COMP 2420 – Intro to Data Mngt, Anal & Security

2. Data Protection & Data Privacy

Roger Clarke
Xamax Consultancy, Canberra
Visiting Professor, A.N.U. and U.N.S.W.

http://www.rogerclarke.com/DV/Comp2420.html#L1
http://www.rogerclarke.com/DV/Comp2420-1 {.ppt, .pdf}

ANU RSCS – 12 May 2021

Data Protection & Data Privacy

1. **Introduction**
   - Data, Information
   - Data Sensitivities
   - Data Security
2. **Privacy**
   - The Concept
   - The Reasons
   - The Dimensions
3. **Data Privacy**
   - Threats across the Data Life-Cycle
4. **Safeguards**
   - Organisational
   - Legal
   - Technical (PETs)
     - Counter-PITs
     - Savage PETs
     - Gentle PETs

XAMAX Consultancy

Data

A symbol, sign or measure that is accessible to a person or an artefact

- Empirical Data represents or purports to represent a real-world phenomenon; Synthetic Data does not
- Quantitative Data gathered against Ordinal, Cardinal or Ratio Scales is suitable for various statistical techniques
- Qualitative Data gathered against a Nominal scale is subject to limited analytical processes
- Data is collected in a selective manner
- Data is collected for a purpose
- Data may be compressed at or after the time of collection, e.g. through sampling, filtering of outliers, averaging

Information

- **Information** is Data that has **Value**
- The value of Data depends upon **Context**
- The most common such Context is a **Decision**, i.e. selection among a number of alternatives

More Abstract Notions

- **Knowledge** is the matrix of impressions within which a human situates new Information
- **Wisdom** is the capacity to exercise judgement by selecting and applying Decision Criteria to Knowledge combined with new Information

Data Quality Factors

Assessable at time of collection

- D1 – Syntactic Validity
- D2 – Appropriate (Id)entity Association
- D3 – Appropriate Attribute Association
- D4 – Appropriate Attribute Signification
- D5 – Accuracy
- D6 – Precision
- D7 – Temporal Applicability

Information Quality Factors

Assessable only at time of use

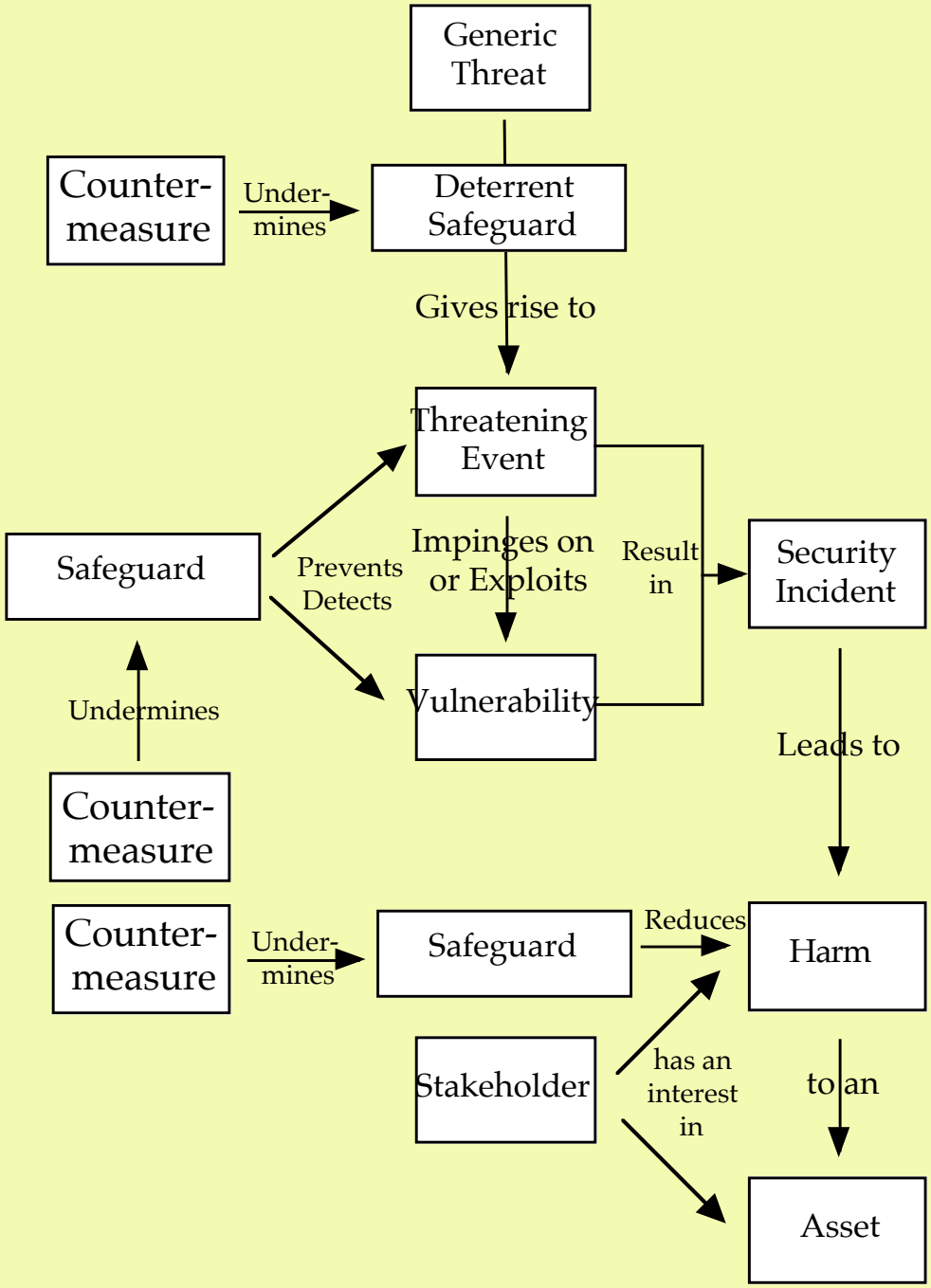
- I1 – Theoretical Relevance
- I2 – Practical Relevance
- I3 – Currency
- I4 – Completeness
- I5 – Controls
- I6 – Auditability

