

# Exploiting engineering ingenuity to protect personal privacy

Martyn Thomas CBE FREng



The Royal Academy  
of Engineering

# The Role of The Academy



- The UK's national academy
- Priorities:
  - Enhancing national capabilities
  - Recognising excellence and inspiring the next generation
  - **Leading and informing debate**
- Recent report: *Dilemmas of Privacy and Surveillance*

# Most people need privacy sometimes

- You may need to conceal your ...
  - Age, HIV status, addiction, mental illness, religion, politics, past traumas (e.g. rape), race/ethnicity, previous gender, sexual orientation, disability, employer, criminal record, previous identities, address ...
- For reasons such as ...
  - Risk of discrimination, escaping abusive relationships, witness protection, avoiding ID fraud, concealing pre-take-over company investigations, protecting celebrities, statutory requirements (e.g. protecting the identity of children in court cases or following adoption) ... ..



# Dilemmas of Privacy and Surveillance



- Privacy v Accountability
- Privacy v crime detection and prevention
- Privacy v efficiency of service delivery
- Privacy v *authentication* (e.g for age restricted goods)
- Privacy v Social Good (e.g. infection)

# Technology to Protect Privacy

- Don't *identify* if you can merely *authenticate*
  - E.g. the pay-as-you-go Oyster Card (if always bought with cash). Or a proof of age card with a photo but no name.
- Encourage multiple identities
  - A research scientist at Huntingdon Life Sciences is also Jane and Johnny's mother and a counsellor for *Relate*. She needs these lives to be kept separate. Good engineering design can achieve this.
- For example, road user charging need not identify the car or the driver. If identification is needed for other reasons, that should be a separate decision.



# Design for privacy

**Encryption** is a basic *disconnection technology* (it prevents data from being used without the key-holder's consent)

- Encrypt private data with the key of the legitimate user, so that no-one can use it without their consent
- System keys can enable *electronic shredding*
- Private data is complex and layered, the data design and encryption needs to be the same
- Data *anonymisation* is difficult and may be impossible without destroying the value of the data

# Privacy in Web 2.0

- Information posted to (e.g.) social networking sites may be preserved for ever – and may be used at any time in the future by abusers, employers, the media ...
  - “cooling off” delay between posting and publishing?
  - Use of digital rights technology to protect individuals?

# Anonymous Surveillance

- Image recognition systems are being developed that can recognise the signs of a possible crime
- Such systems will enable surveillance cameras to ignore most of what they see, and greatly reduce the privacy impact
- More research is needed



# ID “cards”

- An ID token could be anything – a watch or mobile phone, say.
- Consumer goods could be linked to the token, so that (e.g.) your car, PC or TV will not start unless your ID token is nearby.
  - Combined with encryption/DRM, this could make the data on a lost or stolen PC inaccessible.

# Recommendations

- Be precise about the amount of personal data required – it is probably far less than you first think.
  - Authenticate rather than identify if possible.
- Use multiple identities to keep roles separate.
- Use disconnection technologies to control the availability and persistence of private data.
- Use anonymous surveillance where possible.



# Further Details

This is just a summary. The Royal Academy of Engineering report contains a technology roadmap, analysis of possible scenarios, a discussion of trust, profiling and reciprocity, and many more recommendations.

See:

[http://www.raeng.org.uk/news/publications/list/reports/dilemmas\\_of\\_privacy\\_and\\_surveillance\\_report.pdf](http://www.raeng.org.uk/news/publications/list/reports/dilemmas_of_privacy_and_surveillance_report.pdf)