Professional Computing

Year Two, Semester One

Lecture One – An Introduction

This module aims to give the learner the ability to identify, understand and describe ethical, social, legal and professional issues in computing. But what does "professional" mean?

The word "professional" has a wide range of meanings. For example, there are recognised professions such as medicine, law, teaching, dentistry and engineering – which are jobs that usually require:

- Substantial education/training, where members of the profession decide the nature of the training required.
- One or more professional bodies
- Standards of conduct with which members must comply.

Professional Bodies

Professional bodies are responsible for many things, such as establishing a Code of Conduct, and mechanisms for the dissemination of knowledge & good practice to members. They also set standards for education (e.g. degree accreditation), and serve as advisers to the Government and regulators (for instance in the drafting of new law).

To call yourself a member of the profession you must be recognised by the professional body. For example, to advertise yourself as an architect is illegal without permission of the ARB (Architects Act, 1997). This is a concept known as reservation of title.

Reservation of function is a similar concept - to carry out the functions associated with the profession, you must be recognised by the body. For example, to audit the accounts of any public company, you must be recognised by the Association of Certified Accountants.

The Engineering Profession

In the US, most types of engineer have reservations on both title and function associated with a professional body. A few State (not federal) laws prohibit:

- Calling yourself an engineer without registration
- Companies from using the word "engineer" without employing registered engineers
- Academic programmes which use the word "engineer", where the majority of teaching is not by registered engineers.
- Carrying out engineering work without the supervision of a registered engineer.

How does this apply to Software Engineers?

Engineering in the UK

The term "engineer" is unrestricted in the UK. The IT industry is unregulated but it does have a professional body – the BCS. While BCS does not have regulatory powers, it does:

- Accredit degree programmes (ours!)
- Advise the government on IT related issues
- Disseminate good practice and attempt to define "Professional Behaviour"
- Maintain a Code of Conduct (here)

However, there have been a few incidents in computing history that have prompted the discussion of whether or not the term "software engineer" should be restricted.

For example, in October 1992, shortly after introduction, the London Ambulance Service's Computer Aided Dispatch system failed catastrophically. The system could not cope with the load placed on it by normal use. Communication with several ambulances was lost and as a result, response to emergency calls rose to *several hours*.

Another incident was the Therac-25 disaster from 1986-87, where a radiation therapy machine's software experienced fatal failure, causing patients to be exposed to massive radiation overdoses on six separate occasions. Four people died.

Software engineers were ultimately responsible for these events, and tighter regulation on training and practice may have helped avoid them.

LECTURE TWO – LEGAL PERSPECTIVES

[Disclaimer:** These notes do not constitute legal advice. If legal advice is required, please contact a lawyer.**]

What is the Law?

This has the potential to be a very philosophical question, but we are able to define the Law as "a set of laws which can be enforced by a court".

The geographical area governed by a single set of laws is known as Jurisdiction. For example, State Law in the US applies only to a specific state, while Federal law applies throughout all states. This is a fairly simple concept, but jurisdiction can become very complicated when applied to computer use.

The Law is actually more than a set of rules. It constitutes different systems of courts, differing rules concerning how appeals are made, and different rules about how new and old laws work together.

In the UK, there are two types of law – Criminal and Civil.

Criminal Law:

- Designed to protect "society" from wrong doers
- Involves police investigation and arrest
- CPS proceeds with prosecution
- Adheres to the concept of "Innocent until proven guilty"
- Guilt must be proven beyond reasonable doubt

Civil Law

- Involves settling disputes between people (where companies can become "people")
- Litigation must be brought by one of the parties of the dispute (the plaintiff) against another (the defendant)
- Both parties must present arguments and the final decision is based on "balance of probabilities"
- Usual objective is to obtain damages (money) or injunction (court order)

Torts

Under Common Law, a tort is a civil wrong-doing that may not necessarily be illegal (or criminal) but somehow has caused harm which can be re-addressed through the courts. Torts are usually re-addressed through awarding of damages. There are a few varieties of Torts:

- Nuisance
- Negligence
  - Duty of care
  - Dereliction of duty
- Defamation

English Law – A (Very) Brief History

In roughly 1086, the system of Common Law was introduced. Back then, law was mostly based on precedent, with a sprinkling of common sense from judges. Central authority at the time laid with the court of the King. Equity (fairness beyond the common law) was handled by the Court of Chancery.

During the 15th Century, legal power moved from the King to Parliament, with legislation now being made by political bodies.

In the 19th Century, the courts reorganised to combine common law and equity, and legislation became more important than them both.

Legislation

A "Legislative Act of Parliament" (or statute) can create, amend or repeal any new or existing law. Any statute overrules any previous act or precedent (but not court decisions)

The body of law is regularly reviewed by the Law Commission, using the following process:

1. Bill is drafted (usually under supervision of government minister)
2. Bill introduced in either the House of Commons or the House of Lords (but usually passed by both)
3. Several stages of reading and amendment
4. Bill becomes an Act following Royal Assent.

Legislation is also controlled, to a degree, by the European Union.

Europe

The European Economic Community (EEC) was established in 1957, and Britain joined in 1973. Now, the Council of the European Union and European Parliament have legislative powers within member states:

- **Regulations** – directly enforceable by Parliament and English Courts.
- **Directives** – instructions for member states to alter their laws.
- **Decisions** – specific decisions for states, enterprises and individuals.

A piece of European legislation we're particularly interested in is the European Convention on Human Rights – specifically:

- **Article 5** - "Everyone has the right to liberty and security of person."
- **Article 7** – Prevents a person from being held guilty of an offence that was not an offence at the time it was committed.
- **Article 8** - "Everyone has the right to respect for his private and family life, his home and his correspondence."
- **Article 10** – "Everyone has the right to freedom of expression."

A Few Case Studies

Facebook Hacking

In January 2011, Gareth Crosskey (a 21-year-old living in Sussex) hacked a US citizen's Facebook account and gained access to an email account. The breach was reported to Facebook, who reported it to the FBI. The FBI then traced the hack to the UK, and informed the UK police.

Crosskey was charged under the Computer Misuse Act (1990, 2004). Due to evidence presented, Crosskey pleaded guilty and was imprisoned for 12 months in May 2011.

R v. Gold & Schifreen (1988)

During the period between late 1984 and early 1985, Robert Schifreen and Stephen Gold gained unauthorised access to BT's viewdata service (called Prestel), after Schifreen had shoulder surfed a Prestel engineer and noted their login credentials.

They were charged under the Forgery and Counterfeiting Act (1981), using the argument that that they'd defrauded BY using a "false instrument" – the internal condition of BT's computers after it had processed the lifted password. Gold and Schifreen were tried and fined £750 and £600 respectively.

The pair later appealed, citing a lack of evidence that they'd intended material gain, evidence that BT didn't take security seriously (the engineer's stolen credentials were apparently 1234:22222222), and the fact that their case wasn't really a case of Forgery and Counterfeiting. They were acquitted by Lord Justice Lane, and the acquittal was upheld by the House of Lords upon appeal by the prosecution – because the Forgery and Counterfeiting Act blatantly was not intended to apply to a situation such as this.

The Computer Misuse Act (1990) was introduced partly in response to the result of this case.

The Computer Misuse Act (1990)

The original Computer Misuse Act recognised three new offences:

1. Unauthorised access to a computer.
2. Unauthorised access to a computer with intention to commit a serious crime.
3. Unauthorised modification of the contents of a computer.

A person is considered guilty of a crime if either they or the computer in question is in the UK at the time of the offence.

Section One

A person is guilty of an offence if:

- They cause a computer to perform any function with intent to secure access to any program or data held in any computer;
- The access they intend to secure is unauthorised; and
- They *know* at the time when they caused the computer to perform the function that this is the case.

This is punishable by a fine up to £5000 or 6 months' imprisonment.

Section Two

The second section of the act covers unauthorised computer access to commit a more serious crime. It is not necessary for the more serious crime to have been carried out, as long as intent to do so can be proven.

This is punishable by up to five years' imprisonment or an unlimited fine.

Section Three

A person is guilty of an offence if:

1. They do any act which causes an unauthorized modification of the contents of any computer; and
2. At the time when they do the act they have the requisite intent and the requisite knowledge, where requisite intent covers:
    - To impair the operation of any computer;
    - To prevent or hinder access to any program or data held in any computer; or
    - To impair the operation of any such program or the reliability of any such data.