Data Sensitivities

- Commercial-in-Confidence
- Cabinet-in-Confidence
- Defence/NatSec Classifications
- Personal Data
  - Financial Services Data
  - Payment-Related Data
  - Health Data
  - Location Data
  - ...

XAMAX Consultancy

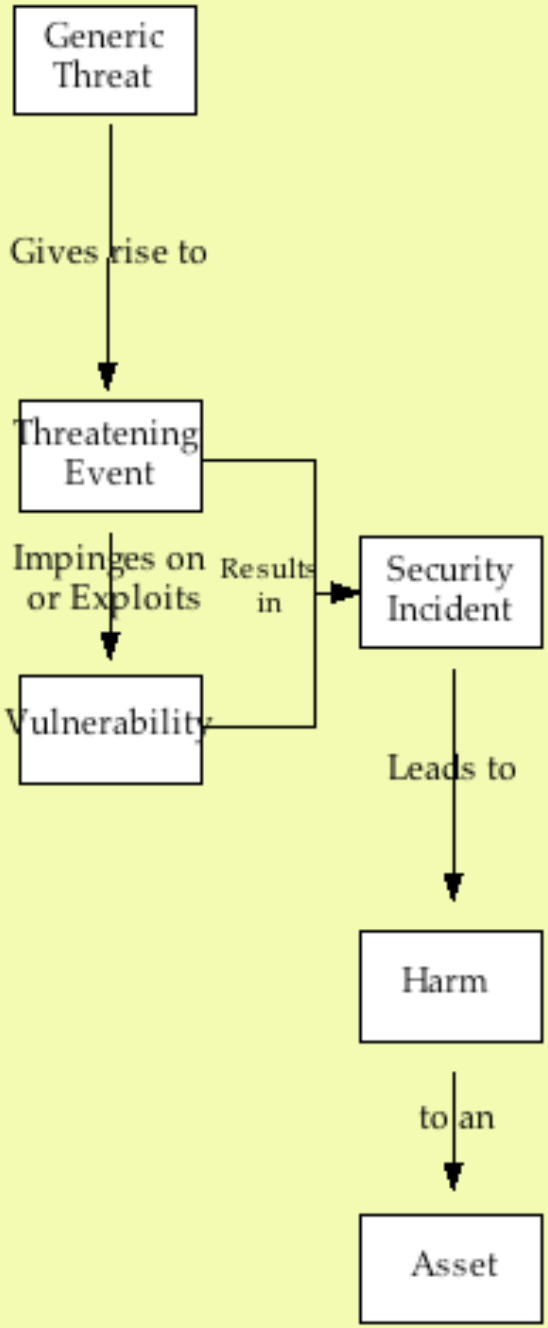
The Conventional Security Model



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

XAMAX Consultancy

The Conventional Security Model



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

XAMAX Consultancy

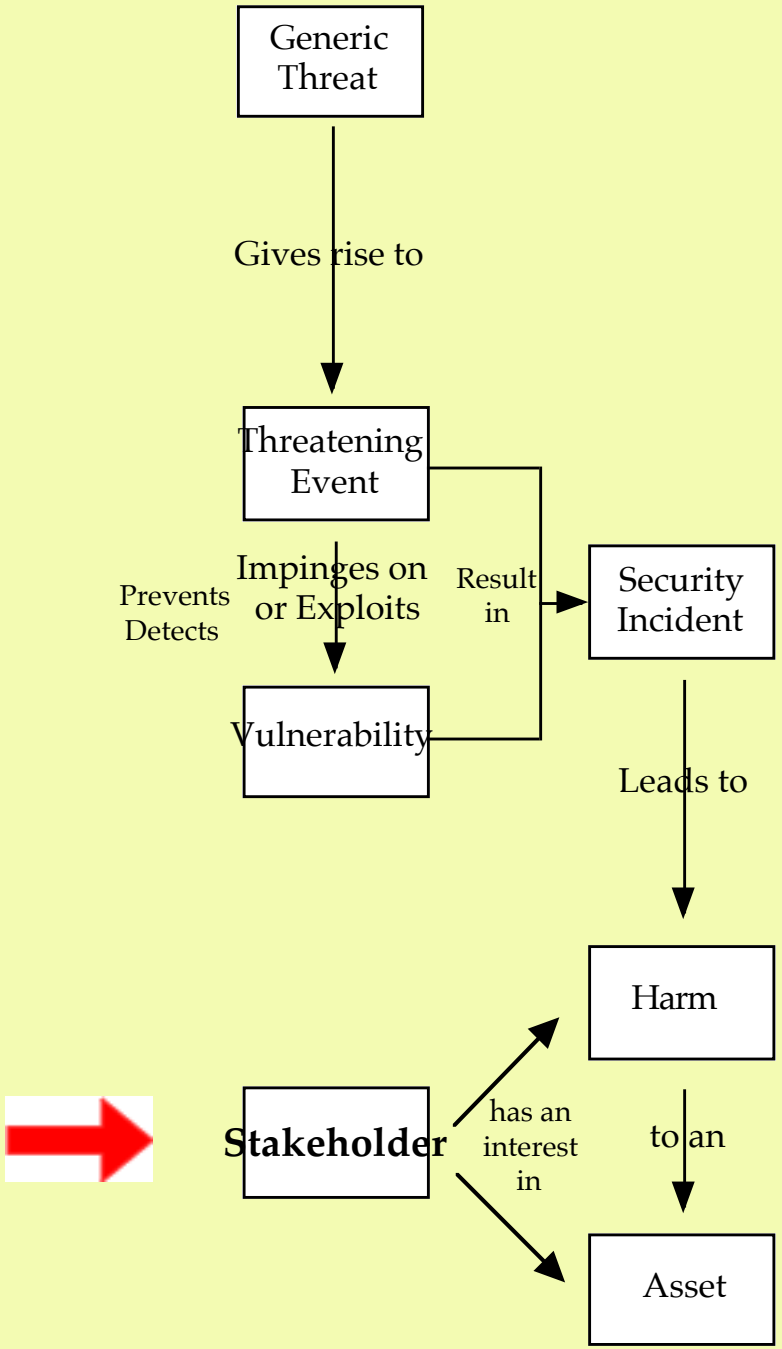
Categories of Threat

- **Environmental Events** (Acts of Gods or Nature)
- **Accidents**, caused by:
  - Humans who are directly involved
  - Other Humans
  - Artefacts and those Responsible for them
- **Attacks**, by:
  - Humans who are directly involved
  - Other Humans
  - Artefacts and Designers, Owners, Operators

Values Associated with Data that may be harmed by Data Analytics

- **Inaccessibility (Confidentiality)**
  - Data Access
  - Data Disclosure
  - Data Interception
- **Quality (Integrity)**
  - Data when Collected
  - Data when Used
    - Modification
    - Corruption
    - Staleness
- **Accessibility (Availability)**
  - Data Existence
  - Data Loss
    - In Volatile Memory
    - In Non-Volatile Memory
    - Theft, Destruction, Malfunction
  - Data Inaccessibility

