Ethics in Networked Systems Research

Ethical, Legal and Policy Reasoning for Internet Engineering

Plan

- Talk about privacy and ethics
- Discuss & present exercise, groups of 4

  → Break

- 45 mins for exercise in groups
- 45 mins discussion with all

Human subject research?

- Collecting personally identifiable data
- Human subject research
  - Medical, social science, psychology, etc.
  - Relatively strict and broadly-understood ethical traditions
- Internet engineering
  - Consideration of these issues is relatively new,
  - Not obvious whether existing best practices from other fields can be successfully imported.
  - Wrong: "Privacy = security"

Internet as socio-technical system

- Society & technology have become intertwined
- Internet is the technical backbone for modern society
- Measuring data flows = measuring behaviour (often)
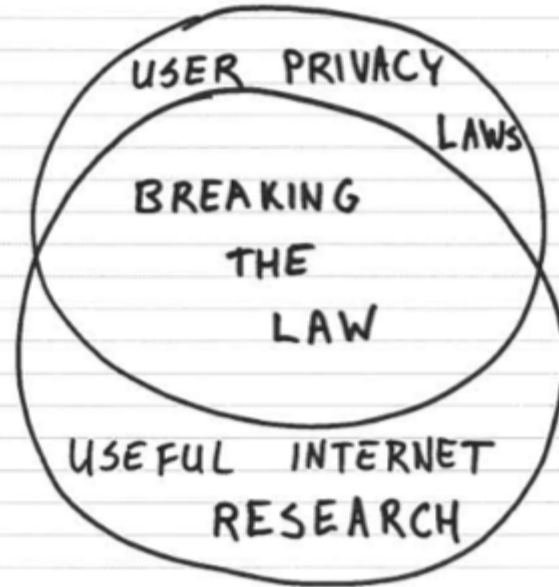
Information privacy theory

Subset of the broader concept of privacy, focuses on the **access and use** of information regarding people.

The claim of persons *"to **determine** for themselves when, how, and to what extent information about them is communicated to others"* (Westin 1967).

Since Westin more narrow definitions focussed on:

- information privacy risk,
- information control and awareness or
- transparency of processing

Information privacy theory constantly **evolves** with the introduction and implementation of new information technologies.

Privacy harms

- Identity theft
- Blackmail
  - Also incriminating information by chance
- Decisions based on databases and algorithms
  - Inaccuracies
  - Lack of transparency = black box for users
- Power relations (and potential misuse)
  - Affect behaviour and sense of freedom

Contextual integrity (Nissenbaum)

- Violation of information privacy can occur when information moves across contexts…
- *Context-relative informational norms*, where the flow and use of specific information is considered to be inappropriate
  - Actors (subject of information, capacity of recipient and power-balance with regards to the sender);
  - Attributes (data types of information);
  - **Transmission principles (constraints under which information flows).**

Nissenbaum explains that these parameters should be imagined to be

"[…] juggling balls in the air, moving in sync: contexts, subjects, senders receivers, information types, and transmission principles."

Laws can be confusing/outdated

- For example: Google/Spain,
  - Right to be Forgotten

Existing law and policy

- Even when relevant policies do exist,
- They are often ambiguous or inadequate
- As the were **designed for times with a less versatile technology** than computing.

Policy vacuums

- The **malleability** of computer allow them to be used in novel ways,
- Ways for which we frequently do not have formulated policies for controlling their use,
- Advancing computer technology produces policy vacuums in its wake.

Conceptual muddle

- Need an analysis which provides a **coherent conceptual framework** within which to formulate a policy for action.
- First understand how different disciplines understand their conceptual framework - identify opportunities for translation.

Task of ethics:

A basic job of computer/information ethics to:

- **identify** these policy needs,
- **clarify** related conceptual confusions,
- **formulate** appropriate new policies,
- and ethically **justify** them.

Computer ethics:

- The analysis of the nature and **social impact** of computer technology and,
- The corresponding **formulation** and **justification** of policies for the ethical use of such technology.

  - (Moor 1985)

Ethics muddle

- Consequentialism
  - *Just* consequentialism
- Deontology
- Virtue ethics
  - *By design in machines/software*?
- Feminist ethics
  - Emancipatory ethics?

