**Chapter 11 Lecture 16**

**Intellectual Property Rights**

**Intellectual Property Rights**

If someone steals your bicycle, you no longer have it. If someone takes away

a computer belonging to a company, the company no longer has it.

If you invent a drug that will cure all known illnesses and leave the formula on

your desk, someone can come along, read the formula, remember it, and go

away and make a fortune out of manufacturing the drug. But you still have the

formula even though the other person now has it as well. This shows that

the formula – more generally, any piece of information – is not property in the

same way that a bicycle is.

**Intellectual property**

Property such as bicycles or computers is called tangible property, that is,

property that can be touched. It is protected by laws relating to theft and

damage.

Property that is intangible is known as *intellectual property*. It is

governed by a different set of laws, concerned with *intellectual property*

*rights*, that is, rights to use, copy, or reveal information about intellectual

property.

**Laws**

The international law relating to trade marks and patents is based on the Paris Convention, which was signed in 1883. The Berne Convention, which lies at the basis of international copyright law, was signed in 1886.

**DIFFERENT TYPES OF INTELLECTUAL PROPERTY RIGHTS**

* *Copyright* is, as the name suggests, concerned with the right to copy something. It may be a written document, a picture or photograph, a piece of music, a recording, or many other things, including a computer program.
* *Patents* are primarily intended to protect inventions, by giving inventors a monopoly on exploiting their inventions for a certain period.
* *Confidential information* is information that a person receives in circumstances that make it clear they must not pass it on.
* *Trade marks* identify the product of a particular manufacturer or supplier.

**COPYRIGHT**

* Copyright is associated primarily with the right to copy something. The ‘something’ is known as the work.
* Only certain types of work are protected by copyright law. The types that concern us here are ‘original literary, dramatic, musical or artistic’ works. The 1988 Copyright Design and Patents Act states that the term ‘literary work’ includes a table or compilation, a computer program, preparatory design material for a computer program and certain databases.

Copyright comes into existence when the work is written down or recorded in some other way. It is not necessary to register it in any way.

**The rights of the copyright owner**

Copyright law gives the owner of the copyright certain exclusive rights. The rights that are relevant to software and, more generally, to written documents, are the following:

* The right to make copies of the work: Making a copy of a work includes copying code from a disc into RAM (random access memory) in order to execute the code. It also includes downloading a page from the web to view on your computer, whether or not you then store the page on your local disk.
* The right to issue copies of the work to the public, whether or not they are charged for it.
* The right to adapt the work: This includes translating it – whether from English to Chinese or from C to Java.

**What you can do to a copyright work**

The law specifically permits certain actions in relation to a copyright work and some of these are of particular relevance to software.

* First, it is explicitly stated that it is not an infringement of copyright to make a backup of a program that you are authorized to use. However, only one such copy is allowed. If the program is stored in a filing system with a sophisticated backup system, multiple backup copies are likely to come into existence.
* Secondly, you can ‘decompile’ a program in order to correct errors in it. You can also decompile a program in order to obtain the information you need to write a program that will ‘interoperate’ with it, provided this information is not available to you in any other way.
* Thirdly, you can sell your right to use a program in much the same way that you can sell a book you own. However, when you do this, you sell all your rights. In particular, you must not retain a copy of the program.

**Databases**

Copyright subsists in a database if ‘its contents constitute the author’s own intellectual creation’. There are many databases that do not satisfy this criterion but which, nonetheless, require a lot of effort and a lot of money to prepare. Examples might include databases of hotels, pop songs, or geographic data. In order to encourage the production of such modest but useful databases, regulations were introduced in 1997 to create a special intellectual property right called the database right.

The database right subsists in a database ‘if there has been substantial investment in obtaining, verifying or presenting the contents of the database’.

* It lasts for 15 years and prevents anyone from extracting or reusing all, or a substantial part of, the database without the owner’s permission.

**Copyright infringement**

Anyone who, without permission, does one of the things that are the exclusive right of the copyright owner is said to infringe the copyright.