The Conventional Security Model + Stakeholder

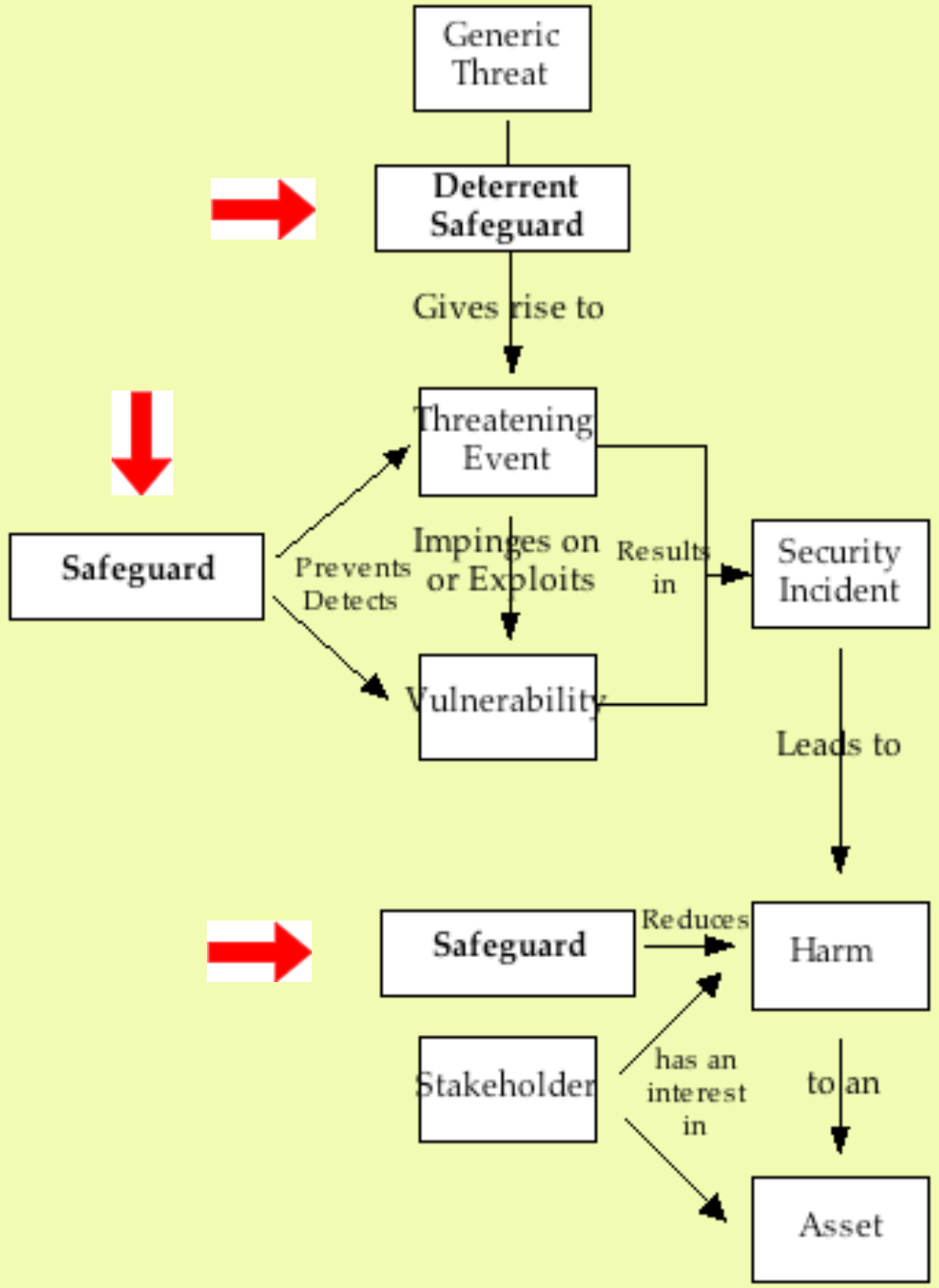


http://www.rogerclarke.com/EC/SSACS.html#App1

XAMAX Consultancy

The Conventional Security Model + Safeguards

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



XAMAX Consultancy

Locations of Security Risks

- 1st Person – Users, User Organisations
  Vulnerable Devices, Software & Infrastructure, User Threats

- 2nd Person – Their Business Partners, Service Providers
  Abuse, Vulnerable Storage, , Infrastructure, User Threats

- 3rd Person – Their Business Partners and Service Providers; Hackers
  Access
  Abuse, Vulnerable Storage, Infrastructure, User Threats

XAMAX Consultancy

But Many Organisations Create Insecurities

- **Insecurity by Design (IbD)**

  Consumer Devices are designed to be open to exploitation, for the benefit of marketers

- **Bring Your Own Device (BYOD)**

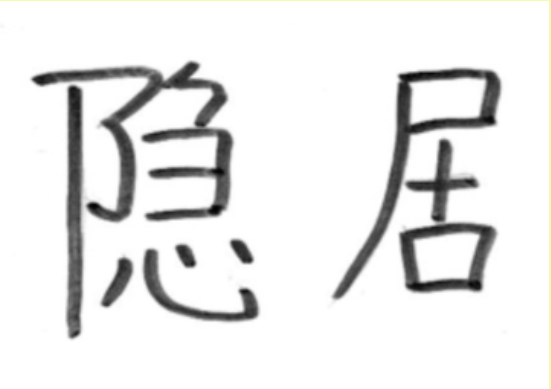
  So Consumer Device Insecurity is invited by organisations inside their firewalls

- **NatSec Agencies Want Access to Everything**

  e.g. TOLA / AA / DA legislation (legal authority to compromise devices and subvert end-to-end encryption)

2. Privacy

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



Very different from
Inaccessibility / 'Confidentiality' / Secrecy / Non-Disclosure

Harms arising from Privacy Breaches

- **Physical**
  Discovery of identity or location leads to assault and worse
- **Psychological**
  Closed doors, drawn curtains, 'jumping for joy'; loss of control over one's life, image, and respect, undermining social cohesion
- **Economic**
  Stifling of non-conformist, risk-taking, inventive and innovative behaviour, undermining cultural, scientific and economic change
- **Political**
  Embarrassments, stigmas; self-repression (the 'chilling effect'); political repression; a reduced pool of political contributors
- **Philosophical**
  Autonomy, self-determination, human dignity, personal integrity

XAMAX Consultancy

Why Privacy ?

