# Criteria for Secure Messaging

EFF's Secure Messaging Scorecard  
<https://www.eff.org/node/82654>

But ...

It's in revision:  
<https://www.eff.org/secure-messaging-scorecard>

## 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**

# Categories of PETs – 3. Data Management

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

<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/>

<http://www.rogerclarke.com/DV/UPETs-1405.html#Cat>

# Categories of PETs

- **Communications**
  - ...
- **Traffic Management**
  - ...
- **Data Management**
  - ...

**Enormous Diversity, No Cohesion**



## Want a security starter pack?

Start from the beginning with a selection of simple steps.

Surveillance impacts all of us, no matter where we live or what we do. While some of us might be directly affected, others may simply want to know what measures they *can* take to protect their communications and data from spying. This introductory playlist will help you discover how to assess your personal **risk**<sup>①</sup>, protect your most cherished communications and information, and start thinking about incorporating privacy-enhancing tools into your daily routine.

1. Choosing Your Tools
2. Protecting Yourself on Social Networks
3. An Introduction to Threat Modeling
4. Communicating with Others
5. Creating Strong Passwords
6. Keeping Your Data Safe
7. What Is Encryption?



## 5. Tools

### Discussion Primers

Are there better, or complementary, classification schemes for PETs?

Are there examples of PET clusters?

Are there more exemplars of integration with systems and application software?



## 6. Design

- A Risk Management Strategy
- A Cohesive Tool-Set
- Integration with Systems Software
- Usability-Assured
- Architected

# 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

# 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

# PETs as Responses to Insecurity

## Data Obfuscation

- Disk Encryption

## Message Obfuscation

- EFF's 'HTTPS Everywhere'
- IAB / IETF Encryption as Default
- BlackPhone / PrivatOS / SilentSpace
- Wickr IM

