

Data Protection

Outline Schedule

| | Topic |
|------------------|------------------------|
| Lecture 1 | IT Profession |
| Lecture 2 | Data Protection |
| Lecture 3 | Freedom of Information |
| Lecture 4 | Computers and the Law |
| Lecture 5 | Software and the Law |
| Lecture 6 | IT workers and the Law |
| | Revision |

Data Protection Acts

First Act passed in 1984

By mid-1990s problems included online capture of personal data via cookies etc, junk email – “spam”

European Directive on Data Protection leading to

- 1998 Data Protection Act
- Privacy and Electronic Communications (EC Directive) Regulations 2003

Privacy

European Convention on Human Rights states:

“Everyone has the right to respect for his private and family life, his home and his correspondence”

Led to UK Regulation of Investigatory Powers Act 2000

Freedom of Information

Public pressure for greater openness by UK
Government

Demand for access to Government
information led to

Freedom of Information Act 2000
but that is the next lecture

Data Protection Act 1998

Key player is the Office of the Information Commissioner

Runs an excellent informative web site on Data Protection

<http://www.ico.gov.uk/>

Data Protection Act - Concepts

Data – information being processed automatically or collected with that intention or part of a relevant filing system

Data Controller – “person” who determines who or how personal data is processed

Personal data – data about a living person who can be identified from the data possibly used with other data the Data Controller may have

Data Protection Act - Concepts

Data subject – individual who is subject of personal data

Sensitive personal data – data about racial or ethnic origins, political opinions, religious beliefs etc

Processing – obtaining, recording or holding data or carrying out any operation on it

Data Protection Act - Principles

1. Personal data shall be processed fairly and lawfully and in particular shall not be processed unless (a) data subject has given their consent and (b) for sensitive data has given their *explicit* consent

Failing to tick an opt-out box is not sufficient for (a) and for (b) processing and any possible disclosure must be explained

Data Protection Act - Principles

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 those purposes

Data Controllers must tell the Information Commissioner what data they are collecting and the purpose for which it is being collected

Data Protection Act - Principles

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

Data cannot be collected that is not needed, for example shops collecting customers addressing when not delivering goods

Data Protection Act - Principles

4. Personal data shall be accurate and, where necessary, kept up to date

Very difficult. Universities are often not told of changes of address by students and it is very difficult for the university to update its records

Data Protection Act - Principles

5. Personal data processed for any purposes shall not be kept for longer than necessary for those purposes

Retention periods must be determined for all data.
Auditors require data kept for 7 years, civil court actions can start up to 6 years after an event being complained of

Data (including backups) must be deleted at the appropriate time

Data Protection Act - Principles

6. Personal data shall be processed in accordance with the rights of the data subjects

Data subjects have a right to know:

- Description of data being held

- Why it is being held and processed

- People and organisations to whom it may be disclosed

- Intelligible statement of data held about them

- Source of the data

Data subjects also have a right to:

- Prevent processing likely to cause damage and distress

- Prevent processing for direct marketing

- Compensation for damage caused by unlawful processing

Data Protection Act - Principles

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

Data Protection Act - Principles

8. Personal data shall not be transferred to a country outside the EEA unless the country ensure an adequate level of protection for the rights and freedom of data subjects in relation to the processing of their personal data

This both protects an individual against having personal data transferred to countries lacking appropriate legislation while expressly permitting organisations to export data to countries that do

Privacy and Electronic Communications (EC Directive) Regulations 2003 regulate:

Telecommunication network and service providers and individuals :

- use of publicly available electronic communications services for direct marketing purposes
- unsolicited direct marketing activity by telephone, by fax, by electronic mail (this means text/video/picture messaging and email) and by automated calling systems

Telecommunication network and service providers only:

- processing of electronic communications traffic data
- location data and billing data
- calling or connected line identification
- directories of subscribers
- security of telecommunications services and the use of cookie type devices

Prohibits unsolicited phone calls, texts, emails for direct marketing without the prior permission of the recipient

Complaints can be made to Information Commissioner but ...

Difficult to enforce if caller/sender is outside EEA

Dear Roger,

Wednesday 22 February 2006



energy saving trust™

How will you save your 20%?



If you save just 20% of the energy you use every day you'll help prevent climate change.

We all use energy every day - at home, at work and when we travel. To generate that energy, we burn fossil fuels (coal, oil and gas) that produce 'greenhouse' gases - in particular carbon dioxide (CO₂) - which are changing the climate and damaging our environment.