- Human Dignity / Autonomy
- Political Needs
- Economic Needs / Asset Protection
- Social / Sociological Needs
- Psychological Needs
- Physical Needs / Safety

cf. the Maslowian Hierarchy of Needs

https://en.wikipedia.org/wiki/Maslow%27s_hierarchy_of_needs

http://www.rogerclarke.com/DV/Biel15.html#PM

Categories of 'Persons-at-Risk'

Ethical Issue: Data Exposure may be Life-Threatening

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

XAMAX Consultancy

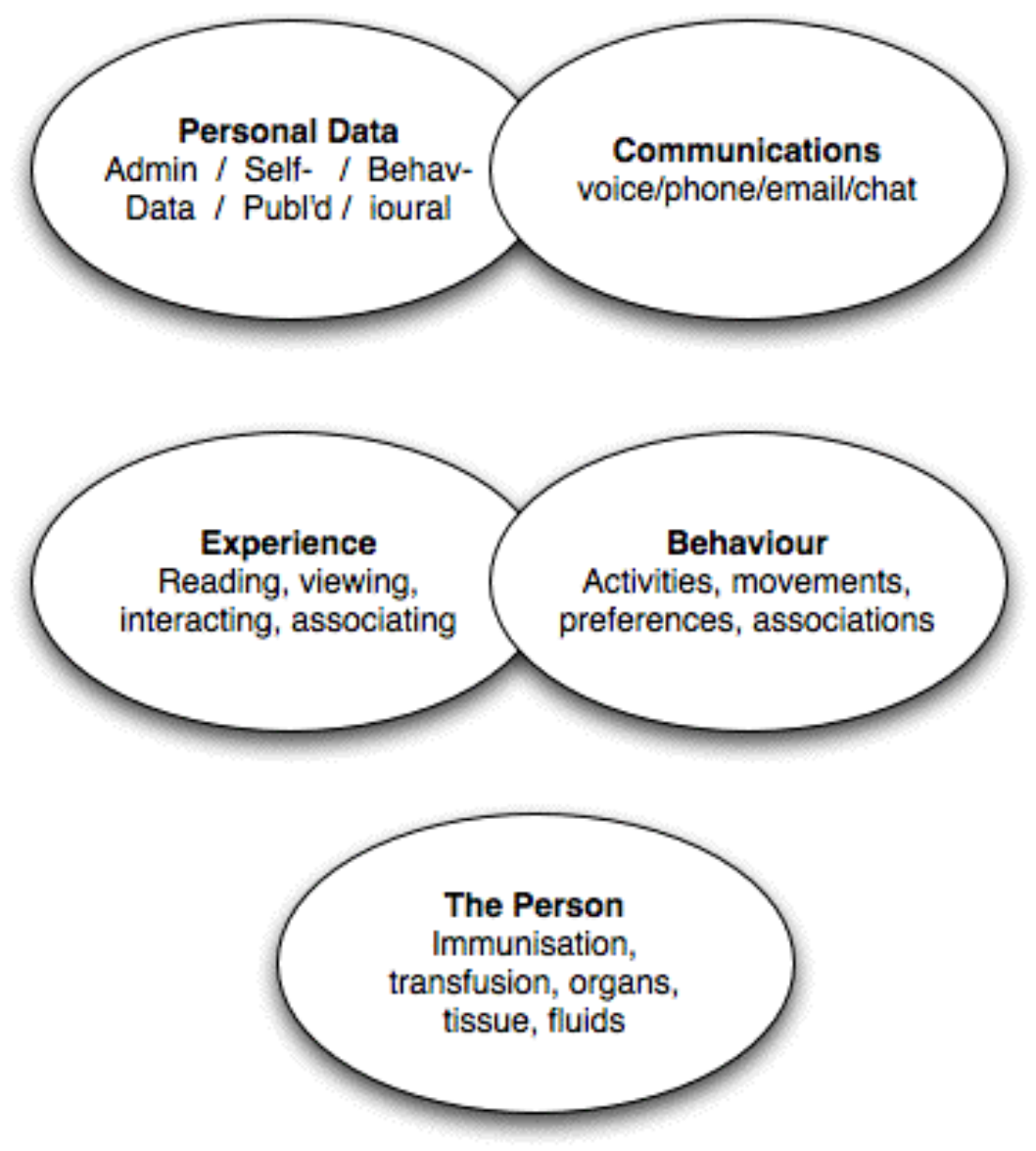
http://www.rogerclarke.com/DV/UPETs-1405.html#MS
http://geekfeminism.wikia.com/wiki/Who_is_harmed_by_a_%22Real_Names%22_policy%3F

Privacy Protection

- Privacy is one interest among many
- Privacy may conflict with other interests:
  - Personal conflict of interests
  - 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**