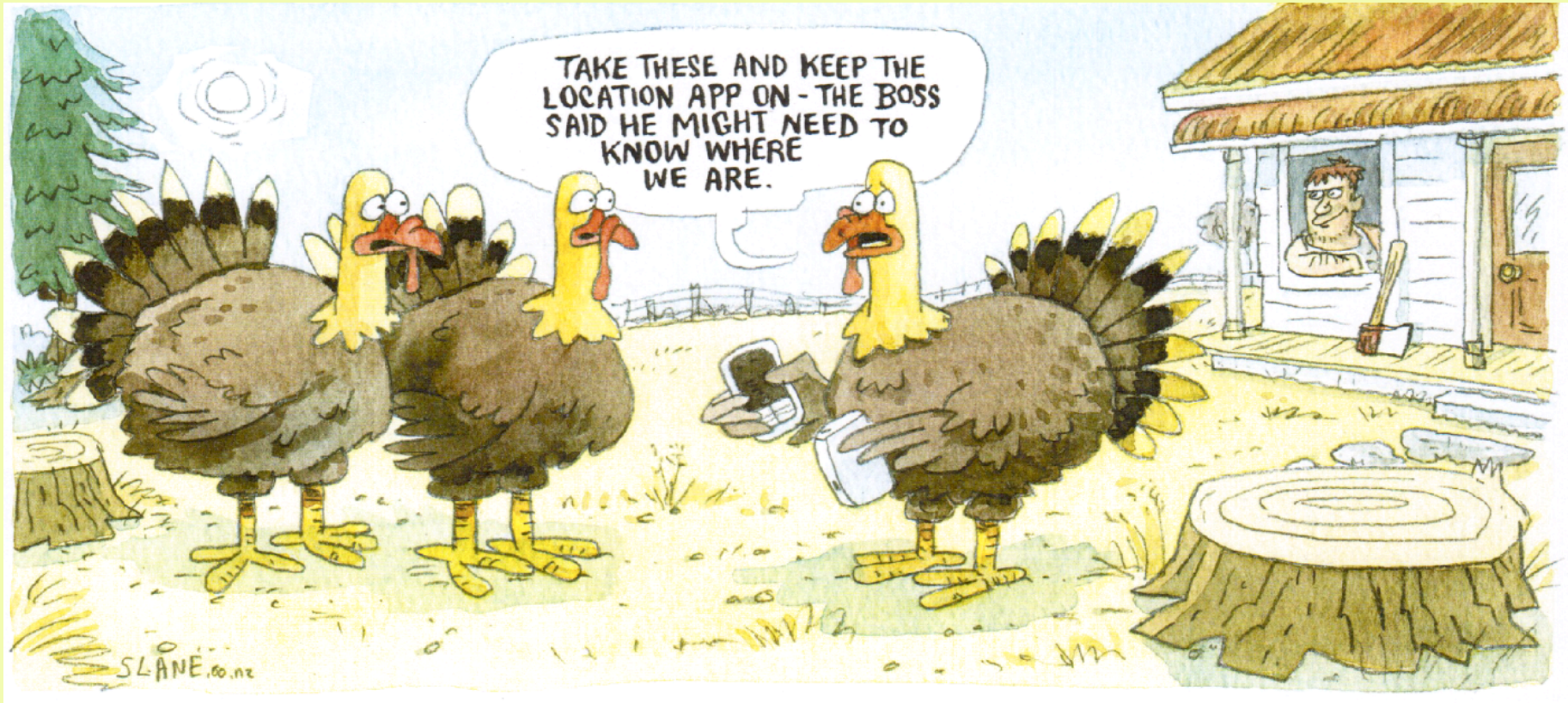
## Identity Obfuscation

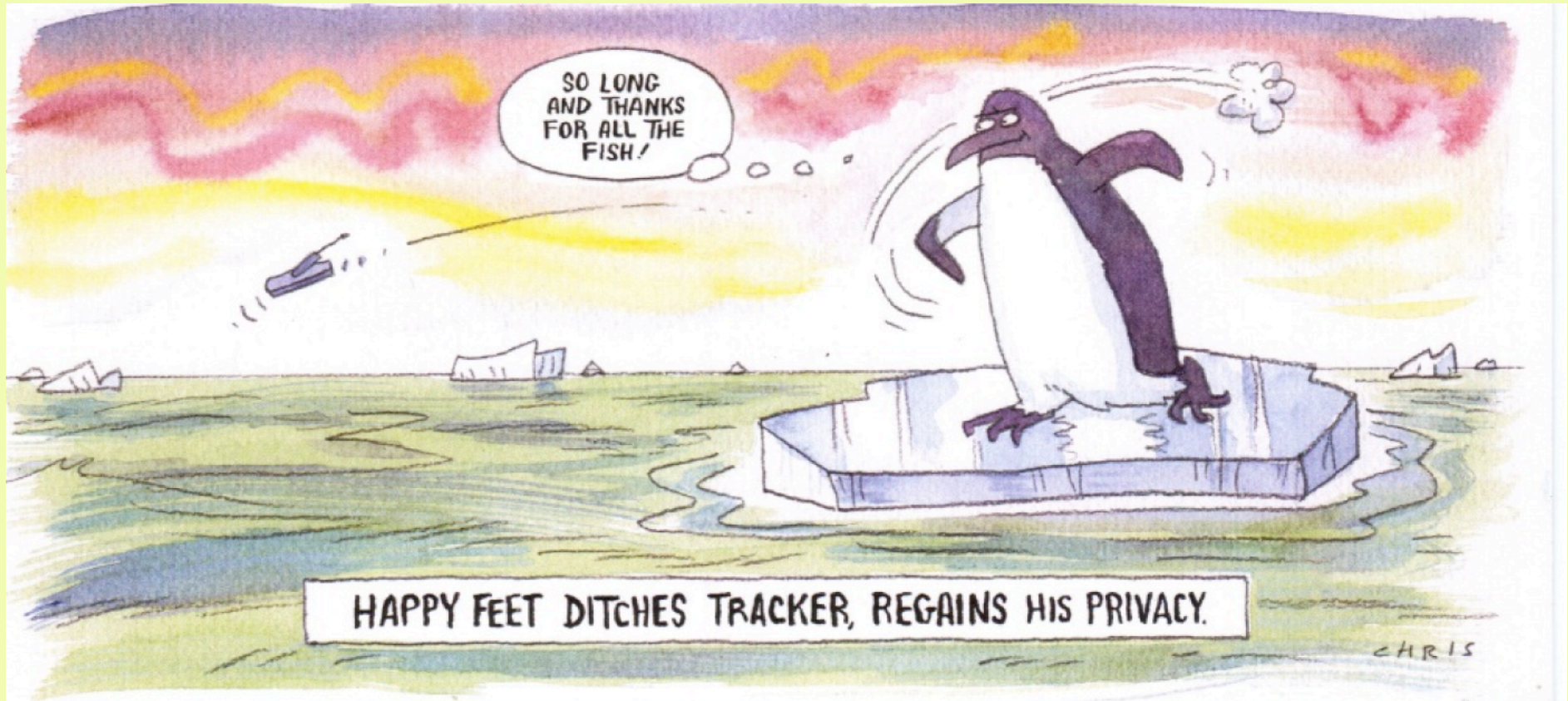
- PRISM-Break.org
- SecureDrop, GlobaLeaks

## Traffic and Social Network Obfuscation

- Tor







HAPPY FEET DITCHES TRACKER, REGAINS HIS PRIVACY.