The maximum penalty is 5 years or unlimited fine. Some examples of this offence would be:

- Spreading a virus
- Encrypting files and demanding a ransom for revealing the key
- Redirection of browser home pages etc.

The Computer Misuse Act – Review (2004)

The CMA was reviewed in 2004 with input from professional bodies, including BCS. The maximum sentence for unauthorised access was raised from six months to two years, and DoS attacks were explicitly criminalised by a newly recognised offence described as "impairing access to data".

Despite these changes, the UK has had relatively few prosecutions under the CMA.

Police and Justice Act (2006)

2006's Police and Justice Act contains amendments to the CMA:

- **Section 35** - Unauthorised access to computer material, punishable by up to 2 years in prison or a fine or both.
- **Section 36** - Unauthorised acts with intent to impair operation of computer, etc. punishable by up to 10 years in prison or a fine or both.
- **Section 37** - Making, supplying or obtaining articles for use in computer misuse offences, punishable by up to 2 years in prison or a fine or both.
- **Section 38** - Transitional and saving provision.

Further amendment is being discussed to address the definition of a smartphone, following 2011's News International Phone Hacking Scandal.

Computer Misuse Act: Issues

The common view is that the real issue with computer crime is a lack of resources for investigation and prosecution rather than a lack of laws. Phishing, for instance, is better dealt with as a case of Fraud – but "Fraud" is an unclear term in English law.

There are also many kinds of "deception" in UK Law - can a computer be deceived? What about AI? The discussions on these topics are ongoing.

It is also argued that some instances of Digital Rights Management (DRM - a systematic approach to copyright protection for digital media) should be explicitly liable under the CMA.

Another Case Study: Gary McKinnon

Between 2001 and 2002, Gary McKinnon, a systems administrator from Scotland, hacked into 97 US military and NASA computers. He deleted critical files, copied passwords and shut down the US Army's Military District of Washington computer network for 24 hours. While these attacks caused serious damage to military and NASA computers, McKinnon claimed he was only looking for evidence of UFO cover-ups and Free Energy suppression.

The investigation and extradition processes were long and complex, with seven counts of computer misuse being brought against McKinnon (totalling a maximum sentence of 70 years). A Judicial review into the extradition was granted in 2010, due to concerns that McKinnon (who had previously been diagnosed with mild autism/Asperger's) would be a suicide risk if extradited. Extradition was blocked by the Home Secretary in 2012, and later that year the Crown Prosecution decided not to prosecute due to difficulty in evidence location in the US.

Lecture Three – Data Protection & Freedom of Information

Google Street View

Google's Street View project is a great idea, but it's always needed some refinements. Their use of cameras in public was frowned upon, despite anonymization of faces and car registration, and Street View is no longer developed in some counties – including Austria, Germany and India.

During the collection of data for Street View in the US and UK, information concerning unsecured Wi-Fi was also gathered – for "potential use in future projects". This was a violation of several country's Data Protection legislation. Google has since been fined by France FCC for $142,000, and in 2010 Google agreed to destroy the data. As of July 2012, Google has admitted to still having "some" UK data.

Data Protection Act (1984)

The Street View project is a great example of prevalent concerns about large amounts of data being collected about people, and data being used for reasons other than the reason it was collected, are.

The European Council held a convention which stated various principles for controlling data collection, use and storage. The UK's Data Protection Act of 1984 was designed to protect individuals against:

- The use of inaccurate/incomplete personal information
- The use of information by unauthorised persons
- The use of information for reasons other than it was collected for.

Data Protection Act (1998)

The new (and current) Data Protection Act replaced its predecessor, in an effort to bring UK data legislation into line with the European Data Protection Directive. It provided new definitions for a few terms:

- **Data** – information that is being processed automatically or is collected with that intention or recorded as part of a "relevant filing system"
- **Processing** – obtaining, recording, or holding data or carrying out any operation on it
- **Data Controller** – who controls why or how data is processed
- **Data Processor** – anybody who processes the data on behalf of the controller
- **Personal Data** – data which relates to a living person who can be identified using this data (possibly with other data the DC might have)
- **Sensitive Data** – Personal data relating to racial, ethnic, religious, political, sexual (etc.) aspects of a person.

It also lays down some principles.

First Principle

Personal data will be processed fairly and lawfully and in particular will not be processed unless:

a. At least one condition in Schedule 2 is met (consent is given or some legal obligation to process data [tax returns, law enforcement etc.]), and
b. In the case of Sensitive Data at least one condition in Schedule 3 (Explicit consent is given).

Second Principle

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 that purpose or purposes.

In laymen's terms, data can't be collected "just in case it's useful".

Third Principle

Personal Data should be adequate, relevant, and not excessive in relation to the purpose or purposes for which it is collected.

This principle is often broken without thinking – such as by asking questions regarding marital status when processing a library membership request, etc.

Fourth Principle

Personal data should be accurate and where necessary kept up to date.

Fifth Principle

Personal data processed for any purpose or purposes should not be kept for longer than it is necessary for that purpose or those purposes.

The debate on how long "is necessary" is a tricky one. For example:

- Financial data needs to be kept for 7 years for auditing.
- Civil actions can be issued six years after any event.
- Common advice is that emails should be kept for 7 years.
- University Exam results might be held indefinitely.
- CCTV data is routinely deleted after one month (this has implications for FOI) due to storage constraints.

Procedures for data deletion must be rigorous and specified, including deletion of backed up data.

Sixth Principle

Personal data should be processed in accordance with the rights of the data subjects under this act.

Subjects have a right to:

- Know whether a DC held data relating to them, the right to see the data, and the right to have the data corrected or erased if inaccurate. - DPA (1984)
- A description of the data being held.
- An explanation of the purpose for this it is being held.
- A description of to whom the data can be disclosed.
- An intelligible statement of the specific data about them.

- A description of the source of the data.
- (If the data is used to automatically make a decision) ask about the logic behind the automatic decision, and for the decision to be reconsidered non-automatically.
- Prevent the processing of data likely to cause damage or distress or for direct marketing.
- To be awarded compensation in the case of damage.

Seventh Principle

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction, or damage to personal data.

In other words, data security is a legal requirement.

Eighth Principle

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in the relation of processing of data.

This principle specifically allows companies to transfer data over national boundaries.

A Few Case Studies

Durant v. FSA (2003)

Michael Durant had an unsuccessful dispute with Barclays Bank, which led him to approach the Financial Services Authority (FSA) and ask them to investigate the bank for misconduct. The FSA carried out their investigation, but refused to tell Durant of outcome, citing reasons of confidentiality.

If the FSA did find Barclays in breach, Durant could have re-opened the dispute, so naturally, he wanted to find out the outcome. Durant attempted to use DPA to access his "Personal Data" held by the FSA - who shared only electronic data and withheld all paper-based information

Durant took the FSA to court and then court of appeal – losing in both. The FSA's defence was that the sought paperwork was not part of a "proper filing system". The final judgement was that opinion on validity of a claim was not "Personal", even if it included Durant's name.

The lesson to learn from this case is that the DPA "is not an automatic key to any information" that contains one's name.

Gaskin v. United Kingdom (1989)

Graham Gaskin was placed in care as a child and later claimed to have suffered childhood abuse while in care. He requested access to his records held by Liverpool Social Services so to take legal action, but was only granted partial access – citing a duty of confidentiality of third parties.

Gaskin objected to this and appealed to the Court of Appeal – who upheld the access refusal.

Gaskin then went to the European Court of Human Rights, who ruled in his favour, for these reasons:

- Gaskin's human rights were breached since there was no independent appeal body to whom Gaskin could have taken his case.
- Care Records may act as substitutes for family memories, to which the average individual does indeed have access.

This case had a huge impact on the revision of the 1984 DPA. Following the revision, people in Social Service Care have legal rights to any information held, though this is not the case if they are in the care of a private charity.

Privacy

Citizens of the UK now have very little privacy. As of 2009, there is one CCTV camera for every 14 people. There is also the Investigatory Powers Act (2016) – also known as the Snoopers' Charter – to bear in mind, which:

- Allows police, intelligence officers, and managers of several government departments (such as the British Transport Police, HMRC, Gambling Commission, and the Welsh Ambulance Trust) to see Internet connection records (as part of a targeted and filtered investigation) without a warrant.
- Allows police and intelligence agencies to carry out targeted equipment interference (basically hacking) and bulk equipment interference for national security matters related to foreign investigations.
- Creates a new criminal offence for a Communication Service Provider (CSP) or CSP employee to reveal that data has been requested.