* Primary infringement takes place whenever any of the exclusive rights of the copyright owner is breached.
* Secondary infringement occurs when primary infringement occurs in a business or commercial context. Can lead to heavy fine and even imprisonment. It involves piracy of software for trading or business usage.

**Ownership**

* As a general rule, the copyright in a work belongs initially to its author. If the work is jointly written by several authors, they jointly own the copyright.
* If the author is an employee and has written the work as part of his or her job, then the copyright belongs to the employer, unless there is an explicit, written agreement to the contrary.
* The employer owns the copyright only if the author is legally an employee. If the author is an independent contractor, he or she will own the copyright unless there is an agreement to the contrary. For this reason, if a company commissions an independent contractor (freelance programmer) to write software, it is important to have a formal agreement regarding ownership of the copyright in the resulting software.

**Licensing**

It is very common for the owner of the copyright in a piece of software to

license other people or organizations to carry out some of the activities that

are otherwise the exclusive right of the copyright owner. The copyright

remains the property of the owner, but the *licensees* (the people to whom the

software is licensed) acquire certain rights.

**PATENTS**

A patent is a temporary right, granted by the state, enabling an inventor to prevent other people from exploiting his invention without his permission.

* Unlike copyright, it does not come into existence automatically; the inventor must apply for the patent to be granted. However, the protection it gives is much stronger than copyright, because the grant of a patent allows the person owning it (the *patentee*) to prevent anyone else from exploiting the invention, even if they have discovered it for themselves.

**Patents need**

* Patents were originally intended to encourage new inventions, and in particular to encourage the disclosure of those new inventions.
* Inventors are often hesitant to reveal the details of their invention, for fear that someone else might copy it. A government-granted temporary monopoly on the commercial use of their invention provides a remedy for this fear, and so acts as an incentive to disclose the details of the invention. After the monopoly period expires, everyone else is free to practice the invention. And because of the disclosure made by the inventor, it is very easy to do so.

**What can be patented?**

In Europe, the law relating to patents is based on the European Patent Convention. This was signed in 1973 by 27 European countries, and came into force in 1978. The UK’s obligations under the Convention were implemented in the Patents Act 1977, although there have been some subsequent modifications. The 1977 Act states that an invention can only be patented if it:

* is new;
* involves an inventive step;
* is capable of industrial application;
* is not in an area specifically excluded.

Similar criteria apply in all the countries that are signatories to the Convention.

**What Patent Act Excludes……**

Following the European Patent Convention, the Patents Act 1977 excludes the following:

* Scientific theories: The theory of gravity cannot be patented although a machine that uses it in a novel way could be.
* Mathematical methods: This means, for example, that the methods used for carrying out floating point arithmetic cannot be patented. A machine that uses the ideas can however be patented.
* A literary, dramatic, musical or artistic work or any other aesthetic creation: As we have already seen, these are protected by copyright.
* The presentation of information: Again this is covered by the law of copyright.
* A scheme, rule or method for performing a mental act, playing a game or doing business, or a program for a computer.

**Obtaining a patent**

Unlike copyright, which comes into existence automatically when the protected work is recorded, whether in writing or otherwise, a patent must be explicitly applied for. Applying for a patent can be an expensive and time consuming business.

Patents are granted by national patent offices. Inventors who want protection in several different countries must, in principle, apply separately to the patent offices of each country.

**Enforcing a patent**

The grant of a patent is not a guarantee that it can be effectively enforced. If

you own a patent and you find that someone is infringing the patent, you may

have to go to the courts to enforce your rights.

The problem is that enforcing a patent that you own or challenging a patent held by someone else is a time-consuming and expensive process.

**Software patents**

In the USA software can be patented if:

* it is part of a product that is itself eligible to be patented;
* it controls a process that has some physical effect;
* it processes data that arises from the physical world.

The European Patent Office has been granting patents for software since 1998, as has the UK Patent Office.

Patent offices in the different European countries have adopted different policies towards the patenting of software, with the result that there is much confusion about what is and what is not patentable.

