3012/GC25 Interaction Design
Privacy

Miguel Malheiros

by Chris Slane
Contents

• What is privacy?
• Dimensions of privacy
• Data Protection Act 1998
• Social Networking
• What is personal data?
• People’s views of privacy
• Designing for privacy
• Exercise
• Discussion
What is privacy?

• Limited access to personal space or information

• Control over your personal information

• Intimacy and moral capital
Dimensions of privacy

• Bodily privacy
  – e.g.: drugs testing; DNA sampling; strip searches

• Territorial/behavioural privacy
  – e.g.: CCTV; home searches; trespass

• Personal communications privacy
  – e.g.: wiretapping; mail interception; internet surveillance

• Information privacy
  – e.g.: collection of personal data; transfer of personal data between organisations
Dimensions of privacy

- **Data Subject**
  - Surveillance
  - Interrogation

- **Information Collection**
  - Intrusion
  - Decisional Interference

- **Data Holders**

- **Information Processing**
  - Aggregation
  - Identification
  - Insecurity
  - Secondary Use
  - Exclusion

- **Information Dissemination**
  - Breach of Confidentiality
  - Disclosure
  - Exposure
  - Increased Accessibility
  - Blackmail
  - Appropriation
  - Distortion
Data Protection Act 1998 (DPA)
Information Commissioner’s Office

• Personal information must be:
  – Fairly and lawfully processed
  – Processed for limited purposes
  – Adequate, relevant and not excessive
  – Accurate and up to date
Data Protection Act 1998 (DPA)
Information Commissioner’s Office

• Personal information must be:
  – Not kept for longer than is necessary
  – Processed in line with the individual’s rights
  – Secure
  – Not transferred to other countries without adequate protection
Data Protection Act 1998 (DPA)
Information Commissioner’s Office

- Individual’s rights:
  - Accessing information
  - Correcting information
  - Preventing processing of information
  - Preventing unsolicited marketing
Data Protection Act 1998 (DPA)
Information Commissioner’s Office

• Individual’s rights:
  – Preventing automated decision making
  – Claiming compensation
  – Investigating breach of act

• http://www.ico.gov.uk
What is personal data?
Data Protection Act

• “Data which relate to a living individual who can be identified from those data”.
  – E.g.:
    • name
    • address
    • DoB

• Sensitive personal data:
  – E.g.:
    • racial or ethnic origin
    • political opinions
    • religious beliefs
Firm 'sold workers' secret data'

A company that allegedly sold workers' personal details, including union activities, to building firms is to be prosecuted by the information watchdog.

The Information Commissioner's Office (ICO) said the Consulting Association, in Droitwich, had committed a "serious breach" of the Data Protection Act.

The ICO said a secret system had been run for over 15 years to enable firms to unlawfully vet job applicants.
Social Networking
Information Commissioner’s Office

• http://www.ico.gov.uk/youth.aspx
Facebook remark teenager is fired

A 16-year-old girl from Essex was fired after she described her office job as "boring" on her Facebook page.

Kimberley Swann, 16, of Clacton, had been working at Ivell Marketing & Logistics, in Clacton, for three weeks before being fired on Monday.
What is personal data?
Different view

• Facts, communications, or opinions

• Relate to the individual

• He or she would regard as intimate or sensitive
People’s views of privacy

- Not binary
- Layers of sensitivity
- Not static
- Individually identifiable data ≠ privacy invasion
People’s views of privacy

![Diagram showing the relationship between context, user, information sensitivity, information receiver, and information usage. The diagram illustrates how the user assesses risk/benefit and trust in the context of information usage and sensitivity.](image)
People’s views of privacy

• Risks
  – Secondary level information
  – Future usage
  – Lack of feedback
  – Privacy invasion \rightarrow Technology rejection

• People trade risks for benefits
Designing for privacy

• Issues
  – Privacy not user’s main goal
  – Many types of users
  – Usability impact bigger in privacy applications
  – Update mechanism
Designing for privacy

• Risks
  – Obscuring potential information flow
  – Obscuring actual information flow
  – Emphasizing configuration over action
  – Lacking coarse grained control
  – Inhibiting established practice
Designing for privacy

![Internet Options window](image)

- **Medium**
  - Blocks third-party cookies that do not have a compact privacy policy
  - Blocks third-party cookies that save information that can be used to contact you without your explicit consent
  - Restricts first-party cookies that save information that can be used to contact you without your implicit consent

- **Pop-up Blocker**
  - Prevent most pop-up windows from appearing.
  - Turn on Pop-up Blocker
Designing for privacy
Exercise

Introducing Google Latitude

See where your friends are on a map

Start using it on your phone
See your friends' locations and status messages and share yours with them.

Enter your number or visit google.com/latitude on your mobile web browser.

Will it work with my phone?
Google Latitude is a feature of Google Maps for mobile on these phones:

- Android-powered devices, such as the T-Mobile G1 (coming soon)
- iPhone and iPod touch devices (coming soon)
- most color BlackBerry devices
- most Windows Mobile 5.0+ devices
- most Symbian S60 devices (Nokia smartphones)
- many Java-enabled (J2ME) mobile phones, such as Sony Ericsson devices (coming soon)

Fred wants to hang out with his friends, and checks to see where they are.
Exercise
Google Latitude

Sharing request
Privacy settings
User profile
Exercise
Google Latitude

• Useful links:
  – Google Latitude
    http://www.google.com/mobile/default/latitude.html
  – Mobile Privacy Policy
    http://www.google.com/mobile/privacy.html
  – Location Privacy
    http://google.com/support/mobile/bin/answer.py?answer=136654&topic=20061
  – Privacy Settings
    http://google.com/support/mobile/bin/answer.py?answer=136650&topic=20061
Discussion & Questions
Summary

- What is privacy?
- Dimensions of privacy
- Data Protection Act 1998
- Social Networking
- What is personal data?
- People’s views of privacy
- Designing for privacy
- Exercise
- Discussion