# Privacy Design Strategies

	PRIVACY BY DESIGN STRATEGY	DESCRIPTION
1	Minimize	The amount of personal data should be restricted to the minimal amount possible (data minimization).
2	Hide	Personal data and their interrelations should be hidden from plain view.
3	Separate	Personal data should be processed in a distributed fashion, in separate compartments whenever possible.
4	Aggregate	Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.
5	Inform	Data subjects should be adequately informed whenever processed (transparency).
6	Control	Data subjects should be provided agency over the processing of their personal data.
7	Enforce	A privacy policy compatible with legal requirements should be in place and should be enforced.
8	Demonstrate	Data controllers must be able to demonstrate compliance with privacy policy into force and any applicable legal requirements.

Table 1: Privacy by design strategies [6]

Hoepman J.-H. (2014) 'Privacy Design Strategies'  
Proc. IFIP International Information Security Conference,  
2014, at <http://arxiv.org/pdf/1210.6621>

## Darkside Strategies

**Table 1. Privacy Strategies vs. Dark Strategies.**

Strategies	
Hoepman	Dark Strategies
MINIMIZE	MAXIMIZE
HIDE	PUBLISH
SEPARATE	CENTRALIZE
AGGREGATE	PRESERVE
INFORM	OBSCURE
CONTROL	DENY
ENFORCE	VIOLATE
DEMONSTRATE	FAKE

Bösch C. et al. (2016) 'Tales from the Dark Side: Privacy Dark Strategies and

Privacy Dark Patterns' Proc. PETS 2016 (4):237-254

[http://www.degruyter.com/downloadpdf/j/popets.2016.2016.issue-4/](http://www.degruyter.com/downloadpdf/j/popets.2016.2016.issue-4/popets-2016-0038/popets-2016-0038.xml)

[popets-2016-0038/popets-2016-0038.xml](http://www.degruyter.com/downloadpdf/j/popets.2016.2016.issue-4/popets-2016-0038/popets-2016-0038.xml)



# Usability Foundations

- 'Usability Engineering' (Nielsen 1993)  
Proposed 5 "usability attributes":  
**Learnability, Efficiency of Use, Memorability,  
Lowness of Error-Rate, Satisfaction**
- Human-Computer Interaction (HCI) theory
- User Interface (UI) design theory
- 'The Design of Everyday Things' (Norman 2000)
- ISO 9241-11 (1998), identified 4 key elements:  
**Effectiveness, Efficiency, Satisfaction, Learnability**

# Usable Security

- Whitten & Tygar (1999) tests (re PGP):
  - W1. Users are reliably made **aware** of the security tasks they need to perform
  - W2. Users are able to figure out how to successfully **perform** those tasks
  - W3. Users don't make dangerous **errors**
  - W4. Users are sufficiently **comfortable** with the interface to continue using it
- Garfinkel & Miller (2005) guidelines:
  - G1. Users should be **aware** of the steps they have to perform to complete a core task
  - G2. Users should be able to determine how to **perform** these steps
  - G3. Users should know when they have successfully **completed** a core task
  - G4. Users should be able to recognize, diagnose, and recover from non-critical **errors**
  - G5. Users should not make dangerous **errors** from which they cannot recover
  - G6. Users should be comfortable with the **terminology** used in interface dialogues, documentation
  - G7. Users should be sufficiently **comfortable** with the interface to continue using it
  - G8. Users should be aware of the application's **status** at all times
- Herzog & Ahahmehri (2007)
- Camp (2013)'s principles of 'translucent security':
  - C1: High security defaults
  - C2: Single-click override
  - C3: Context-specific settings
  - C4: Personalised settings
  - C5: Use-based settings

# User Interface Design for Privacy

EU-funded studies, oriented to the EU Directive:

- Patrick et al. (2002)  
(Chapter 12 of van Blarckom, 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/>