The result is that there is a conflict between the law and practice, a very undesirable situation.

http://www.legislation.gov.uk/ukpga/1988/48/resources

On the one hand, it is illogical and unfair that something that would be clearly patentable if implemented completely in hardware should not be patentable if implemented in software. Furthermore, patents encourage investment because:

* a patent is a well-defined asset that allows shareholders and, in particular,
* venture capitalists to be confident that their investment is producing something of value;
* patents ensure that the benefit of research and development accrues to the people who financed it.

**TRADE MARKS AND PASSING OFF**

The law regarding trade marks in the UK is based on the Trade Marks Act 1994, which consolidated and updated existing legislation. The Act defines a trade mark as:

**. . . any sign capable of being represented graphically which is capable of distinguishing goods or services of one undertaking from those of other undertakings. A trade mark may, in particular, consist of words (including personal names), designs, letters, numerals or the shape of goods or their packaging.**

Even where a trade mark is not registered, action can be taken in the civil courts against products that imitate the appearance or ‘get up’ of an existing product. This is known as the tort of ‘passing off’.

**Trade mark**

There are comprehensive rules limiting what can be registered as a trade mark. Place names and the names of people, for example, will not generally be accepted for registration.

The1994 Act makes it an offence to:

* apply an unauthorized registered trade mark (that is, a registered trade mark that you do not own or do not have the owner’s permission to use) to goods;
* sell or offer for sale (or hire), goods or packaging that bear an unauthorized trade mark;
* import or export goods that bear an unauthorized trade mark;
* have in the course of business, goods for sale or hire goods (or packaging) that bear an unauthorized trade mark.

**Domain Names**

Internet domain names are ultimately managed by the Internet Corporation

for Assigned Names and Numbers (ICANN). ICANN is an internationally

organized, non-profit making corporation. Its main responsibility is ensuring

the ‘universal resolvability’ of internet addresses; that is, ensuring that

the same domain name will always lead to the same internet location

wherever it is used from and whatever the circumstances. In practice, ICANN

delegates the responsibility for assigning individual domain names to other

bodies, subject to strict rules.

Domain names were originally meant to be used just as a means of simplifying the process of connecting one computer to another over the internet.

However, because they are easy to remember, they have come to be used as away of identifying businesses. Indeed, they are frequently used in advertising.

Conversely, it is not surprising that companies should want to use their trade marks or their company names as their internet domain names.

* The potential for conflict between trade marks and domain names is inherent in the two systems.
* Trade marks are registered with public authorities on a national or regional basis. The owner of the trade mark acquires rights over the use of the trade mark in a specific country or region.
* Identical trade marks may be owned by different persons in respect of different categories of product.
* Domain names are usually allocated by a nongovernmental organization and are globally unique; they are normally allocated on a first come, first served basis. This means that if different companies own identical trade marks for different categories of product or for different geographical areas, only one of them can have the trade mark as domain name, and that will be the first to apply.

**Cyber squatting**

* An example of cybersquatting is when someone registers a domain name that is similar to an existing domain with the intent of profiting from it. Here are some examples of cybersquatting:
* France2.com and France3.com

They then offer to sell these domain names to the owner of the trade mark at an inflated price. It is usually cheaper and quicker for the trade mark owner to pay up than to pursue legal remedies, even when these are available.

**WIPO report I**

In 1999, the WIPO published a report entitled ‘The management of

internet names and addresses: Intellectual property issues’. WIPO is an

international organization with 177 states as members. The report recommended

that ICANN adopt a policy called the Uniform Domain Name

Dispute Resolution Policy (UDRP), which includes specific provisions

against cyber squatting. This policy has proved reasonably effective. Within

two years, over 3,000 complaints had been dealt with by one of the arbitration

centres alone, with 80 per cent being resolved.

**WIPO report II**

In 2001, WIPO published a second report, ‘The recognition of rights and

the use of names in the internet domain system’. This addresses conflicts

between domain names and identifiers other than trade marks.

