Legal Issues

Relevant areas of legislation

Intellectual Property (IP) rights

Copyrights; patents; trademarks; brands; and secrets

Copy*left:* Creative Commons; GNU Public Licences

Contract law

Data Protection and Freedom of Information

Data Protection Act 2018 (subsumes GDPR);

Product liability and negligence

Computer misuse

Computer Misuse Act 1990; Police and Justice Act 2006; Regulation of Investigatory Powers Act 2000

Data Protection and Freedom of Information

Original UK **Data Protection Act 1984**, then **1998**, now superseded by the **Data Protection Act 2018**, which includes the European General Data Protection Regulation (**GDPR**)**.**

Gives an individual rights regarding information about themselves.

Freedom of Information Act 2000 (equivalent Scotland Act was in **2002**).
Gives right to access information held by public authorities.

Privacy and Electronic Communications Regulations came into force on **11 Dec 2003**. It concerns electronic marketing and the confidentiality of electronic data traffic.

GDPR Data Protection Principles

Personal data shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals **'lawfulness, fairness and transparency' ;**
2. Collected for specified, explicit and legitimate purposes and not use for other unrelated purposes **'purpose limitation'**;
3. Adequate, relevant and limited to what is necessary **'data minimisation';**
4. Accurate and kept up to date **'accuracy'**;
5. Not kept any longer than necessary **'storage limitation'**;
6. Processed and kept securely **'integrity and confidentiality'**.

7. Additionally, data controllers are required to be responsible for complying (and demonstrating compliance) with the first 6 principles.

GDPR Rights for individuals

Individuals have the following rights regarding their personal data:

1. **Right to be informed** about how their data is collected and processed**;**
2. **Right of access**: can find out what personal data is held about them;
3. **Right to rectification:** can ask for corrections to errors in the data held;
4. **Right to erasure**, or **right to be forgotten**: can ask for data to be deleted;
5. **Right to restrict processing**: can ask to limit the ways their data is used;
6. **Right to data portability:** can access and transfer data for their own use;
7. **Right to object**: can ask organisations to stop processing their data;
8. **Rights in relation to automated decision-making and profiling**.

GDPR: what's new?

- **Increased territorial scope:** any company *anywhere in the world* must comply with GDPR if it is processing the personal data of persons ("data subjects") who are in the EU.
- **Increased penalties:** 4% of annual turnover or € 20 Million (greater of these)
- **Consent:** Much stricter conditions for obtaining consent from data subjects
- **Expanded rights for data subjects**:
  - Data breaches must be notified within 72 hours
  - Improved right to access; new "right to be forgotten" and "data portability"
- **Stronger requirements for security and compliance** ("privacy by design", designated data protection officers)
- **GDPR is included in the UK's 2018 Data Protection Act.**
  - The UK act also has some additional aspects specific to the UK.

Information Commissioner

Job of the **Information Commissioner's Office** is to ensure that there are data protection safeguards to ensure that the information that is collected about us is not misused.

They deal with:

- Data Protection Act 2018
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003
- Environmental Information Regulations 2004.

Freedom of Information Act

This came into force in 2005.

Means that **the public has right to access information held by public authorities** – obvious conflict with data protection.

One result is that a lot of **information is no longer held** by these bodies.
(If you no longer hold the information, then you do not have to respond to a request for it.)

Requests can be refused if they cost more than £600.

Computer Misuse Act

The UK **Computer Misuse Act** came into force in **1990**. Three new criminal offences were introduced.

1. **Unauthorised access** (including *attempted* access) to computer material. The penalty is up to **6 months** in prison. This covers **simple** hacking and is an offence even if nothing is changed.

2. **Unauthorised access** with intent to commit or facilitate commission of **further offences**.This covers situations for example where the material obtained was used to access a person's bank account.

3. Unauthorised **modification** of computer material. This covers issues such as planting **viruses**, malicious **deletion** of files or **altering bank account** details.