Aim of project

- To develop guidelines,
- For internet engineering research,
- Which will act as a proxy for Internet engineering more generally,
- To act as a bridge in translation between disciplines & expertise.
- Get involved: ensr.oii.ox.ac.uk

Setting community standard

Working with:

- Computer scientists
- Network engineers
- Philosophers
- Lawyers
- Social scientists
- Science, Technology & Society (STS)

Ethics and morality

- Facts
  - What practices and methodologies do we determine to be "objective," and what do we determine to be "anecdotal" or "subjective"?
  - What values and modes of thinking are embedded in these assumptions?
- Values
  - What values frame our research questions/engineering projects? Do we believe the Internet is good? Do we believe fast is better? Do we want access everywhere? What uses and identities to we imagine when we imagine an Internet User? What does this include and exclude?

Internet as socio-technical system

1) Internet designed by a **homogeneous** group

- Created standards last for a very long time
- Use has extended these beyond original purpose
  - Can be easily exploited (e.g. wifi snooping)

2) Access to the Network is **democratised**

- Recognise Internet is a diverse socio-technical system.
- Increasingly difficult to measure the effect of the Internet on the lives of its users.

Trade-off benefits and harms

- Problem **defining** risk
  - What is bad? How bad is it? In what way?
  - Not necessarily to individuals, but to groups,
  - Need exists for research on the negative consequences of Internet research.
- Problem **identifying** risk
  - Assessment difficult in changing/dynamic environment of the Internet,
  - Risks materialise in the long term - related benefits are immediate,
  - Harms are dependent on socio-economic & political context of the user.

Responsibilities of stakeholders

- Inherent knowledge & power imbalance
  - Data subjects and,
  - Technically literate researchers and orgs.
- Relevant social norms often not understood by engineers
- Do not underestimate agency of people
  - But people can be overconfident.

Informed consent

- Users
  - Are uninformed & lack agency
- Informed consent is meaningless if:
  - No intuitive understanding of personal data ecosystem,
  - No technical understanding of their devices.
- Problem
  - One document to speak to all users
  - Risk identification cannot be exhaustive

Privacy by Design

- Information privacy design can be designed by applying an interdependent **construct** of
  - technical tools,
  - legal agreements and,
  - project governance to the information system (Bennett & Raab 2006).
- This requires a **sophisticated approach** whereby the combination of Transmission Principles used can vary greatly depending on the project, the type of data collected and their intended purpose (Altman et al. 2014).

Transmission principles

- ## Technical
  - *"a system of ICT measures protecting informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system"* (van Blarkom et al. 2003)
- ## Legal
  - Informed consent and data sharing agreements.
- ## Organisational
  - Access limitations, privacy audits, etc.

(Privacy) Impacts assessments

- Methodology is a process (Clarke 2009; Clarke 2014),
- Used proactively during the design of a project (Oetzel & Spiekermann 2013),
- Which serves to **identify** and **assess** information privacy risks and to **take remedial actions** to mitigate or minimise **negative effects** (Wright 2013)

Download Guidelines

http://tinyurl.com/GuidelinesOII

E.g.

- Rich information, data subjects identifiable (through linking with public data), longitudinal purposes, "spray and pray", etc.:
  - Interactive dissemination methods (differential privacy, managed access)
  - + appropriate k-anonymity levels
  - + enforcing sharing agreements.

- Low info sensitivity, data minimization at collection, add synthetic data:
  - Go for open data!

Your ethics issues

- Have you experienced ethics dilemmas?
- How did you mitigate the situation?

Ethics exercise

- 13 groups of 4
- Internet measurement project
  - First, ideal data collection - no ethics
    - Design together - blue sky scenario
  - Then - iterate the discussion"
    - 2 people become ethics board and scrutinise
    - Other 2 people address the concerns
- Exercise document: http://goo.gl/KOvFRQ

Example topics

- Passive censorship measurements worldwide via mobile phones.
- Quantify social network access trends in a university dataset and looking into fluctuations in the performance
- Predict the gender and relationship status of a student at an institution based on their online shopping patterns.
- Net neutrality measurements in Cataluña using Telefonica network (with permission from company engineers)
- Collecting Wifi and Bluetooth probes to map social networks and social spaces within a university
- Collecting Tweets with a specific hashtag where people express outrage and argue online

Coming months

- Internet Science conference, 27 May, Brussels.
- Connected Life conference, 4 June, Oxford
- CEPE-IACAP 2015 Symposium 22-24 June 2015, Delaware.
- Citizen Lab Summer Institute, 24-26 June, Toronto.
- ACM SigComm, 21 August, London.
- Amsterdam Privacy Conference, October 2015.
- Internet Governance Forum, November 2015, Brazil.