Examples:

The use of personal names in domain names or the use of the names of particular peoples or geographic areas by organizations that have no connection with them. These conflicts are more difficult to deal with than conflicts between trade marks and domain names because the international framework that underlies trade marks is missing in these other cases.

**Chapter 13 Lecture 17**

**Data Protection, Privacy and Freedom of Information**

Background :

* Public concern about data protection was first aroused when it was realized

that a very large amount of data about individuals was being collected and

stored in computers and then used for purposes that were not only different

from those intended when the data was collected, but also unacceptable.

* There were also concerns that unauthorized people could access such data

and that the data might be out of date, incomplete or just plain wrong.

**Data Protection Act 1984**

These concerns surfaced in the 1970s.

They were particularly strong in the UK and the rest of Europe and led to a Council of Europe Convention on the subject.

The first UK Data Protection Act, passed in 1984, was designed to implement the provisions of the Convention.

**The Data protection Act 1984**

It was designed to protect individuals from:

* the use of inaccurate personal information or information that is incomplete or irrelevant;
* the use of personal information by unauthorized persons;
* the use of personal information for purposes other than that for which it was collected.

**Key responsibilities**

* It was meant primarily to protect individuals against the misuse of personal data by large organizations, public or private.

Example :

Such misuse might occur, for example, if data-matching techniques are used on credit card records to build up a picture of a person’s movements over an extended period.

* Further, errors can often creep into data that has been collected or data may be interpreted in a misleading way, and it was difficult to persuade the holders of the data to correct these.

Example:

Credit rating agencies might advise against giving a person a loan because someone who previously lived at the same address defaulted on a loan.

**Progressing of the Act**

By the mid-1990s, a different danger had become apparent.

As individuals began to use the internet for an ever wider range of purposes, it became possible to capture information about the way individuals use the internet and to build profiles of their habits that can be used for marketing purposes and also, perhaps, for more sinister purposes such as blackmail.

What is more, this can be done by much smaller and much shadowier organizations than those that were the object of the 1984 Act.

These and other concerns led in 1995 to the European Directive on Data Protection which, in turn, led to the 1998 Data Protection Act.

**DATA PROTECTION**

The first UK legislation on data protection was the 1984 Data Protection Act. However, this was taken over by the 1998 Act.

* The Act defines a number of terms that are widely used in discussions of data protection issues. In some cases these are different from the terms used in the 1984 Act.

To get a clear picture we need to be familiar with some terminologies regarding Data protection

**Terminology**

* *Data* means information that is being processed automatically or is collected with that intention or is recorded as part of a relevant filing system
* *Data controller* means a person who determines why or how personal data is processed. This may be a legal person or a natural person.
* *Data processor*, in this context, means anyone who processes personal data on behalf of the data controller and who is not an employee of the data controller. This might include an application service provider, such as a company that provides online hotel booking services.
* *Personal data* means data which relates to a living person who can be identified from data, possibly taken together with other information the data controller is likely to have it recorded as part of a relevant filing system.
* *Data subject* means the individual who is the subject of personal data.
* *Sensitive personal data* means personal data relating to the racial or ethnic origin of data subjects, their political opinions, their religious beliefs, whether they are members of trade unions, their physical or mental health, their sexual life, or whether they have committed or are alleged to have committed any criminal offence. The rules regarding the processing of sensitive personal data are stricter than for other personal data.

**Processing**

* *Processing* means obtaining, recording or holding the information or data

or carrying out any operations on it, including:

(a) organization, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data.

**Data protection principles**

The 1998 Act lays down eight data protection principles, which apply to the collection and processing of personal data of any sort.

Data controllers are responsible for ensuring that these principles are complied with in respect of all the personal data for which they are responsible.

***First data protection principle***

“Personal data shall be processed fairly and lawfully and in particular shall not

be processed unless (a) at least one of the conditions in Schedule 2 is met and

(b) in the case of sensitive personal data, at least one of the conditions in

Schedule 3 is also met.”

The most significant condition in Schedule 2 of the Act is that the data subject has given their consent. If this is not the case, then the data can only be processed if the data controller is under a legal or statutory obligation for which the processing is necessary.