Regulation of Investigatory Powers Act (2000)

The Regulation of Investigatory Powers Act (RIPA) was introduced as a framework for lawful interception of computer, telephone and postal messages. Amongst other things, it permitted ISPs (and most employees) to monitor communications without consent - provided it's to:

- Establish facts.
- To ensure company regulations are being complied with.
- To ascertain standards which ought to be achieved.
- To prevent crime.
- To investigate unauthorised use of telecommunications systems.
- To ensure effective operation of system (e.g. detecting denial of service attacks).
- To find out whether a communication is business or personal.
- To monitor but not record calls to confidential counselling helplines run free of charge by the business.

Such organisations are required to make reasonable efforts to inform users that such interception might take place.

Interception Warrants

The RIPA also allows government agencies the right to ask for interception warrants to monitor communications to or from specific persons or organisations. For example:

- **2009-2011** - 9,600 instances of councils using RIPA
- **Stockton Council** - used RIPA to investigate the movement of pigs
- **BBC** – uses RIPA to investigate licence fee avoidance
- 26 Local Authorities used RIPA to spy on cases of dog fouling.

Councils are now limited to cases involving criminal offence (with at least a potential tariff of six months' imprisonment) from Nov 1st 2012.

Freedom of Information Act (2000)

The Freedom of Information Act (FOI) provides public access to information held by public authorities, with certain conditions and exemptions.

Where information is exempted from disclosure, a public interest test must be made, balancing the public interest in maintaining the exemption against the public interest in disclosing the information – unless the exemption is classified as "Absolute".

The operation of the Act is the responsibility of the Office of the Information Commissioner. The Act imposes a duty for all public bodies to adapt a scheme of publication of information which must be approved by the IC.

The Act is not without its issues. For example:

- There are potential conflicts between FOI requests and the DPA in cases where there is personal data involved.
- FOI requests must (usually) be answered within one month of receipt:
  - Sometimes this is impossible
  - For some data, this means the data is effectively inaccessible (CCTV).
- FOI requests have been used to "punish" perceived slights.
- Public bodies often charge for FOI requests (Birmingham Council charges £25 per request).
- Few Public Organisations possess the necessary infrastructure to handle FOI requests.

The US has an older (and stronger) Freedom of Information Act which includes Personal Data. Any law enforcement agency must reveal all knowledge of criminal activities of a subject – the FBI claims to have handled 300,000 such requests.

Lecture Four – Contracts & Liability

Contracts

Contract law is old English law in England and Wales. Generally, a contract is formed when one person makes an offer, and another person accepts it by either communicating their acceptance or carrying out the offer's terms. Another way of thinking of a contract is as an **agreement that is enforceable in court.**

For a contract to be binding, all parties **intend** to make the contract, and be **competent**. For some contracts, each party must provide and receive something of value. This is known as consideration.

There is no requirement for lawyers or witnesses to be present, and a contract doesn't even have to be in writing – these are simply tools for making contracts easier to enforce.

Contract law is changing in the face of new technology. This is inconsequential to most technological advancements – but not software.

Software Contracts

The Standish Group's CHAOS report (in 2009) reported that only 32% of software projects:

- were completed on time.
- were completed within budget.
- provided the expected functionality.

It also reported that 24% of projects **failed** completely.

BCS estimates that only 16% of software projects were successful in 2004.

This is all evidence that software projects are **high risk**. However, there are few contractual solutions that help to protect both parties:

- Fixed Price Contracts
- Time and Materials
- Consultancy and Contract Hire

Fixed Price Contracts

Fixed price contracts are typically tailor made, for projects involving a bespoke system. They include a short agreement on who the parties are, the standard T&Cs (how the supplier usually does business) and a set of schedules/annexes, such as:

- Particular requirements of the contract
- What is supplied
- Deadlines
- What payments are to be made

The Product

The contract must define the "product" to be produced in clear terms. Usually the Standard T&Cs will refer to a particular Annex, which will in turn refer to a

Specification of Requirements. However, Requirement Specifications are notoriously difficult to produce well:

- Good Software Engineering is hard.
- The needs of the Client **will** evolve.
- Technologies change.

The contract must address how such changes are accommodated, and there must be a method for calculating payment to deal with modifications.

The Delivery

Delivering the product is rarely a simple case of just handing over the code as a file. Thus, the contract must specify **exactly** what is to be delivered:

- Source code
- Command files for building executables
- Documentation
- Reference/Training/Operations manuals
- Training
- Test data and results

Another issue is intellectual property. Who owns the IP once the software is delivered? This must be included in the contract, as must terms of confidentiality.

Payment

An example of a clause pertaining to payment would be the following:

> *"Payment shall be due within 30 days of the date of issue of an invoice. If payment is delayed by more than 30 days, the Company will have the right to terminate the contract or apply a surcharge at an interest rate 2% above the bank base lending rate."*

However, it is unlikely that such a clause will ever be used in contracts pertaining to software projects. Instead, payment is more likely to be staggered, as this protects the supplier from cash flow issues and the risk of the client going out of business. Some examples of how to stagger payment could be:

- Initial payment of 15% on signing
- Stage payments during project (say, at 65% completion)
- 25% at acceptance of software
- Final 10% at end of contract.

A more general approach to staggering would be:

- By calendar month – benefitting the supplier.
- In terms of project completion – benefitting the client.

Penalty Clauses

While payment clauses protect the supplier, the client may wish to add penalty clauses to protect themselves from significant delays. An example could be a million-pound contract, where payment is reduced by £5000 per week of project overrun, up to a maximum penalty of £100K (10%).

As we've already seen, software is often delayed, but such penalties are limited by their own definition:

- Suppliers are often very reluctant to accept penalty clauses
- Smaller pool of reputable suppliers
- Contracts involving penalties usually increase bid price by at least 50% of the penalty
- If the software is running particularly late and the penalty is very high, the supplier has no incentive to complete the work.

Client Obligations

The contract must also specify what the supplier needs from the client, such as:

- Documentation
- Access to appropriate staff
- Machine facilities for testing
- Accommodation

Most suppliers will have their own standards of testing and quality assurance, but large clients may prefer to use their own.

Acceptance, Warranty & Indemnity

The client must provide a fixed set of acceptance tests. These will include the nature of the tests, the expected results, and accuracy figures etc. Successful demonstration of system will constitute acceptance – the contract must also take into consideration what happens when tests are not 100% successful.

The industry standard warranty is 90 days, with any errors identified during this time fixed free of charge. Once the warranty expires, fixes are subject to negotiation. It is more likely that the system will be enhanced than time will be spent on fixing individual errors. It is improbable that any fixed price is realistic.

There is always a risk of the supplier infringing the intellectual property rights of a third party. Usually a contract will indemnify both the client and supplier so each other is not liable for any infringement by the other due to own fault.

Termination

It's not uncommon for projects to be cancelled. Whether it's because the client went bust or merged with a larger company, or simply because the technology became obsolete mid-production, the contract needs to detail what payments are owed to the supplier for unfinished projects and what IP rights exist.

Arbitration

After reading these last few sections you may be thinking that contracts are very complicated. You'd be right. Contracts and their complexity make litigation very expensive, and often not worthwhile. The contract may specify that in the case of a dispute, the opinion of an independent arbitrator will decide. This avoids legal costs.

BCS maintains a list of qualified IT arbitrators.

Time and Materials Contracts

With a Time and Materials Contract – otherwise known as a "Cost plus" contract – payment is based on the supplier's expenses (usually up to a maximum), as well as a daily rate so that the supplier can secure a profit.

These contracts are usually cheaper than Fixed Price contracts, which are usually very difficult to set up anyway because the lack of clarity with regards to the project.

Despite this, there is currently a shift in the IT sector from Time and Materials contracts to Fixed Price, especially for public-funded projects.

Contract Hire & Consultancy

Contract Hire offers a far simpler alternative to Fixed Price contracts. With this type of contract, the supplier provides services for staff for a fixed period, with agreed hourly/daily rates. The client takes responsibility for managing staff, and termination by either side can be done at short notice.