# PrimeLife Guidelines for Usable PETs (enhanced)

- H1. **Consistency** , i.e. common elements and processes
- H2. Feedback
- H3. Efficiency, including the avoidance of undue interruptions by privacy features of the task that is the user's primary focus
- H4. Flexibility
- H5. Clearly marked exits
- H6. Wording in the users' language
- H7. Control
  - X7A. Where a PET blocks or degrades a service, it must notify the user, and provide access to an explanation of the reasons why, and the options available
  - X7B. Users must have the following conveniently-accessible capabilities re the operation of a PET feature:
    - to 'suspend / resume' (i.e. an on-the-fly on/off switch)
    - to 'leave generally off, but apply to this transaction only'
    - to 'leave generally on, but override for this transaction only'
- H8. Recovery and forgiveness, i.e. an 'undo' button is always desirable
- H9. Minimization of memory load
- H10. **Transparency**, i.e. an explanation of the effect of each choice must be available
- H11. Aesthetics and emotional effect
- H12. Distinctiveness of remote vs. local handling of data
- H13. Internationalization, to accommodate different written, spoken and visual languages and cultural values
- H14. Support for informed and specific consent
- H15. **Privacy-friendly defaults**
- X16. Provide simplified **Profiles** that aggregate parameter-settings, which a user can select, and can customise

## 6. Design Discussion Primers

Does 'Obfuscation and Falsification' capture the key points?

Do Hoepmann's 'Privacy Design Strategies' provide a firm basis for progress?

Can you name specific PETs that are exemplars of those strategies, incl. usability?

## 7. Architecture

How the elements of the infrastructure fit together  
in order to deliver:

Cohesion within the tool-set  
and  
Integration with systems software

# 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

# Example: Architecture for Consumer-Oriented Social Media

- **Interoperability**
  - Content Openness  
(not a 'walled garden' / 'island')
  - Message Openness  
(to / from any email, chat / IM)
- **Portability**
  - Content Export-Import  
(profile, postings, messages)
- **Security**
  - Control over Messages,  
Traffic, Social Network, ...



# Example: Architecture for Consumer-Oriented Social Media

## plus: Decentralised Control

- **Client-Server**  
Centralised storage and control by the service-provider
- ... with Replication  
Multiple copies, but centralised control
- ... with Distribution  
Scattered storage, but centralised control
- **Peer-to-Peer (P2P)**  
All content and control on participants' own devices  
e.g. <http://tent.io/>
- **Semi-Peer-to-Peer (P2P)**  
Content and control scattered across many participant-controlled devices  
e.g. <http://jappix.org/why>

## 7. Architecture Discussion Primers

Are important architecture principles  
omitted / misrepresented?

## 8. Test Applications

### Example 1 – Web-Browser as Work-Horse

- Mainstream browsers such as IE, Firefox and Chrome are highly insecure and privacy-invasive
- Alternatives exist, e.g.
  - (Stripped) Chromium, WhiteHat Aviator, Tor Browser, Opera/VPN, ...
- They need to be evaluated and / or enhanced, and productised and distributed

## Example 2

# Consumer-Oriented Social Media (COSM)

- **Distributed Architecture**  
Probably P2P, 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

# COSM – Privacy-Sensitivity

## 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**

# Diaspora Features

- **Distributed Content and Control** (partial P2P)
  - Community 'Pods' (servers), or host-your-own
- **Interoperability** (emergent)
  - Public posts are open, public web-pages
  - Cross-posting – to Facebook, Twitter, Tumblr
- **Profiles** (all items optional)
  - Public Profile, open to the world
  - Private Profile, open to anyone in your Aspects
  - 'Aspect' (a poorly-conceived identity / persona, but merely a Group of other Diaspora users)

# COSM? – 'Federated Social Media' Talk-Fests

- **Federated Social Web Summit, Portland OR, Jul 2010 "Invite only. Implementers only"**  
[http://www.w3.org/2005/Incubator/federatedsocialweb/wiki/Federated\\_Social\\_Web\\_Summit\\_2010](http://www.w3.org/2005/Incubator/federatedsocialweb/wiki/Federated_Social_Web_Summit_2010)
- **Federated Social Web Europe, Berlin, June 2011**  
<http://d-cent.org/fsw2011/>
- **Federated Social Web Summit, SFO, 26 Oct 2012**  
**"Closed door but knockable"**  
[http://www.w3.org/2005/Incubator/federatedsocialweb/wiki/Federated\\_Social\\_Web\\_Summit\\_2012](http://www.w3.org/2005/Incubator/federatedsocialweb/wiki/Federated_Social_Web_Summit_2012)
- **Social Standards: The Future of Business, SFO, 7-8 Aug 2013**  
<http://www.w3.org/2013/socialweb/>
- **Social Web Standards, W3C Working Draft, 3 Jun 2016**  
<https://www.w3.org/TR/social-web-protocols/>

## 8. Test Applications Discussion Primers

Are privacy-friendly browsers readily available?