For processing sensitive personal information, Schedule 3 requires that the data subject has given explicit consent.

***Second data protection 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 those purposes.”

Data controllers must notify the Information Commissioner of the personal

data they are collecting and the purposes for which it is being collected.

***Third data protection principle***

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

***Fourth data protection principle***

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

* While this principle is admirable, it can be extremely difficult comply with.

Examples: In the UK, doctors have great difficulty in maintaining up-to-date data about their patients’ addresses, particularly patients who are students, because students change their addresses frequently and rarely remember to tell their doctor.

Universities have similar difficulties.

***Fifth data protection principle***

“Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.”

This principle raises more difficulties than might be expected:

* It is necessary to establish how long each item of personal data needs to be kept. Auditors will require that financial data is kept for seven years. Action in the civil courts can be initiated up to six years after the events complained of took place so that it may be prudent to hold data for this length of time. It is appropriate to keep some personal data indefinitely (e.g. university records of graduating students). In all cases, the purpose for which the data is kept must be included in the purposes for which it was collected.
* Procedures to ensure that all data is erased at the appropriate time are needed, and this must include erasure from backup copies.

***Sixth data protection principle***

“Personal data shall be processed in accordance with the rights of data subjects under this Act.”

***Seventh data protection principle***

“**Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**”

It implies the need for access control (through passwords or other means), backup procedures, integrity checks on the data, vetting of personnel who have access to the data, and so on.

***Eighth data protection principle***

“Personal data shall not be transferred to a country or territory outside

the European Economic Area unless that country or territory ensures an

adequate level of protection for the rights and freedoms of data subjects in

relation to the processing of personal data.”

This principle can be viewed in two ways.

* It can be seen as protecting data subjects from having their personal data transferred to countries where there are no limitations on how it might be used.
* It can also be seen as specifically allowing businesses to transmit personal data across national borders provided there is adequate legislation in the destination country.

**Rights of Data Subjects**

The 1984 Act gave data subjects the right to know whether a data controller held data relating to them, the right to see the data, and the right to have the data erased or corrected if it is inaccurate.

The 1998 Act extends this right of access so that data subjects have the right to receive:

* a description of the personal data being held;
* an explanation of the purpose for which it is being held and processed;
* a description of the people or organizations to which it may be disclosed;
* an intelligible statement of the specific data held about them;
* a description of the source of the data.

**Data subject rights**

The 1998 Act also gives data subjects the right:

* to prevent processing likely to cause damage and distress;
* to prevent processing for the purposes of direct marketing;
* to compensation in the case of damage caused by processing of personal data in violation of the principles of the Act.

**Scope of the Act**

* There are a number of important exceptions or limitations to the right of subject access, for example: where disclosing the information may result in infringing someone else’s rights; where the data consists of a reference given by the data controller; examination candidates do not have the right of access to their marks until after the results of the examinations have been published;
* personal data consisting of information recorded by candidates during an academic, professional or other examination are exempt from the right of access.

**PRIVACY**

* The starting point is the Regulation of Investigatory Powers Act 2000, which sets up a framework for controlling the lawful interception of computer, telephone and postal communications.
* The Act allows government security services and law enforcement authorities to intercept, monitor and investigate electronic data only in certain specified situations such as when preventing and detecting crime. Powers include being able to demand the disclosure of data encryption keys.

Under the Act and the associated regulations, organizations that provide computer and telephone services (this includes not only ISPs (internet service providers) and other telecommunications service providers but also most employers) can monitor and record communications without the consent of the users of the service, provided this is done for one of the following purposes:

* to establish facts, for example, on what date a specific order was placed;
* to ensure that the organization’s regulations and procedures are being complied with;
* to ascertain or demonstrate standards which are or ought to be achieved;
* to prevent or detect crime (whether computer-related or not);
* to investigate or detect unauthorized use of telecommunication systems;
* to ensure the effective operation of the system, for example, by detecting viruses or denial of service attacks;
* to find out whether a communication is a business communication or a private one (e.g. monitoring the emails of employees who are on holiday, in order to deal with any that relate to the business);
* to monitor (but not record) calls to confidential, counselling helplines run free of charge by the business, provided that users are able to remain anonymous if they so choose.