Another alternative is consultancy – expert analysis of a key part of business. Consultancy usually produces a report than a product, and is usually done at a fixed price. It is far more difficult for a report to fail an acceptance test than a product. However, consultancy has a few issues:

- **Confidentiality** – There need to be safeguards to ensure the consultant doesn't profit against the client, following the project.
- **Terms of Reference** – There must be a clear definition of what the consultancy is meant to be looking at. Often the issue isn't in the originally-agreed-upon scope, which is a major source of disagreements.
- **Control Over Final Version** – Usually the client approves a draft version of the document, and the client may require amendments that – if included in the final version – may damage the consultant's reputation.
- **Liability** – Few consultants wish to be liable for their expert advice, but most clients disagree, and also need to be able to verify the consultant really in an expert.

Liability

Most suppliers are very reluctant to agree to any liability for defective software or hardware. Standard T&Cs will usually limit liability to the project cost, or even a fraction of this.

However, the Law disagrees – the Unfair Contract Act (1977) makes it impossible to limit liability in the result of a death or personal injury.

Consumer Protection

A client is considered a "consumer" if:

1. The Client is a private person;
2. The Supplier is acting as a business;
3. The goods are of a type usually intended for private use.

There are laws protecting consumers from bad products and businesses. The Sale of Goods Act (1979) enforces that goods are fit for purpose, while the Goods and Services Act (1982) enforces that goods are produced with reasonable care.

It's unclear, though, if software is classed as "goods". Licenced software sold in electrical retail stores certainly is, but bespoke systems probably aren't.

Case Study: St. Albans v. ICL (1996)

St Albans Council contracted International Computers Ltd. to produce software for calculating community charge tax. ICL insisted on using its standard T&Cs, which stated:

> *"Liability will not exceed price or charge of equipment, program or service, or £100,000, whichever is lesser."*

There were errors in the software which led to an overestimation of the population. This subsequently caused the council to undercharge the residents, leading to a loss of £1.3M. The council went on to claim breach of contract and that the liability limitation was unreasonable.

The judge found that the software was indeed not fit for purpose, and that the project manager was negligent. ICL – as an international company – had liability insurance worth £50M. The judge found ICL's T&Cs unfair and required full compensation to be paid by ICL to the council.

Lecture Five – Intellectual Property

Theft is the "intentional taking of somebody else's property with the intention of permanently depriving them of it". However, sometimes that deprivation is difficult to define. For example:

- If someone steals your laptop, this is clearly theft, because you're no longer able to use it. A laptop is an example of **tangible** property, and is protected by laws related to theft and damage.
- If someone steals the formula for a drug that you've developed that cures the common cold, and releases it to a rival company, the lines are blurred – because while you still have access to the formula itself, you've been deprived of the money and recognition the cure would have brought you.
- What if the formula is instead released to WikiLeaks?

Information is **intangible**, and thus is governed by different laws.

Intellectual Property

Intellectual Property is not a new concept – trademarks and patent law is based on the Paris Convention of 1883. The problem is that some intangible property, such as music, films, chemical formulae and *software*, can be very valuable indeed.

There are several types of IP rights:

- Copyright
- Patents
- Confidential Information
- Trademarks

They each apply to different circumstances. We'll explore each in-depth.

Copyright

Copyright is governed by the **Copyright, Design and Patents Act (1988)**, and the **Copyright (computer programs) Regulations Act (1992)**. The owner of any IP work has certain exclusive rights:

- The right to make copies of the work
- The right to issue copies of the work to the public (either paid or for free)
- The right to adapt the work e.g. translating from English to Japanese (or Java to C)

These rights are automatic, and permission must always be requested and given by the author before breaching this exclusivity – though often permission is implicit, such as in the case of webpages.

Copyright lasts for **70 years after the death of the author**, but does not stop anybody publishing identical work – only copied work.

It is **not** an infringement to:

- Make a back-up of a program you are authorized to use, as long as it's only one copy.
- Decompile code to correct any errors, or to write new code to interoperate with it.
- Sell your right to use a program - without keeping a copy.

Databases

Database Copyright is a special case. It only applies where there is "substantial investment in obtaining, verifying, or presenting the contents of the database." – but this is typically not the case.

For example, if a football fan made a database of every game played by Liverpool FC, it would indeed be a lot of hard work, but doesn't involve any original content, so wouldn't be protected.

Infringement

There are two types of copyright infringement:

- **Primary** – Where the exclusive rights of the copyright holder are infringed, leading to a Civil issue (damages, injunctions, etc.)
- **Secondary** – Where primary infringement occurs in a business context. This involves selling copies of the copyrighted work, or using pirated software in a business (just as an example). This leads to a Criminal issue, with substantial fines and imprisonment.

The majority of software uses Digital Rights Management (DRM). Providing information about how to avoid DRM is the same as actual copyright infringement in the eyes of the law (since 1998).

A good example of the usage of DRM is by maths textbooks. These textbooks will occasionally contain deliberate errors to ensure (and prove) copyright. Software can do the same – by including lines of non-functional code, for instance.

Case Study: Kim Dotcom

Born Kim Schmitz (1974), Kim Dotcom was a German Internet Teenage Tycoon in the 1990s. In 1994 he was convicted of hacking crimes, and went on to be convicted again in 2001 – this time for insider trading and embezzlement.

He moved to Hong Kong in 2003 and set up AI driven Hedge Fund promising a guaranteed 25% return. He was subsequently fined by the Hong Kong Securities. He went on to found Megaupload Ltd. in 2005 - a huge cloud computing file sharing site, before moving to New Zealand in 2010.

In January 2012, The US Department of Justice closed down Megaupload and started criminal cases against the owners. Hong Kong Customs froze HK $300 million, and Dotcom was arrested by NZ Police on 20th of January for extradition to the US – with an additional $17 million worth of assets being frozen.

In June 2012, it was found that the search warrants used in January were not legal, leading to $750k worth of assets being returned. In September 2013, Dotcom had plans to enter NZ politics, and started a new music streaming service. As of September 2015, there's a new trial for extradition ongoing in Auckland.

Patents

A patent is a temporary right granted by the state, enabling the inventor to prevent other people from copying his work without permission. They are governed by the Patents Act (1977).

Patents must be applied for, but are far stronger than copyright – as they prevent others from coming up with identical works.

Patents were designed to encourage innovation, as they reward the inventor a grace period to recoup development costs.

For a product to be patentable it must:

- Be **new**.
- Involve an **inventive** step.
- **Not** be an **obvious** solution anybody well-qualified could come up with.
- Be capable of industrial application (i.e. is **practical**)
- **Not** be in an area specifically **excluded** - i.e. no
    - Scientific theories
    - Mathematical methods
    - Literary/dramatic/artistic work
    - Presentation of information
    - A scheme, rule, method for performing a mental act, playing a game or doing business, or a program for a computer.

Obtaining & Enforcing

Patents are granted on a national basis, meaning *technically* you need to apply in each country - but there are trade schemes such as WIPO, European PO etc. that help with this.

Computing - being a global business - requires the patent to be taken out in enough countries to ensure it is challengeable.

Timing is crucial when it comes to patents. The date of initial application determines what is "new", but full patent specification requires specialist work, which takes a *long* time to draft. The overall patent application process often takes four years to complete.

Enforcing a patent is difficult, with many patents contested due to an unclear inventive step, or the existence of "prior art". Patent enforcement costs time and money – something which small companies often cannot afford.

Software Patents

The US Patent and Trademark Office has always refused to patent software, though this changed in 1981, with a patent for curing rubber (using software to determine required heat) being granted. As it stands, software can be patented if:

- It is part of a product that can be patented;
- It controls some process with a physical effect; or
- It processes data that arises from the natural world.

The European Patent Convention, and the Copyright, Design and Patents Act (1988), state that (technically) software cannot be patented - but several countries do in fact patent software. The EU Commission produced a draft directive in 2002, but it has since then been heavily modified and is unlikely to be accepted by member states.

In short, Software Patents are a mess.

Pros and Cons

Patents are designed to reward innovation. The advantages of patents are:

- ✓ They allow for financial rewards for innovators and creators
- ✓ They enable funding for future research
- ✓ They fund computer scientists!