XAMAX Consultancy

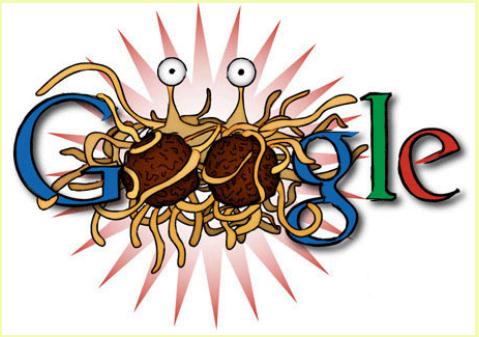
Privacy Dimensions



XAMAX Consultancy

http://www.rogerclarke.com/DV/Intro.html#Priv

3. Data Privacy

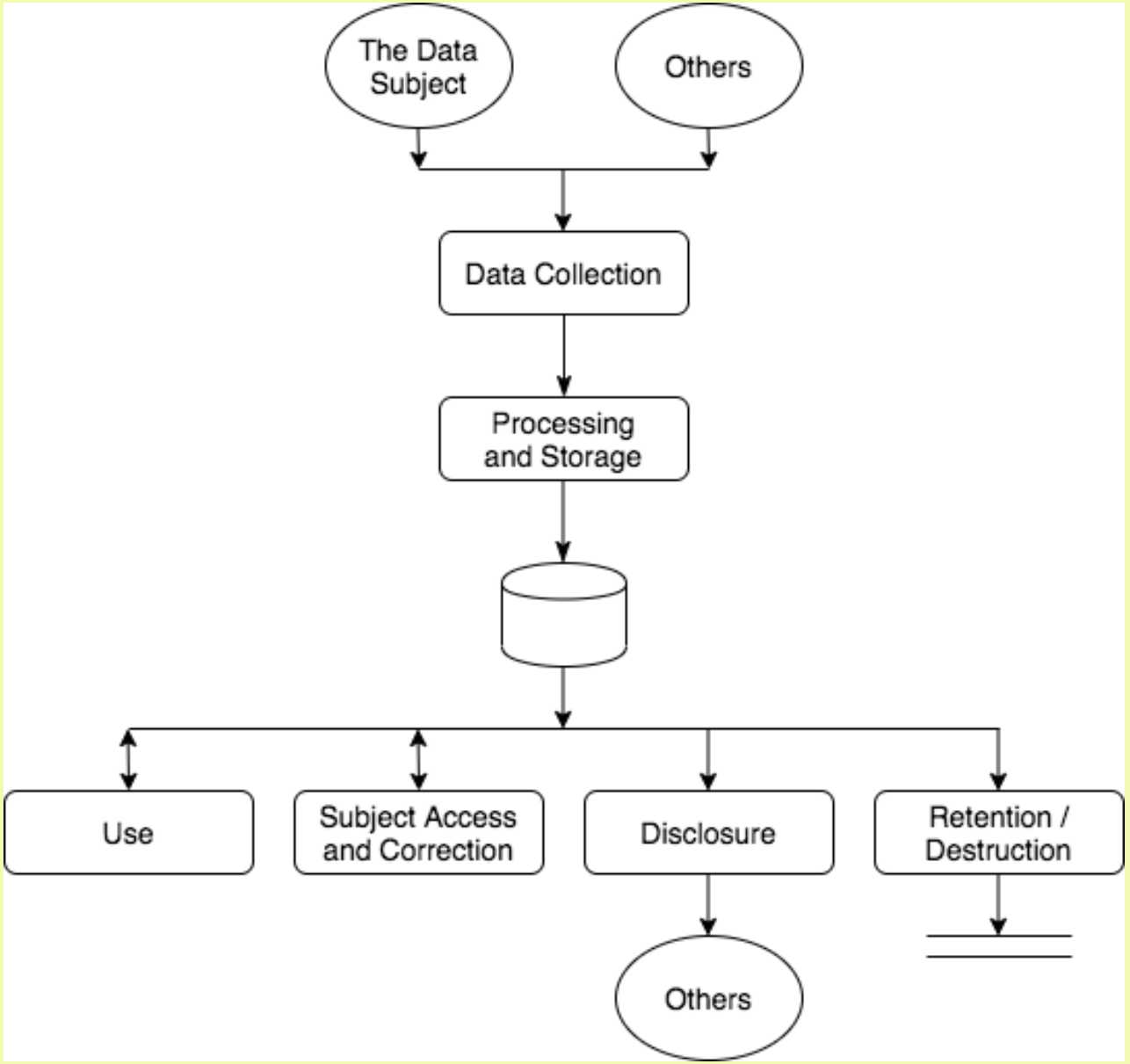


- **Data Privacy** is the interest that individuals have in controlling the handling of data about themselves
- **Communications Privacy** is the interest in communicating with others without monitoring or interception by others

- These underpin the other privacy dimensions:
  - Privacy of Personal Behaviour
  - Privacy of Personal Experience
  - Privacy of the Physical Person

XAMAX Consultancy

The Life-Cycle of Personal Data



XAMAX Consultancy

4. Data Safeguards

- **Organisational Safeguards**
  - Policies, Procedures, Practices
  - Training
  - Incident and Complaints Systems
- **Legal Safeguards**
  - Laws
  - Codes
  - Standards
  - Guidelines
- **Technical Safeguards**
  'Privacy-Enhancing Technologies' (PETs)