**FREEDOM OF INFORMATION**

* The primary purpose of the Freedom of Information Act is to provide clear rights of access to information held by bodies in the public sector. Under the terms of the Act, any member of the public can apply for access to such information.
* The Act also provides an enforcement mechanism if the information is not made available. The legislation applies to Parliament, government departments, local authorities, health trusts, doctors’ surgeries, universities, schools and many other organizations. The main features of the Act are:
* There is a general right of access to information held by public authorities in the course of carrying out their public functions, subject to certain conditions and exemptions.
* In most cases where information is exempted from disclosure, there is a duty on public authorities to disclose where, in the view of the public authority, the public interest in disclosure outweighs the public interest in maintaining the exemption in question.
* There is a new office of the Information Commissioner (see the ‘Further reading’ section for the website) and a new Information Tribunal, with wide powers to enforce the rights, was created.
* A duty was imposed on public authorities to adopt a scheme for the publication of information. The schemes, which must be approved by the Information Commissioner, specify the classes of information the authority intends to publish, the manner of publication and whether the information is available to the public free of charge or on payment of a fee

**Chapter 14 Lecture 18**

**Internet Issues**

**Benefits of internet:**

The benefits that the internet has brought are almost universally recognized. It has made access to all sorts of information much easier. It has made it much easier for people to communicate with each other, on both an individual and a group basis. It has simplified and speeded up many types of commercial transaction. And, most importantly, these benefits have been made available to very many people, not just to a small and privileged group – although, of course, the internet is still far from being universally available, even in developed countries.

Inevitably, a development on this scale creates its own problems.

**Problems of internet availability**

The following three areas are mainly covered as major problems arising due to the availability of internet:

* Defamation
* Pornogarphy
* Spam

that are a matter of concern to everyone professionally involved in the internet, as well as to many other people. These are topics that cannot sensibly be discussed in technical terms alone. There are social, cultural and legal issues that must all be considered. Different countries approach these issues in very different ways but the internet itself knows no boundaries.

Every country has laws governing what can be published or publicly displayed. Typically, such laws address defamation, that is, material that makes unwelcome allegations about people or organizations, and pornography, that is, material with sexual content. They may also cover other areas such as political and religious comment, incitement to racial hatred, or the depiction of violence. Although every country has such laws, they are very different from each other.

Some countries, for example, consider that pictures of scantily clad women are indecent and have laws that prevent them from appearing in publications and advertisements. In other countries, such pictures are perfectly acceptable. In some countries, publication of material criticizing the government or the established religion is effectively forbidden, while in others it is a right guaranteed by the constitution and vigorously defended by the courts.

**Availability of internet playing the role**

The coming of the internet (and satellite television) has made these differences

much more apparent and much more important than they used to be.

Since material flows across borders so easily, it is both much likelier that

material that violates publication laws will come into a country and more

difficult for the country to enforce its own laws.

The roles and responsibilities of ISPs are a central element in the way these

issues are addressed and we therefore start by discussing the legal framework

under which ISPs operate. Then we shall look at the problems of different

legal systems. Only then can we address the specific issues of defamation,

pornography and spam.

**INTERNET SERVICE PROVIDERS**

The central issue we need to consider is how far an ISP can be held responsible for material generated by its customers. In Europe, the position is governed by the European Directive 2000/31/EC. In the UK this directive is implemented through the Electronic Commerce (EC Directive) Regulations 2002. These regulations follow the EC Directive in distinguishing three roles that an ISP may play: *mere conduit*, *caching*, and *hosting*.

The role of mere conduit (a channel) is that in which the ISP does no more than transmit data; in particular, the ISP does not initiate transmissions, does not select the receivers of the transmissions, and does not select or modify the data transmitted. It is compatible with the role of mere conduit for an ISP to store information temporarily, provided this is only done as part of the transmission process. Provided it is acting as a mere conduit, the regulations provide that an ISP is not liable for damages or for any criminal sanction as a result of a transmission.

