Erasmus Research Centre for Media, Communication and Culture

A secure city for private citizens

Jason Pridmore (pridmore@eshcc.eur.nl)

Thelma Arnold

- AOL Searches
  - Numb fingers
  - 60 single men
  - Landscapers in Lilburn GA
  - Dog that urinates on everything

”Eve”

- Consumption Purchases:
  - Overweight
  - Concerned about appearance
  - Poor complexion
  - Long hair
  - Wears contacts, glasses occasionally
  - Numerous problems with feet
  - Has hay fever
  - Plans holiday gifts and cards well in advance

Oligopticon Effect

Cannot see everything, but what you can see, you can see very well

Ethical Issues

- Two questions for us
  - How do we maintain data security?
  - How to ensure the personal privacy of our citizens?

- Four interrelated statements
  - Implications for practices

1. There is no such thing as personal data (on its own)

Data is only personal in relation to other data

Implications

What connections are made?
How do these create a unique set of circumstances that may put those identified at risk?

2. Every manifestation of digital practices is unique.

Each instance carries its own set of risks and opportunities because of how these interconnections are made

Privacy by Design Principles

1. Proactive not reactive: preventative not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality: positive-sum, not zero-sum
5. End-to-end security: full lifecycle protection
6. Visibility and transparency: keep it open
7. Respect for user privacy: keep it user-centric

Security by Design Principles

1. Minimize attack surface area
2. Establish secure defaults
3. Principle of Least privilege
4. Principle of Defense in depth
5. Fail securely
6. Don’t trust services
7. Separation of duties
8. Avoid security by obscurity
9. Keep security simple
10. Fix security issues correctly

Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Implications

Consider your context unique, while learning from previous experiences regarding your data security challenges and privacy concerns

3. Complete data security is impossible.

It is always dependent on the weakest link in the data security chain.

Implications

Identify vulnerabilities without prejudice towards or against technology or people

How a problem is defined already presupposes a particular answer to that problem.

Technological solutions are always developed in relation to a particular way of defining the problem.

Implications

Rethink your definitions and approach. What opportunities does this afford? What potentials does this close off?