The disadvantages, however, are:

- × The software industry has been very successful without patents
- × Most original development is done by small companies, which is then licenced to/exploited by big companies
- × Patents allow big companies (with big R&D departments) to claim basic computer functionality as their exclusive right
- × A great deal of software has already been written without patents, yet now we see retrospective patents being granted

Case Study: Richard Wiseman

Richard Wiseman worked as a hacker for MIT between the 70s and 80s. In 1983 he launched the GNU project with the aim of giving computer users freedom and control in their use of their computers and computing devices. This aim was achieved by developing and distributing software that was free to run, examine, modify and share. You may recognise this software as Linux. He also participated in activism against Privacy, Copyright, etc.

Confidential Information

Often work involves an obligation of confidence. For example, software development for a company might reveal commercially sensitive information or conditions of employment for employees. There are long periods of notice for employees with sensitive knowledge, and clauses in consultancy agreements for consultants.

Even without such conditions, obligations might occur under Equity – "Obligation occurs if a reasonable person in such a position would reasonably understand that information was given in confidence."

The Public Interest Disclosure Act (1998) legislates that information can be disclosed if the employee believes any of the following might occur:

- o A criminal offence
- o Failure to comply with a legal obligation
- o A miscarriage of justice

- Danger to health and safety
- Environmental damage

Trademarks

Any sign capable of being represented graphically which is capable of distinguishing goods and services, can be trademarked. This is extremely useful to protect some kinds of retail software, even if it can be difficult to enforce when software is the subject. Logos, on the other hand, are remarkably easy to protect.

Trademarks can be either registered or not. Many countries require registration before legal protection, though the US and Canada do not. Registration in the UK is done via the Patent Office. There are, of course, rules for what can be a trademark (i.e. not people's names or places).

In the UK, the Trade Marks Act (1994) makes it illegal to:

- Apply unauthorised trademark to goods
- Sell or hire goods with such a trademark
- Have in the course of business such goods

Breaches of these laws are usually regarded as criminal offences, but civil actions can also be brought.

UK law also protects unregistered trademarks, but far less strongly than registered trademarks. Passing off is where a business, passes off another party's goods or services as if they are their own, by misrepresentation, and is governed by Tort law.

LECTURE SIX - HUMAN RESOURCES

History of Industrial Relations

Up to the 1970s, industrial disputes were common. Most strikes were politically motivated by left wing unions. Strikes were marked by aggressive picketing.

Many professions were closed shops requiring union membership. Nearly all trade unions imposed a political levy which funded the Labour party. As a result, Trade Unions were effectively immune from legal action.

However, in 1979, the Conservatives come to power, and imposed a mandate for root and branch reform. It took four successive Tory governments to break the power of the unions. During this time, legislation came into action to:

- Increase the power/protection of individual employees.
- Enforce equal pay of women.
- Introduce the concept of "unfair dismissal".
- Combat discrimination

Human Resource Departments

With all of this new legislation in place, Human Resources management in companies became very complex. Effort needed to be made to:

- Ensure recruitment/selection/promotion complied with legislation.
- Training and develop staff.
- Conduct staff appraisals.
- Know and adhere to dismissal and redundancy procedures.
- Administer grievance procedures.
- Stay up to date with new legislation.
- Take Health and Safety precautions.
- Etc.

Recruitment is now expensive and keeping employees happy actually makes sense. This all falls under the responsibility of the HR department.

Recruitment and Selection

Recruitment always involves soliciting applications, which is often out-sourced to a recruitment agency. Several stages of pre-selection and shortlisting occur in the cases of large companies. Recruitment agencies typically charge 25% of first year of salary for providing these services.

Selection on the other hand is usually left to the parent company, though the agency may advise/set up the selection procedures – which may take one or several of the following forms:

- One to one interviews with senior management -
    - A reliable method of selection, especially if records can be reviewed for future applications

        - Difficult to comply with existing anti-discrimination legislation
    - Interview by panel -
        - Very common
        - Easy to comply with legislation
        - Research suggests not reliable
        - Smooth talkers have a decided advantage
        - Common to have independents
        - Avoid nepotism/corruption
    - Assessment by references -
        - Important in Academic and Public bodies, but less so in private companies
        - Often not much more than a final check
        - Law often allows applicants to read their own references
        - Potential for civil action, either by the applicant for unfair references, or by the employer if reference misses negative aspects
        - Often referees will write banal but positive praise
        - Have become far less important
    - Tests –
        - Ability tests – which test general ability in written skills etc.
        - Aptitude tests focussing on ability to learn. Reliable for assessing programming ability
        - Personality Tests, which are surprisingly common despite competing theories of "personality" and unclear value

Staff Training and Management

UK industry is frequently criticized for lack of interest in staff training, especially when compared to the USA, where employers commonly fund part time master degrees for graduate employees.

Successive UK governments have provided initiatives to improve this. The most notable is the Investors in People scheme (1991), which sets the standard for staff management, is held by 14,000 organisations *worldwide*.

These initiatives often have less impact on professional careers. For instance, staff development of IT careers may be limited.

Remuneration

Disparity of pay (and benefits) is a major cause of dissatisfaction amongst the general public.

Public services normally use fixed pay scales with annual incrementation. Promotion means moving to a better pay scale, but the pay is rarely competitive with the private sector.

In private companies, remuneration is generally based on individual agreements within broad guidelines (equal pay for equal work & anti-discrimination legislation),

and is often difficult to justify. Job evaluations are common in order to aid justification.

Appraisal Schemes

Until recently it was possible to complete professional career without ever being appraised or reviewed. Often in Academia/Teaching, staff would receive feedback up to (say) age 35, with no appraisal beyond that point.

This has changed drastically.

Management by Objectives is a management model that aims to improve the performance of an organisation by clearly defining objectives that are agreed to by both management and employees. This involves:

- Regular – often annual - meetings with manager
- Agreed objectives which should be:
  - Clear
  - Measurable
  - Achievable
- Revised objectives for next period

Redundancy & Dismissal

HR is responsible for ensuring proper redundancy and dismissal procedures are followed. In all cases, such actions are difficult for the employee and general staff morale.

Laws concerning redundancy are complex and ever-evolving. The reason for dismissal must be valid in order to avoid being sued for Unfair Dismissal, where there is a possible award to the plaintiff of up to £72,300. Employment Tribunals are costly in time & money, so should be avoided. Despite this, there were 236,000 hearings in 2010.

Legislation lists the following reasons as justification for dismissal:

- Lack of capability
- Misconduct
- Statutory duty/restriction prevents continued employment
- Redundancy
- *Any other reason* **(???)**, but not:
  - Union activity (as long as it's legal)
  - Legal action to enforce employment rights
  - Issues covered by anti-discrimination law (for instance, maternity leave)

Statutory Dismissal Procedure

From 2004 to 2009 there was a set procedure for dismissal:

- Employer required to give reasons for dismissal in writing
- Meeting arranged for all parties to state their case

- If employer goes ahead, employee has right to appeal (ideally to senior management)
- Unfair dismissal can be claimed only after one year of employment

Any dismissal which breached the above was automatically considered unfair.

As of 2009, there is the ACAS Code of Practice. This isn't a set procedure but rather a guide to best practice, where a tribunal will consider the actual practice in the case of conflict. This legislation may increase pay-out by up to 25% in cases of unfair dismissal, though a minimum of 2 years' employment is required before any claim of unfair dismissal can be brought against the employer - with certain anti-discrimination exemptions.

Our current government is very keen to further streamline/de-regulate dismissals, supposedly in attempt to boost the economy.

Redundancy

Redundancy occurs when the company no longer requires people to do a certain job. This could potentially be because the company itself has gone bust.

The law entitles employees to minimum levels of compensation based on age, salary & experience. Most (good) companies will pay more than these levels.

If the company intends to make 20 or more employees redundant in 90 days or less, consultation is required. In UK law, there are two concepts of redundancy:

1. For purposes of **compensation**, redundancy is where employer no longer needs employees to do that job.
2. For purposes of **consultation**, redundancy is dismissal where reason is not related to individuals concerned

It is notoriously difficult to select who to make redundant. The most common strategy by far is "Last in, First Out", but this is usually unfair. Despite the unfairness, it is accepted by Trade Unions & courts, as it's not contrary to any anti-discrimination laws.

Constructive Dismissal

Constructive Dismissal is where a company behaves to an employee in such a way that they feel they must resign. Some examples of this are:

- Moving office to other side of country without consultation
- Employing a trained accountant to spend their time as a receptionist
- Senior management countermanding instructions issued by junior manager

Any breach in terms of employment contract can be seen as constructive dismissal.

