Privacy by Design
The "Whole System" Approach

Dr A. A. Adams

School of Systems Engineering

University of Reading

PRISE Conference

29th April 2008

Overview

- Cost/Benefit Analyses

- Security Theatre

- The Misuse Question

- The Abuse Question

- The Re-purposing Question

- People as Part of the System

Cost/Benefit Analyses

- Security Myth: "Saving one life is worth any cost"

- Security Reality: Trades between safety and other benefits are made every day: e.g. speed limits

- Privacy and Security are not a zero-sum game.

- Individual privacy is a significant part of personal security.

- Mission Creep and Scope Creep must be considered in the design, implementation, deployment and oversight of systems.
  e.g.: London Congestion Charging, UK nationwide traffic monitoring.

Security Theatre

- Security Myth: Making citizens *feel* safer is a security goal.

- Security Reality: Security theatre can easily undermine real security by:

  - Diverting resources from real security

  - Making staff feel secure and therefore less conscientious

  - Making citizens feel more secure and therefore less reactive

- Better to clean the streets than deploy CCTV if the aim is to make citizens feel safer.

- Is the goal, prevention, detection, resource deployment control, investigation, evidence?

The Misuse Question

- Who will buy security systems?

- Automated identification of coalescing group: use by oppressive regimes (c.f. sale of internet filtering technology by US to China)

- Can security technology be used by criminals to scrutinise targets?

- Can security technology be applied to commercial surveillance?

- Can security technology be applied to trivial offences (c.f. RIPA powers and school place applications)

The Abuse Question

- Individual abuse: e.g. sexual voyeurism by CCTV operators

- Group abuse: e.g. shopping malls tracking/ejecting "hoodies".

- Official abuse: mission-creep/scope-creep

- Political abuse: technological determinism; "seen to be doing some-
  thing"

- Commercial abuse: over-selling (facial recognition); unfit for purpose
  (who decides the purpose, evaluates fitness, makes cost/benefit analyses)

The Re-Purposing Question

- Aeroplane security: applied to buses and trains, e.g. knife ban on the Eurostar

- PIA and similar processes should consider other purposes and provide recommendations on suitability, different design concepts, etc. when re-purposing may occur

- When will Western Society re-normalise? Are we in a permanent "emergency"?

- As society re-purposes, security technology must be re-scrutinised

People as Part of the System

- Deployment decisions: made by whom, reviewed by whom, regulated by whom?

- Maintenance

- Regulation of access

- Imbalance of power

- Embedding of bias

- General social norms

Conclusions

- The Whole System must be considered: the whole system is Society

- Regulation must be by independent, well-financed experts

- Scrutiny of aims, objectives and methods must be as public as possible

- Re-purposing of systems, mission creep and scope creep require further scrutiny

- Right of appeal must be embedded in the system

- Technological determinism must be avoided (large- and small-scale)

- Cost/Benefit analyses must be clear and broad

- "None sing hymns to privacy," said Yama. "But, oh to be without it!" (with apologies to Roger Zelazny)

- Emotional single-case appeals should be seen as cynical manipulation (e.g. Jamie Bulger, Sharon Beshenivsky)