**Caching**

The caching role arises when the information is the subject of automatic, intermediate and temporary storage, for the sole purpose of increasing the efficiency of the transmission of the information to other recipients of the service upon their request. An ISP acting in the caching role is not liable for damages or for any criminal sanction as a result of a transmission, provided that it:

* does not modify the information;
* complies with conditions on access to the information;
* complies with any rules regarding the updating of the information, specified in a manner widely recognized and used by industry;
* does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information;
* acts expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrativeauthority has ordered such removal or disablement.

**Hosting**

Where an ISP stores information provided by its customers, it is acting in a

hosting role. In this case, it is not liable for damage or criminal sanctions

provided that:

* it did not know that anything unlawful was going on;
* where a claim for damages is made, it did not know anything that should have led it to think that something unlawful might be going on; or
* when it found out that that something unlawful was going on, it acted expeditiously to remove the information or to prevent access to it, and
* the customer was not acting under the authority or the control of the service provider.

**Law across National Boundaries**

* Criminal law
* The international convention on cybercrime
* Civil law

**Criminal law**

Suppose a person, X, commits a criminal offence in country A and then moves to country B.

* Can country A ask that X be arrested in country B and sent back to A so that he can be put on trial?
* Or can X be prosecuted in country B for the offence committed in country A?

The answer to the first of these questions is that, provided there exists an

agreement (usually called an *extradition treaty*) between the two countries,

then in principle X can be extradited, that is, arrested and sent back to face

trial in A. However, this can only be done under the very important proviso

that the offence that X is alleged to have committed in A would also be an

offence in B. What is more, extradition procedures are usually extremely

complex, so that attempts at extradition often fail because of procedural

weaknesses. Within the EU, the recent proposals for a European arrest warrant

are intended to obviate the need for extradition procedures.

In general, the answer to the second question is that X cannot be prosecuted

in B for an offence committed in A. However, in certain cases some

countries, including the UK and the USA, claim *extraterritorial jurisdiction*,

that is the right to try citizens and other residents for crimes committed in

other countries; in particular, this right is used to allow the prosecution of

people who commit sexual offences involving children while they are abroad.

However, the issue of extraterritoriality is much wider than this and attempts

to claim extraterritorial jurisdiction make countries very unpopular.

**Result???**

Suppose that you live in country A and on your website there you publish material that is perfectly legal and acceptable in country A, but which it is a criminal offence to publish in country B. Then you can’t be prosecuted in country A and it is very unlikely that you would be extradited to country B. You might, however, be unwise to visit country B voluntarily.

**DEFAMATION**

Defamation means

“making statements that will damage someone’s reputation, bring them into

contempt, make them disliked, and so on.”

**Defamation Act**

The Defamation Act 1996 states that a person has a defence if they can

prove that:

* he was not the author, editor or publisher of the statement complained of,
* he took reasonable care in relation to its publication, and
* he did not know, and had no reason to believe, that what he did caused or
* contributed to the publication of a defamatory statement.

**The Internet Content Rating Association**

The Internet Content Rating Association (ICRA) is an international, independent

organization whose mission, it claims, is: ‘to help parents to

protect their children from potentially harmful material on the internet,

whilst respecting the content providers’ freedom of expression.’ Its board

includes representatives from the major players in the internet and communications

markets, including AOL, BT, Cable and Wireless, IBM, Microsoft

and Novell.

**SPAM**

Spam is best defined as ‘unsolicited email sent without the consent of the

addressee and without any attempt at targeting recipients who are likely to

be interested in its contents’.

**Stopping Spams**

There are some technical means of fighting spam, for example:

* closing loopholes that enable spammers to use other people’s computers to relay bulk messages;
* the use of machine learning and other techniques to identify suspicious features of message headers;
* the use of virus detection software to reject emails carrying viruses;
* keeping ‘stop lists’ of sites that are known to send spam.