Constructive Dismissal is not necessarily considered Unfair, though it often is in practice. 2004 regulations lay down statutory grievance procedures, which must be used before a claim for constructive dismissal can be made.

Case Study: Tapere v. Lewisham NHS Trust (2009)

Tapere worked at Lewisham Primary Care Trust for several years before being moved to Beckenham Trust. Beckenham was further to commute and also involved navigating the M25 ring road. Tapere objected to the move, and was then allowed to arrive zxsa5 minutes later than previously.

Tapere resigned and claimed Unfair Dismissal. The initial hearing found against Tapere, as the Judge felt that there was no material detriment to Tapere. This was overturned on appeal, as testing should only test whether or not it is reasonable for the employee to believe they have suffered a material detriment.

Transfer of Undertakings, Protection of Employment (TUPE)

TUPE is a set of laws governing situations where one company is taking over another:

- Employees of the old company automatically become employees of the new company
- Conditions of employment must be maintained
- Representatives of employees have the right to be informed about the transfer
- Consultation must occur about any changes affecting employees (e.g. office relocation)

TUPE was replaced in 2013 by the Enterprise and Regulatory Reform Act, though similar provisions were included in the new act.

Anti-Discrimination Laws

Since the 1970s a wide range of anti-discriminatory laws have been introduced. They provided similar (but not equal protection) against discrimination of a:

- Sexual;
- Gender;
- Disabilities;
- Religion; or
- Political

nature. Each type of discrimination was monitored by a different government body.

The Equality Act (2010) consolidated all previous laws into a single act, and provides a single framework which guarantees:

- Anti-discrimination;
- Equal pay and employment conditions; and
- Equal access to sales and services,

for the following characteristics:

- Gender
- Sexual Preference
- Marital status
- Age

- Race
- Religion
- Political Views
- Disabilities

With some explicit exemptions.

Case Study: McDonalds Dismissal

In March 2012, a 19-year-old employee of McDonalds (Llangunor branch) was dismissed for "gross misconduct".

A co-worker, while purchasing a McFlurry, asked the employee to "make it a nice one", and the employee used two portions of chocolate topping instead of one. She was fired on the spot, despite previously being an "exceptional" employee with a spotless 18-month employment history.

The employee appealed to Employment Tribunal on grounds of unfair dismissal, and the case was settled out-of-court in December 2012.

LECTURE SEVEN - THE INTERNET

Internet Service Providers

An interesting question is the following:

How responsible are ISPs for their customers' behaviour?

This question was addressed by the EU Electronic Commerce Directive 2000/31/EC, which was implemented in the UK by the Electronic Commerce Regulations in 2002. Essentially, ISP responsibility depends on what the ISP does:

1. Mere conduit
2. Caching
3. Hosting

ISP as Conduit

This is the situation where the ISP does no more than transmit data to/from internet. The ISP does not initiate transmissions, or select/modify data – though can store data as part of the transmission process.

When this is the case, the ISP is:

- Not liable for any civil damages.
- Not open to any criminal sanction.

ISP as Caching Service

If information is subject to automatic, intermediate and temporary storage - for instance to improve the efficiency of transmission to other recipients upon their request – the ISP is regarded to be acting as a caching service.

In this case, the ISP is not responsible, provided they:

- Do not modify information.
- Comply with conditions on access to the information.
- Comply with any rules regarding the updating of information, as specified and used by industry practice.
- Do not interfere with the lawful use of technology, as widely recognised and used by industry.
- Act expeditiously to remove or disable access to the information once made aware that it has been removed at the source of the transmission or access to it has been disabled, or that a court has ordered such removal or disablement.

This is just a complex way of stating whether or not the ISP is following Industry standard practice as a caching service.

ISP as Host

The ISP is not liable if:

- It did not know anything unlawful was going on.

- Where a claim of damages is made, it did not know anything which should have led it think something unlawful was going on.
- When it found something illegal was going on, it acted expeditiously to remove the information or disable access.
- The customer was not acting under the authority or control of the ISP.

UK ISPs are able to release (or be compelled by a court to release) information pertaining to anonymous posting on blogs.

In the US, ISPs are far better protected – a hosting ISP would be roughly equivalent to a Caching ISP. On top of this, US ISPs cannot be compelled to release information unless a serious crime is involved.

National Boundaries

Suppose a crime is committed in country A and then the criminal moves to country B. If there's an extradition treaty in place, then the criminal can be arrested in B and sent back to A - but only if crime is also illegal in country B.

Extraditions are complex, take a *long* time, and often fail.

The criminal, generally, would be safe from prosecution in country B. However certain countries claim extra-territorial jurisdiction. The UK, for instance, will prosecute child abuse committed in other countries.

The Internet

Suppose you live in country A, and publish a website which is legal in country A but a criminal offence in country B.

- You cannot be prosecuted in A
- It's highly unlikely you'll be extradited to B
- It's probably unwise to visit country B

Case Study: Gerald Töben

Germain-born Australian citizen Gerald Töben was imprisoned in 1998 in Germany. Following his release, he moved to Australia, where he published a holocaust denial website. The website was issued with a takedown request by the Australian Government in 2000.

Töben attempted to fly to US via Heathrow in 2008. He was arrested in the UK on behalf of the German government, though extradition (eventually) failed. This was partly because while Holocaust denial is illegal in Germany, UK law allows anybody to express an opinion.

The German Government has indicated it will continue with future extradition attempts in EU countries.

Convention on Cybercrime

In 2001, the Council of Europe approved a draft convention on cyber-crime. Its aim is to promote cooperation and harmonize existing laws, and focusses on:

- Child pornography

- Copyright infringement
- Computer Fraud
- (Optionally) Religious and Racial hatred

As of March 2016, 49 countries have signed and ratified the convention, while 6 have signed but not ratified. Russia has opposed it on grounds of violation of sovereignty. India and Brazil have declined because they weren't involved in the drafting.

Civil Law

As we've already covered – most contracts will make clear which country has jurisdiction, while IP rights are usually determined by international agreements.

In other cases, there's often a choice.

Consider a US ISP with a London office. An Italian customer of the ISP posts a website defaming a French politician. The politician can take action in any of the involved countries:

- **US** – expensive and defamation laws are weak;
- **Italy** – likely to result in a long (and complex) legal battle;
- **France** – probably easiest to win but will have no effect; or
- **UK** – Strong anti-defamation laws;

but will need to argue *this* is the correct court to take action in.

Defamation

Defamation covers statements which damage a person's reputation. In English law, spoken defamation is called **slander**, while written is called **libel**.

Consider a student blog hosted by our University. A student claims Dr. Smyth is corrupt. Dr. Smyth can now sue for libel, either:

1. The student, who's unlikely to have any money; or
2. The University

The Defamation Act (1996) defends anybody who:

- Is not the author, editor or publisher;
- Took reasonable care in relation to publication; or
- Did not know, and had no reason to believe, publication constituted a defamatory statement.

ISPs typically receive a lot of such complaints. Assessing each claim is costly and time consuming, so ISPs are far more likely just to censor any potential defamation.

The United States

Most internet content originates from the US. Suppose a US citizen writes a website defaming our hypothetical Dr. Smyth, and the website is hosted by a US ISP. Smyth can only take action if the ISP has legal presence in the UK, and even then, there'll only be limited effect on the circulation of the website.

The US citizen (and ISP) would be able to claim:

- "We are governed by US law - and thus the 1st amendment."
- "We cannot reasonably know law in other countries."
- "UK law has no jurisdiction over us."

Obscene Publications

The definition of pornography varies internationally. Is it art? Literature? Also, what constitutes possession, distribution and creation?

Under UK law, a publication is considered obscene if its effect or the effect of any one of its items is, *if taken as a whole* such as to tend to deprave and corrupt persons *who are likely* having regard to all relevant circumstances, to read or hear the matter contained or embodied in it.

Publication and distribution is illegal, while possession is not illegal except for material involving:

- Children (under the Protection of Children Act (1978)) -
  - Does not need to be obscene
  - Possession is an offence
  - Severe penalties
- Other abuse or abuse/violence promoting material –
  - emphasis on shutting down producers

Under US Law, since the 1950s, American pornographers have invoked the 1st amendment on freedom of speech in defence – although this provides no defence if children are involved. To combat this, there is a strong emphasis on controlling access, via content ratings, and age verification.