XAMAX Consultancy

Data Protection Laws

- **Statutory & Common Law Obligations**
  - Financial Regulations
  - Company Directors' obligations re asset protection, due diligence, business continuity, risk management
  - Security Treaty Obligations
  - Evidence Discovery Law
- **The Law of Confidence** specifically
  - Corporate Strategic and Commercial
  - Governmental
- **Contract**, incl. declared Terms of Service, and Conditions imposed on Contracts

Data Privacy Laws

- **OAIC (Private sector, Clth public sector)**
  Privacy Act (Cth)
  The Aust Privacy Principles (APPs)

- **NSWIPC (NSW public sector)**
  Privacy and Personal Information Protection Act 1998 (PIPPA)

- **VicPC / CPDP (Vic public sector)**
  Privacy Data and Protection Act

- **OICQ (Qld public sector)**
  Information Privacy Act

XAMAX Consultancy

http://www.privacy.org.au/Resources/PLawsClth.html
http://www.privacy.org.au/Resources/PLawsST.html

Privacy Act (Cth) and APPs

- The Australian Privacy Principles (APPs)
  https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference/ [And that's the shortened version!]

- The law is full of designed-in loopholes
- The law lacks specific guidance
  e.g. OAIC 'Guide to securing personal information' provides limited assistance, and sets no baseline
- The law is largely unenforced

The EU GDPR

- European General Data Protection Regulation (GDPR)

Data Breach Notification

- **2003-: US Laws**, to embarrass corporations into implementing adequate security safeguards
- **But** US laws failed to improve data security
- **2018-: Australian Laws**
  Privacy Act Part IIIC, ss.26WA-26WT
  Applies to some organisations, some breaches
  1: Contain the breach and do a preliminary assessment
  2: Evaluate the risks associated with the breach
  3: Maybe Notify affected individuals, the PC'er
  4: Prevent future breaches

http://www.rogerclarke.com/EC/DBNL-1211.html
https://www.oaic.gov.au/privacy/notifiable-data-breaches/
https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/

PITs and PETs

Privacy-Invasive and Privacy-Enhancing Technologies

- **PETs** have been worked on since 1995

- **Counter-PITs**, incl. protections for data in storage
  data in transit, authentication, ...
- **Savage PETs**
  for Persistent Anonymity

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

XAMAX Consultancy

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

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

Categories of PETs – 1. Communications

- **Encryption**
  e.g. SSL/TLS and HTTPS Everywhere
- **Email and Instant Messaging / Chat**
  e.g. Protonmail, Hushmail, Fastmail, Signal
- **Handsets**
  e.g. Silent Circle BlackPhone
- **Search-Engines**
  e.g. DuckDuckGo, Ixquick/Startpage
- **Browsers**
  e.g. Stripped Chromium, Brave, Tor, Onion, ...
- **Social Media Services**
  e.g. Diaspora

XAMAX Consultancy

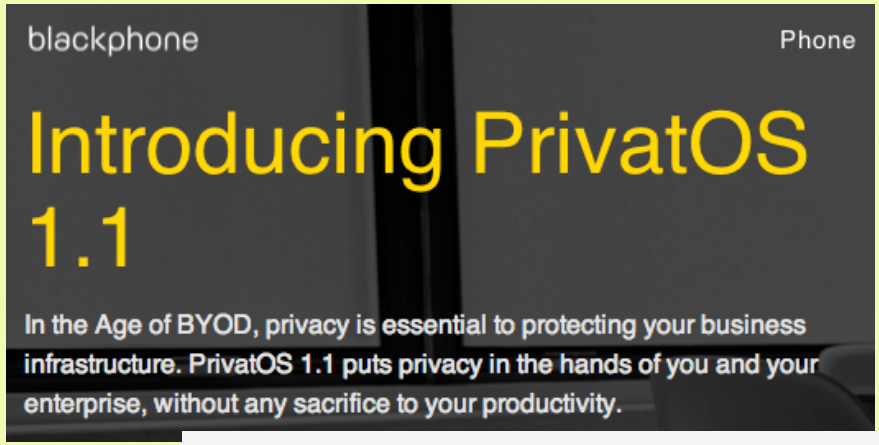
https://www.eff.org/Https-everywhere

Signal

- Text, voice, video, document, image traffic
- End-to-end encrypted
- Auto-Self-Destruct by Message
- Open Source, free-as-in-air & -beer
- Freemium / Premium Business Model

- For Handhelds, with
  Desktop/Laptop as slave

https://signal.org
https://support.signal.org/hc/en-us/sections/360001614191-Security-FAQ



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 Text

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

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

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

XAMAX Consultancy

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??