**European legislation**

The European Community Directive on Privacy and Electronic

Communications (2002/58/EC) was issued in 2002 and required member

nations to introduce regulations to implement it by December 2003. In the

UK, the directive was implemented by the Privacy and Electronic

Communications (EC Directive) Regulations 2003.

**Essential features**

The directive addresses many issues that are not relevant here, but its essential features relating to unsolicited email are:

* Unsolicited email can only be sent to individuals (as opposed to companies) if they have previously given their consent.
* Sending unsolicited email that conceals the address of the sender or does not provide a valid address to which the recipient can send a request for such mailings to cease is unlawful.
* If an email address has been obtained in the course of the sale of goods or services, the seller may use the address for direct mailings, provided that the recipient is given the opportunity, easily and free of charge, with every message, to request that such mailings cease.

**Legislation in the USA**

A superficially similar Act came into force in the USA at the start of 2004. This

is the Controlling the Assault of Non-Solicited Pornography and Marketing

Act 2003, otherwise known as the CAN SPAM Act. Unfortunately, the Act has

fundamental weaknesses, of which the main one is that it is legal to send

spam provided that:

* the person sending the spam has not been informed by the receiver that they do not wish to receive spam from that source; and
* the spam contains an address that the receiver can use to ask that no more spam be sent.

**Registration**

* Both the USA and the UK operate successful schemes that allow individuals to register their telephone numbers as ones to which unsolicited direct marketing calls must not be made.
* In order to enforce the law, it is necessary to be able to identify reliably the source of the communication.
* Telephone operators keep records of calls showing the originator and the destination of the call; such records are needed for billing purposes.
* It is therefore easy, in most cases, to identify the source of any direct marketing call about which a consumer complains and then take the action necessary to enforce the law.

**Computer Misuse**

**THE COMPUTER MISUSE ACT 1990**

The Computer Misuse Act creates three new offences that can briefly be

described as:

* unauthorized access to a computer;
* unauthorized access to a computer with intention to commit a serious crime;
* unauthorized modification of the contents of a computer**.**

**Section 1 of the Computer Misuse Act 1990**

a person is guilty of an offence if

* he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
* the access he intends to secure is unauthorized; and
* he knows at the time when he causes the computer to perform the function that that is the case.

**Section 2**

Section 2 of the Act is concerned with gaining unauthorized access to computer with the intention of committing a more serious offence. A blackmailer

might attempt to gain unauthorized access to medical records, for

example, in order to identify people in prominent positions who had been

treated for sexually transmitted diseases, with a view to blackmailing them. A

terrorist might try to get access to a computer system for air traffic control with a view to issuing false instructions to pilots in order to cause accidents to happen.

**Section 3**

A person is guilty of an offence if

* he does any act which causes an unauthorized modification of the contents of any computer; and
* at the time when he does the act he has the requisite intent and the requisite knowledge.

the requisite intent is an intent to cause a modification of the contents of any computer and by so doing

* 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.

It is the offence created by Section 3 that gives the Act its power. For example, it makes each of the following a criminal offence:

* intentionally spreading a virus, worm, or other pest;
* encrypting a company’s data files and demanding a ransom for revealing the key required to decrypt it;
* concealed redirection of browser home pages;
* implanting premium rate dialers (that is, programs that replace the normal dial-up code for the computer with the code for a premium rate service).

**Computer fraud**

The Law Commission defined computer fraud as:

. . . *conduct that involves the manipulation of a computer, by whatever method, dishonestly obtain money, property, or some other advantage of value, or to cause loss.*

Computer fraud involves manipulating a computer dishonestly in order to obtain

* money,
* property,
* or services,
* or to cause loss.

**Fraud techniques**

Most of the techniques that are used are much older than computers. Such tricks as

* placing fictitious employees on the payroll or
* setting up false supplier accounts and creating spurious invoices

are still the commonest type of fraud as they were before computers appeared.

**Computer Crime**

Alternatively referred to as cyber crime, e crime, electronic crime, or hi-tech crime. Computer crimes an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.