Spam

Spam is unsolicited email. Some technical solutions to spam include:

- Closing loopholes in email servers
- Machine learning/NLP techniques
- Virus detection
- Stop lists of sites

In the UK, spam is governed by Privacy and Electronic Communications (EC Directive) Regulations (2003):

- Spam can only be sent to individuals with their consent
- Spam without a valid return address (and opt out) is illegal
- If email is gained from sale of goods, it can be used for spam as long as customer has clear instructions for opting out.

In the US, Spam is governed by the Controlling the Assault of Non-Solicited Pornography and Marketing Act (2003). CAN-SPAM is far weaker, with spam being considered legal as long as the spammer has not received request by receiver not to receive spam, and the spam contains valid address for opting out – even if this allows for verification of active email addresses for further spamming.

Case Study: Lord McAlpine

On the 2nd November 2012, BBC Newsnight alleged an unnamed Senior Tory was involved in child abuse during the 1970s in a care home in N. Wales. The Interviewed victim did not name the senior Tory.

However, several Twitter users alleged Lord McAlpine, including the wife of the Speaker of the House of Commons - Sally Bercow - with this tweet:

Many others retweeted and replied with their own comments.

Later, Guardian journalists demonstrated that Lord McAlpine was definitely not the alleged abuser. The BBC went into Chaos, with extreme criticism leading to the BBC's Director General to resign.

Lord McAlpine considered legal action against both BBC and a collection of "high-profile" Twitter users, and indeed won against Bercow – who after the ruling said:

> *"The High Court found that my tweet constituted a serious libel, both in its natural meaning and as an innuendo. [...] I remain sorry for the distress I have caused Lord McAlpine and I repeat my apologies. Today's ruling should be seen as a warning to all social media users."*

The warning is this: Internet chat is effectively internationally published, and can be legally significant.

Lecture Eight – Ethics

Ethics is the branch of philosophy which considers what is right and wrong behaviour.

Most people consider do themselves to be "good" – that is:

- Responsible
- Decent
- Honest

However, obviously, bad things *do* happen. A reasonable way of looking at this fact is that **much evil is done by not considering ethics more seriously.** Sometimes the ethics of a situation are complex, and a solution that benefits all parties does not exist.

Case Study: Volkswagen Emissions Scandal

In September 2015, the US Environmental Protection Agency found that Volkswagen had intentionally programmed engines to activate certain emissions controls only during laboratory emissions testing - real-world emissions of certain pollutants was up to 40x greater than in the lab tests.

VW American CEO claimed that this was down to rogue software engineers, but... *come on*.

Whether or not the software engineers were rogue, *someone* wrote the code. What would you have done if you'd been asked to do this?

Moral Philosophy

Philosophy is the rational analysis of assumptions and arguments. Moral Philosophy in particular asks basic questions:

- What does it mean to be/do good?
- What is wrong/evil?
- How can we make sure we live a "good life"?

Moral Philosophy is not directly practical. It doesn't tell us what to do - rather how to evaluate what we do within a moral framework.

Why is Stealing Wrong?

We take many aspects of our morality for granted, in that often it is not immediately clear *why* a particular behaviour is wrong. Let's look at stealing as an example, and the reasons why it's considered wrong:

- **Religion** – Various religious texts condemn theft, but not everybody believes in a religion. Surely atheists can be moral too?
- **Law** – Laws also condemn theft – but remember, slavery was once permitted by law in the US, and institutionalised racial segregation and discrimination (Apartheid) was a thing in South Africa up until 1991.
- **Social Norms** – We often find our morals governed by the morals of those around us – but does that mean morality is just like fashion or popular tastes in music?

Discussion Stoppers

According to Tavani (2011) there are four objections to moral discourse:

1. **Disagreement** - People disagree on solutions to moral issues, but then again there are also disagreements in all aspects of science. The vast majority of society agrees on the major points of morality (don't steal, don't kill, wear clean clothes in computer labs).
2. **A feeling of "Who am I to judge others?"** – While this feeling is somewhat justified, sometimes judgement is necessary. Think about human rights abuses: sometimes we need to intervene.
3. **Privacy of Morality** – Morality can be considered a private matter, but the actions of you and me impact others.
4. **Moral Relativism** – Perhaps morality is a matter for individual cultures to decide, but this is difficult to uphold where there are countries that practice female circumcision and slavery, and maintain low ages of sexual consent – if there's a requirement for consent at all. Generally, there is a considerable agreement of morality across cultures, and an agreement that the morality of cultures is unacceptable.

Here's a statement by German theologian Martin Niemöller (1892-1984) to consider:

> "First they came for the communists, and I didn't speak out because I wasn't a communist.
> Then they came for the trade unionists, and I didn't speak out because I wasn't a trade unionist.
> Then they came for the Jews, and I didn't speak out because I wasn't a Jew.
> Then they came for me, and there was no one left to speak for me."

Case Study: Milgram's Experiment

In 1963, Psychologist Stanley Milgram conducted an experiment focussing on the conflict between obedience to authority and personal conscience, inspired by the Nuremburg War Criminal Trials after WWII.

Participants were paired up, and it was decided apparently by luck of the draw who would play the role of "learner", and who would play the "teacher" – however the draw was fixed so that the "learner" was always one of Milgram's assistants *pretending* to be a participant.

The teachers were asked to help administer an experiment on learning word combinations, where they must administer an electric shock (via electrodes, from a separate room) for every wrong answer. They were told that they should increase the voltage each time.

The participant gave mainly wrong answers (on purpose). When the teacher refused to administer a shock, the experimenter (another of Milgram's associates) would read a series of orders – moving onto the next prod each time there was a disobedience. The prods were:

1. "Please continue."
2. "The experiment requires you to continue."
3. "It is absolutely essential that you continue."
4. "You have no other choice but to continue."

The trial would end after disobedience of the fourth prod.

There was a high degree of stress for most volunteers, but 65% of volunteers willingly gave the maximal 450-volt shock.

Utilitarianism

Jeremy Bentham (1725 AD) is regarded as the founder of modern utilitarianism. He formulated the Hedonic Calculus, which worked based on the theory that any pleasure or pain can be measured and quantified

John Stuart Mill formulated the "greatest-happiness principle", which presented the idea that the correct action to take is the one that will produce the greatest aggregate amount of happiness (pleasure – pain) in a group.

The Law

Humans tend to be selfish, but and the greatest-happiness principle requires altruism to be able to work. The Law exists to enforce altruism for the benefit of society. This idea allows us to return to our discussion on theft and define in terms of morality why it is wrong:

- Stealing increases the happiness of the thief.
- Stealing lowers happiness of original owner.
- It also makes the rest of society feel insecure.

Thus, there are laws against theft in order to protect society. Punishment should be *just enough* to deter anti-social acts - but nothing more.

Problems with Utilitarianism

How do you quantify pleasure and pain? How do we decide what is good if we don't know the consequences? Should I give £20 to two pensioners or 20p to 200 pensioners?

Utilitarianism ignores the needs of an individual. This does cause issues. For instance:

1. Specialist Medical treatments need funding.
2. Funding comes from taxes.
3. Taxes make everybody (else) unhappy.
4. Therefore, perhaps we should stop medical treatments except for common illnesses.

What if your house was on fire – who would you rescue first?

- Your mother, whom you love very much.
- The vicar, who helps the community (and is having tea with your mum)
- The young burglar upstairs, who's a menace to society.

Case Study: Stanford Prison Experiment

Phillip Zimbardo (1971) conducted an experiment where 24 student volunteers were classed as either jailers or prisoners, and placed in a mock prison in the basement of the department.

There was an orientation session for guards, who were given mock uniforms and wooden batons, and advised *not to hurt* prisoners but instead create fear, boredom and anxiety.

On the second day, guards were observed attacking prisoners using fire extinguishers. Within *six*, guards were observed psychologically torturing prisoners. Soon an "honour" cell was formed – which rewarded good prisoner behaviour. The prisoners were observed to (mostly) accept torture, and to gang up on prisoners who refused to continue the experiment.

As with Milgram, it was clear that "situational attribution" is at play: the situation drives the behaviour, rather than the innate personality characteristics (dispositional attribution). Therefore, we can see that environments can be "corrupting".