There are simple steps you can take to make your home more energy efficient (for example, insulating your home or buying energy saving recommended appliances) reducing your home's carbon dioxide emissions and saving you up to £250 a year on your energy bills.

To find out how you can save your 20% [play our interactive board game?](#)

Play our interactive board game for your chance to win a digital camcorder



You have received this email because you have agreed to receive marketing messages by email from Telegraph Group Limited, its group of companies or The Spectator (1828) Limited.

If you no longer wish to receive emails about Telegraph products and services please [use this link to be removed from this mailing list](#) Please note that we will no longer be able to send you updates about the site or your subscriptions.

If you no longer wish to receive emails from the Telegraph, about the products of carefully selected companies then please [use this link to be removed from this mailing list](#)

In accordance with the 1998 Data Protection Act, Telegraph Group Ltd is committed to protecting your privacy. If you wish to know more please access our [privacy policy](#).

Ethical Email

Note

1. Personally addressed
2. Explains why it is being sent and who by
3. Explains how to remove myself from their list
4. Gives access to their privacy policy

Regulation of Investigatory Powers Act 2000

The Act regulates interception of postal system, telecommunication and digital communications

Not surprisingly it is long and complicated

Some examples will illustrate its scope

Regulation of Investigatory Powers Act 2000

(Examples courtesy of JISC)

Example 1

Mr A, a private detective, installs a home-made phone tap on a British Telecom line to intercept Mr B's telephone calls.

This interception is intentional and without lawful authority. It is a criminal offence.

Example 2

Mr A, a private detective, installs a home-made phone tap on a line in the internal phone system of the University of Bumbleside, which is connected via a PBX switchboard to the British Telecom network, to intercept Mr B's telephone calls.

This interception is intentional and without lawful authority. It is a criminal offence.

Regulation of Investigatory Powers Act 2000

(Examples courtesy of JISC)

Example 3

Mr C, a staff member of the University of Bumbleside Computer centre, illicitly uses system privileges on the University computer network, which is connected to the Internet via JANET (the UK's Education and Research Network), to intercept interesting emails sent by Mr D, a member of the University. Mr C does not have the express or implied consent of the person with a right to control the relevant private telecommunication network (the University).

This interception is intentional and without lawful authority. It is a criminal offence.

Example 4

Mr C, a staff member of the University of Bumbleside Computer centre, acting on a memo from the Vice-Chancellor of the University uses system privileges on the University computer network, which is connected to the Internet via JANET, to intercept interesting e-mails sent by Mr D, a member of the University. Mr C has the express or implied consent of the person with a right to control the relevant private telecommunications network (the relevant officer of the University).

This is not a criminal offence. However, unless the relevant officer of the University has lawful authority to require the intercept, Mr D may be able to sue the University.

Regulation of Investigatory Powers Act 2000

Example 5

The University of Bumbleside Alumni Office wishes to conduct phone solicitations of former students (who have consented to their data being used for this purpose). It monitors staff phone calls to Alumni to ensure that staff adhere to correct procedures, including data protection rules, and for future staff training purposes.

Both staff and Alumni should be informed that calls may be monitored and /or recorded.

Example 6

The University of Bumbleside suspects that certain user accounts are being used to commit computer misuse offences. It monitors user accounts that display suspicious behaviour.

Users should be informed that this monitoring/recording may take place; this can be done through the University's Regulations and Guidelines and reinforced by registration documentation, login warnings and stickers on equipment.

Regulation of Investigatory Powers Act 2000

Example 7

The University of Bumbleside has reason to believe that its computer facilities are being misused to send unsolicited commercial emails. It monitors user accounts it suspects of being used to send such messages.

Users should be informed that this monitoring/recording may take place; this can be done through the University's Regulations and Guidelines, and reinforced by registration documentation, login warnings and stickers on equipment.

Example 8

The University uses certain logging mechanisms to ensure the efficient functioning of its email systems. The logging mechanisms allow authorised staff to access and monitor the use of user accounts as an incidental part of that logging.

Users should be informed that this monitoring/recording may take place; this can be done through the University's Regulations and Guidelines, and reinforced by registration documentation, login warnings and stickers on equipment.

Summary

Citizens are entitled to know that information about them will be used only for the purposes for which they gave it
Data Protection Act 1998 gives this protection

Citizens' right to "privacy" is protected by Privacy & Electronic Communications Regulations 2003

Privacy of communication from unreasonable intrusion is provided by the Regulation of Investigatory Powers Act 2000