Categories of PETs

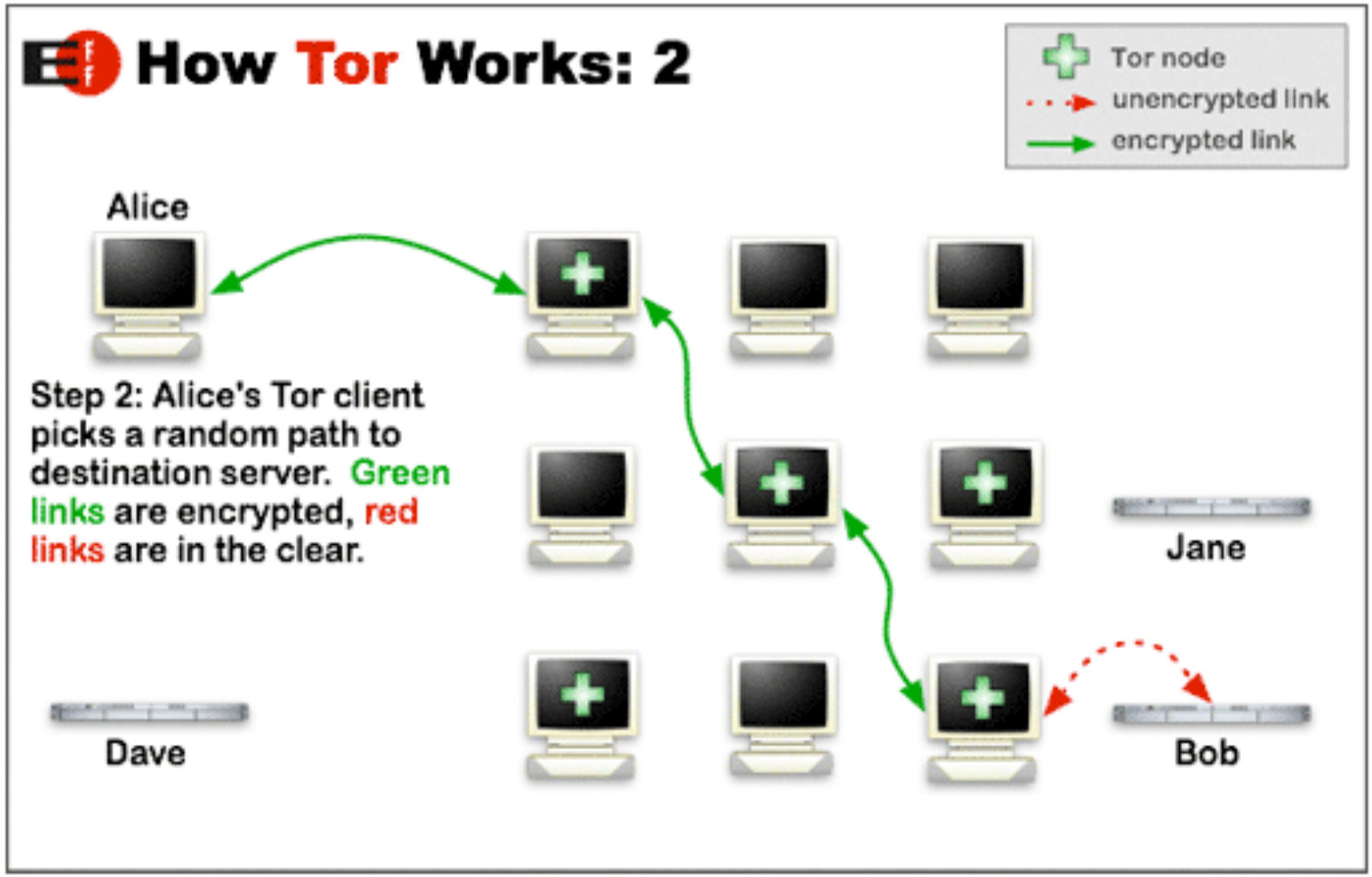
2. Traffic Management

- **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

XAMAX Consultancy



https://www.torproject.org/about/overview.html.en
http://www.rogerclarke.com/DV/Dredge-131105-WhatIsTor.pdf

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

ABC NEWS

Crikey.

The Sydney Morning Herald

XAMAX Consultancy

https://securedrop.org/overview/
https://www.abc.net.au/news/securedrop/

Data Protection & Data Privacy

1. **Introduction**
   - Data, Information
   - Data Sensitivities
   - Data Security
2. **Privacy**
   - The Concept
   - The Reasons
   - The Dimensions
3. **Data Privacy**
   - Threats across the Data Life-Cycle
4. **Safeguards**
   - Organisational
   - Legal
   - Technical (PETs)
     - Counter-PITs
     - Savage PETs
     - Gentle PETs

XAMAX Consultancy

COMP 2420 – Intro to Data Mngt, Anal & Security

2. Data Protection & Data Privacy

Roger Clarke
Xamax Consultancy, Canberra
Visiting Professor, A.N.U. and U.N.S.W.

http://www.rogerclarke.com/DV/Comp2420.html#L1
http://www.rogerclarke.com/DV/Comp2420-1 {.ppt, .pdf}

ANU RSCS – 12 May 2021