Are there readily-available ways to manage sensitive social networks?



## 9. Implementation – Demand-Side

### Innovations need Drivers, and face Impediments

#### Drivers

- **Perceived Need** – justified and/or delusive paranoia  
(RA: Threats, Vulnerabilities, Safeguards, Residual Risks)

#### Impediments

- **(Un)Awareness** – Why would I need one of those?
- **(In)Comprehensibility** – It does what? And why?
- **(Un)Installability** – How do I find it, get it (working)?
- **(Un)Usability** – How do I get it to do what I need?
- **(In)Convenience** – Does it interfere with my activities?  
& Is it integrated with what I use?

# 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

## 9. Implementation – Demand-Side Discussion Primers

Are there exemplars of successful PET innovations?

Can their features be carried over to other PETs?

# 10. Implementation – Supply-Side Technical Challenges

- Security is **Not Designed In** to devices, systems software or network infrastructure – it's always an add-on / retro-fit
- **Diverse Technical Contexts**, at hardware and OS levels, overlaid by multiple apps
- **Closed Technical Contexts**
- Categories of **Threats** are legion, and change continually
- Categories of **Vulnerabilities** are legion, and proliferate
- **Diverse Contexts of Use**
- High value is placed on **Convenience** (which is experienced continually) and low value is placed on security (experienced rarely)
- **Hedonism** undermines considered, reflective and responsible attitudes
- Security Features involve **Intrusiveness** into work and play & require understanding and concentration

# 'A New Digital Security Model'

- "In a highly-interconnected world, Perimeter Security / The Walled Fortress doesn't work any more"

- "The new Core Principle:

*"When-not-if unauthorised access happens, make sure that the data is valueless to anyone other than the user-organisation"*

# 'A New Digital Security Model'

## Some Implementation Techniques

- Obscure the content and identities  
(Only the user-organisation has the decryption-key)
- Use pseudo-identifiers not identifiers  
(Only the user-organisation has the cross-index)
- Split the content into 'small enough' morsels  
(Only the user-organisation has the whole picture)
- Authenticate attributes rather than identities

# Political Challenges

## The Public Sector Fear of the Public



# Economic Challenges Business Models

A Business Model  
is an Answer  
to the Question:

Who Pays?

For What?

To Whom?

And Why?



# Internet-Era Business Models

## Lessons from Open Source and Content

**WHO PAYS? For What? To Whom? And Why?**

- **Customers:**
  - for a Good or Service
  - for Complementary Goods or Services
- Providers
- **Third Parties – esp. Advertisers**
- **'A Fairy Godmother'**

# Open Content Business Models

## Who Pays? A Fairy Godmother

- **Subsidy / Patronage**

Funding from 'external' sources

Deprecated as a gift, unless 'market failure'

- **Cross-Subsidy**

Funding from 'internal' sources

Deprecated (but less so), because it's 'distortive'

- **Portfolio Approach**

Mutual Cross-Funding from 'internal' sources

How business works – 'cash cows' fund the rest

# Internet-Era Business Models

## Lessons from Open Source and Content

Who Pays? FOR WHAT? To Whom? And Why?

- **Goods & Services**
  - **Value-Added Goods & Services**
  - **Complementary Goods & Services**
- Data
  - Information
  - **Expertise / Knowledge**
  - An Idea in Good Standing
  - **Timeliness**
  - **Quality**

# Internet-Era Business Models

## Lessons from Open Source and Content

### Who Pays? For What? To Whom? AND WHY?

#### The Negative

- **Resource Control**
- **Switching Costs (capture, lock-in)**
- Grief Avoidance

#### The Positive

- **Perceived Value**  
(‘the genuine article’)
- **Cost Advantage**  
(incl. Time)
- **Quality Advantage**  
(incl. accuracy, security, timeliness, completeness, complementary services)