The penalty for 2. or 3. is an **unlimited fine** and **up to 5 years** in prison.

Computer Misuse Act

One area where it is deemed to be ineffective is **denial of service** (DoS) attacks where a target computer is saturated with external requests and so cannot carry out its proper function.

There have been court cases in the UK in the last couple of years trying to prosecute perpetuators of denial of service attacks under the Computer Misuse Act, but they have not been successful.

Various proposals in the last few years to update the Computer Misuse Act in this area, e.g. **Police and Justice Act 2006**.

New laws

Police and Justice Act 2006 introduces new offences concerned with “impairing the operation of a computer” including making and distributing hacking tools.

This is to help deal with the **DoS** problem.

Problem is that some of these tools are produced legally for **penetration testing** and identifying **vulnerabilities**.

Proposal therefore includes features such as **intent** - always a problem area.

Note also that the problem was tackled as an add on to another Act.

Regulation of Investigatory Powers Act (RIP)

Introduced in **2000**, it includes the power of **government** to:

- demand that an ISP provides access to a customer's **communications** in secret, i.e. to divulge the websites you have visited and the emails you have sent,
- demand your **decryption keys** so that they can access any encrypted data on your computer (penalty for refusal is 2 years in prison)
- and others activities.

- prevent the existence of an interception warrant, or data collected with it, being revealed in court.

Conflicts

There are of course conflicts between the **RIP** Act and the **Data Protection** Act, etc.

Is there **ethically** a difference between

getting a warrant to gather information on an individual suspected of wrongdoing, or

gathering information on everybody in case, in the future, some of them are to be investigated?

Recent changes

Since **9/11**, the pendulum has swung decisively.

In the **USA**, the **Cyber Security Enhancement Act (2002)** allows law enforcement officers to carry out internet or telephone eavesdropping without first obtaining a court order.

Hacking

In the **UK** and **USA**, **hacking** is seen as a **crime**.

Until recently, in **Germany**, **simple hacking** as such was **not a crime**, although its **consequences** can lead to serious criminal charges.

However, a recent new German **Computer Crime Law** has changed all that and Germany has now one of the **strictest laws**.

Therefore, in different countries, both official and unofficial views of certain acts can vary significantly and the view can change suddenly over time.

As the **Internet** is **international**, this can lead to **major problems** in successfully bringing cases to court.

Ethical hacking?

Some universities have introduced courses with this heading. Is that valid?
Is the name appropriate?

Idea is to teach techniques used by hackers so that they can be countered.

Also can be used to test flaws in security.

We have a new(ish) Honours half module:

CSCU9YS Computer Security and Forensics

which surveys some of these issues.

Jurisdiction

General question of **whose jurisdiction**, certain acts fall.

This does not always help computer users.

In the USA, certain "**adult**" services can be provided via the Internet in, for example, California.

Such services are illegal in some other states.

Californian companies sending products to residents of these other states have been charged with breaking the law.

Jurisdiction

Another example is **Internet Gambling**.

Gambling is illegal in some US states and legal in others. The 1961 Federal Wire Act stopped telephone betting across state lines. This has used to arrest the owner of the Internet Gambling Company *BetonSports*.

Company based outside US, but most customers in USA.

One concern about Internet Gambling is its use in money laundering.

Jurisdiction

The originator of one important virus attack was discovered to live in the Philippines.

The main law there was written chiefly to cover credit card fraud and so there are some problems.

The USA felt that it was the main victim and so extradition was discussed.

Under the **US Computer Fraud and Abuse Act** (1984, 1986, 1996) the maximum penalty is **5** years **for each computer** affected!!!

Jurisdiction

Some countries, of course, have **no laws** against computer misuse of any sort.

Attacks can be launched from these countries even when the perpetrator is not physically there.

Using such countries can make it very **difficult to track down** the instigators of a virus or other kind of attack.

End of lecture

Further study: https://www.open.edu/openlearn/science-maths-technology/software-and-the-law/

A free online course that goes into much greater depth than this lecture.