Intuitionism

Intuitionism is the theory that primary truths and principles (especially those of ethics and metaphysics) are known directly by intuition.

Humans can mostly be observed to adhere to principles of "the right" actions, such as:

- Promoting the happiness of people
- Refraining from harming others
- Treating people justly
- Telling the truth
- Etc. etc.

Sometimes principles do conflict but such cases can be resolved using rational intuition.

Problems with Intuitionism

One of the main issues with Intuitionism is that the principles are not always self-evident. Another is the occasional incompatibility of principles. The very fact that we're able to *debate* what is right and wrong is evidence that morality cannot just be a set of objective facts.

Duty Ethics (or Kantian Ethics)

Duty Ethics present the idea that one cannot treat another person as a means to an end, and that a person must maintain their moral duty to seek an end that is equal for all people.

The Golden Rule

"One should treat others as one would like others to treat oneself. One should not treat others in ways that one would not like to be treated."

"Hence, (keeping these in mind), by self-control and by making dharma (right conduct) your main focus, treat others as you treat yourself." Mahābhārata (~9th century BC, maybe)

"Never impose on others what you would not choose for yourself." – Confucius (5th century BC)

"And as ye would that men should do to you, do ye also to them likewise" Luke 6:31 (70-90 AD ish)

A Summary

Most of us regard ourselves as good people, and for the most part, we probably are. A useful aphorism to bear in mind is Hanlon's Razor: "Never attribute to malice, that which can be explained by stupidity."

However, many studies show that (good) people can behave badly given the right conditions, and history constantly teaches us that people can behave in a *much* worse manner.

"The unexamined life is not worth living" - Socrates

Ethical Dilemmas

Access

You are a computer system manager. An employee is out sick and on behalf of the entire development team, another employee requests that you copy all files from the sick person's computer to theirs so that they can do some work due to an urgent deadline which if missed will have serious financial implications for the entire company. What do you do?

The Trolley Problem

You are the driver of one of a new line of computer controlled trolleys. Unfortunately lack of funding has meant that the software hasn't been fully tested and the trolley has a fatal flaw – when you brake, you actually accelerate! The trolley is speeding to a split in the road – the left route means you will crash into a group of 5 workmen. It's certain you'll kill them. The right route means you'll crash into a lone workman – again killing him. What do you do?

The Trolley Problem, Continued

Most days you have your lunch overlooking a bridge with a wonderful view over the city. Today however you notice an automated trolley speeding towards five men working below (possibly piloted by a panic-stricken computer science student) The men will certainly be killed if you don't do something. Fortunately, there is a very fat man sitting with his legs dangling over the bridge. If you push him to the road below, it's certain to stop the trolley and save the five men working in the road. Unfortunately, this will also kill the man.

Virus

A fellow student wishes to model how viruses spread by creating a benign computer virus to be spread via email. Upon infection, the virus asks the user for consent to:

1. Replicate itself
2. Send back confirmation to the student
3. Self-delete itself within 7 days of infection.

If the user does not give consent, it instantly disinfects the computer and deletes itself without sending any data or changing any files. Is this a good idea?

The Health Lottery:

Every year people die due to the lack of transplant organs. One healthy person has several healthy organs – heart, kidneys, lungs, liver, blood, eyes, etc. Therefore, if we were to select one person and force them to donate all their organs, we could save several lives.

Unfortunately, this would be fatal – but we'd kill one person and save several. Therefore, here's a proposal: Hold a Health Lottery once a month for all citizens between 18 and 30. Selected person(s) will be forcibly euthanized and body parts used to save the lives of many.

A Summary of Relevant Legislation

Architects Act (1997):

Prevents individuals not recognised by the ARB from advertising themselves as architects.

European Convention on Human Rights:

Legislation upon which much of the UK's human rights laws are based.

Computer Misuse Act (1990):

Introduced computer-related offences, partially in response to the R v. Gold & Schifreen (1988) case.

Computer Misuse Act (2004):

Revised the CMA (1990), by increasing punishment and criminalised DoS attacks.

Police and Justice Act (2006):

Amends the CMA.

Data Protection Act (1984):

Original legislation regarding data protection.

Data Protection Act (1998):

Revised legislation regarding data protection, introducing several definitions and eight principles.

Investigatory Powers Act (2016):

Grants additional investigatory powers to several government departments, in particular with regards to computers and internet connections.

Regulation of Investigatory Powers Act (2000):

Legalises the interception of computer, telephone and postal messages.

Freedom of Information Act (2000):

Provides public access to information held by public authorities.

Unfair Contract Act (1977):

Makes it impossible to limit liability in the result of a death or personal injury.

Sale of Goods Act (1979):

Enforces that goods are fit for purpose when sold to consumers.

Goods and Services Act (1982):

Enforces that goods are produced with reasonable care.

Copyright, Design and Patents Act (1988):

Legislation regarding copyright.

Copyright (computer programs) Regulations Act (1992):

Legislation regarding copyright.

Patents Act (1977):

Governs the issuing and enforcing of patents.

European Patent Convention:

States that software cannot be patented.

Copyright, Design and Patents Act (1988):

States that software cannot be patented.

Public Interest Disclosure Act (1998):

Legislation regarding the circumstances under which information can be disclosed by employees of a business.

Trade Marks Act (1994):

Legislation regarding trademarks.

ACAS Code of Practice (2009):

Provides a guide to best practice for employee dismissal.

Transfer of Undertakings, Protection of Employment (TUPE):

Legislation governing employment following company acquisitions.

Enterprise and Regulatory Reform Act:

Replaces TUPE.

The Equality Act (2010):

Consolidates all pervious discrimination laws into a single piece of legislation.

Electronic Commerce Regulations (2002):

Implements the EU Electronic Commerce Directive 2000/31/EC, by governing ISP responsibility.

Convention on Cybercrime (2001):

Council of Europe legislation focussing on child pornography and several other computer-related crimes.

Defamation Act (1996):

Defends third parties against claims of defamation.

Protection of Children Act (1978):

Legislates against obscene publications involving children.

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

Governs spam-related issues in the UK.

Controlling the Assault of Non-Solicited Pornography and Marketing Act (2003):

Governs spam-related issues in the US.

A Summary of Relevant Case Studies

London Ambulance Computer-Aided Dispatch Service Failure (1992):

Software-caused ambulance scheduling incident in which emergency response times in London rose to several hours.

Therac-25 Disaster (1986-87):

Incident in which software controlling a radiation therapy machine caused malfunctions, killing six patients on separate occasions.

Facebook Hacking (2011):

UK hacker gained access to a US citizen's Facebook and email accounts and was charged under the CMA.

R v. Gold & Schifreen (1988):

Complex case where individuals gained unauthorised access to a subsystem of BT's computers. Unsatisfactory court result led to the introduction of the CMA.

Gary McKinnon (2001-02):

Complicated extradition process after Scottish sys-admin hacks into US military and NASA computers.

Durant v. FSA (2003):

Barclays customer incites FSA investigation, and attempts to use Data Protection Act to find out the outcome.

Gaskin v. United Kingdom (1989):

Child abuse victim challenges Social Services for access to his social service records.

St. Albans vs ICL (1996):

ICL delivers faulty software to St. Alban's council, resulting in a loss of £50M in uncollected community tax.

Kim Dotcom:

A German internet tycoon, previously owned Megaupload Ltd.

Richard Wiseman:

MIT hacker launches the GNU project.

Tapere v. Lewisham NHS Trust (2009):

Constructive dismissal case involving a relocated employee of Primary Care Trust.

McDonalds Dismissal (2012):

Unfair dismissal of McDonalds employee who added too many chocolate sprinkles to a fellow employee's McFlurry.

Gerald Töben:

Extradition to Germany of Australian Holocaust denial website publisher fails following UK arrest.

Lord McAlpine (2012):

Defamation involving a senior Tory accused of child abuse and a collection of Twitter users, including the Speaker's wife, Sally Bercow.

Volkswagen Emissions Scandal (2015):

US EPA finds Volkswagen deliberately programmed their cars to produce false emission levels under laboratory conditions – executives blame software developers.

Milgram's Experiment (1963):

Psychology experiment focussed on obedience and personal conscience.

Stanford Prison Experiment (1971):

Behavioural study where student volunteers were "jailed" and observed.