## Some Business Model Scenarios

- Consumers pay in cash rather than in data
- Consumers pay in cash for particular features, or get the service gratis in exchange for their data
- A corporation funds open-source software by selling customised / value-added versions and / or selling their expertise to support custom-builds
- A corporation provides gratis base-grade product, but offers more features in exchange for control over individual consumers' data
- A wealthy organisation or person funds product (whether a conservative, liberal or libertarian)

# Market Failure

- Tech, Ec, Pol Challenges are costly to address
- Business enterprises only invest if:
  - it's a cost of being in the game; or
  - it makes money
- SecLits assess risk dispassionately;  
but SecIllits judge risk spontaneously
- SecIllit Customers don't value security,  
and certainly not enough to pay for it
- Market mechanisms won't solve the problem
- The Security Gap won't be addressed without  
Market Intervention

## 10. Implementation – Supply-Side Discussion Primers

Are any technical challenges  
omitted / misrepresented / exaggerated?

Are any economic challenges  
omitted / misrepresented / exaggerated?

# The Workshop Format

0. Introduction to Topic and Purpose  
Segment Structure: Outline then Responses
  1. The Contexts of Insecurity
  2. Needs
  3. Segmentation
  4. Risk Assessment
  5. Tools
  6. Design
  7. Architecture
  8. Test Applications
  9. Implementation – Demand-Side
  10. Implementation – Supply-Side
99. Summary of Outcomes



# Summary

## A Strategy for Secure eWorking Environments

- 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

# Can We Productise Secure eWorking Environments?

**Roger Clarke**

Xamax Consultancy Pty Ltd, Canberra

Visiting Professor, UNSW Law

Visiting Professor, Computer Science, ANU

<http://www.rogerclarke.com/DV/SeWE16> {.html, .ppt}

**IFIP Summer School on Privacy & Identity Management**

Karlstad SE – 24 August 2016



# Drill-Down / Extra / Discard Slides

# Productisation of Secure eWorking Environments

## The Workshop Content

- Outline the contemporary context of insecurity
- Consider the needs of diverse user segments for Secure eWorking Environments
- Survey existing tools, note deficiencies
- Suggest requirements and architectural principles
- Discuss how comprehensive and integrated working environments can come into being

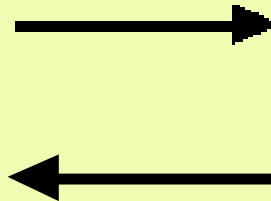
# Do we really know **NOTHING??**

- ASD (2013) 'Information Security Manual' ('**the ISM**') Defence / Australian Signals Directorate, August 2013, at <http://www.dsd.gov.au/infosec/ism/index.htm>
- ASD (2013) '**Strategies to Mitigate Targeted Cyber Intrusions**' Defence / Australian Signals Directorate, April 2013, at <http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm>
- DBCDE (2013a) '**Stay Smart Online – Business**' Dept of Broadband Communications and the Digital Economy, 2013, at <http://www.staysmartonline.gov.au/business>
- DBCDE (2013b) 'Stay Smart Online – Home Users' Dept of Broadband Communications and the Digital Economy, 2013, at [http://www.staysmartonline.gov.au/home\\_users](http://www.staysmartonline.gov.au/home_users)
- **RACGP (2013) 'Computer and Information Security Standards'** Royal Australian College of General Practitioners, 2nd Edition, June 2013, at <http://www.racgp.org.au/your-practice/standards/ciss/>

# Privacy-Sensitive Social Media Research Opportunities

## Social Science

- Distinguish positive and negative Drivers from Influencers
- Measure the Strength of Influencers, under varying scenarios
- Assess trade-offs between positive and negative Influencers, under varying scenarios
- Prioritise possible privacy-sensitive features



## Design and Prototyping

- Specify Desirable Features
- Architect:
  - for Client-Server
  - for P2P
- Design and Code Open-Source Components
- Establish a Test-Harness and / or Demo Apps
- Publish Reference Code
- Publish Demo Apps

# Privacy-Sensitive Social Media Research Opportunities

## Field Research

- Study Exemplars
- Study the Use of Exemplars
- Study Non-Use
- Identify User Categories
- Prioritise the various privacy-sensitive features



## Design and Prototyping

- Specify Desirable Features
- Architect:
  - for Client-Server
  - for P2P
- Design and Code Open-Source Components
- Establish a Test-Harness and/or Demo Apps
- Publish Reference Code
- Publish Demo Apps