INTERNET ISSUES and COMPUTER MISUSE

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

► Sexual Content

► Spam

► political and religious comment

► Depiction of violence

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.

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.

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.

1) mere conduit

► The role of mere conduit 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.

2) 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 that 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 administrative authority has ordered such removal or disablement.

3) 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.

►Also, the customer was not acting under the authority or the control of the service provider.

ISP

► It seems very reasonable that an ISP should cease to enjoy immunity if it fails to remove unlawful material once it has been informed about it.

► A further issue regarding ISPs is the question of anonymous and pseudonymous postings. It is common for contributors to online communities and social media to use pseudonyms for their postings. Their ISP will be aware of their true identity.

► Is the ISP allowed to release, and can it be compelled to release, this information to someone wishing to take legal action against a contributor?

Law across National Boundaries

► Criminal law

1) extradition treaty
2) extraterritorial jurisdiction

► The international convention on cybercrime

► Civil law

1) 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 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 country A.

► However, this can only be done under the very important provison 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.

► 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.

Internet Crime

► 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.

2) Convention on Cybercrime

► In 2001, the Council of Europe approved the Convention on Cybercrime. It deals with crimes committed on the internet and other networks, including criminal copyright infringement, computer-related fraud and hacking, and child sexual abuse imagery on the internet.

► International conventions inevitably are slow to take effect. Governments sign the treaty showing that they approve of it. However, in many cases they will have to persuade their legislature to approve it and the laws necessary to implement it. This process, known as **ratification.**

3) Civil Law

► Consider the case of an ISP based in the USA with a European office in London. One of its customers is an Italian, resident in Italy, who posts an accusation about a French politician on his website (which is hosted by the ISP). The French politician complains but the ISP does nothing to remove the allegation.

► If the French politician wishes to take action, he can, in theory, do so in any of the four countries involved – England, France, Italy or the USA. His best hope of winning a court action may well be in France but there is little point in bringing an action in France unless the ISP has some sort of legal presence there. The same applies to Italy.

DEFAMATION

"making statements that will damage someone's reputation, bring them into contempt, make them disliked, and so on."

In England and Wales, a distinction is made between slander, which is **spoken**, and **libel**, which is written or recorded in some other way.

Possible defenses

a. the defendant is not the author, editor or publisher of the statement complained of;

b. the statement complained of is substantially true;

c. the statement complained of was a statement of opinion and it was made clear in the statement what the basis was for the opinion;

d. the statement was published as a matter of public interest;

e. the statement was posted on a website and the operator of the website was not responsible for posting the statement;

f. the statement complained of was published in a peer-reviewed scientific or academic journal;

g. the statement was a report that is protected by privilege, such as a report of proceedings at court.

Case Study

► **The Silk Road Dark Web Marketplace Takedown (2013)**

Silk Road was a notorious dark web marketplace where users anonymously traded illegal goods like drugs and weapons. The FBI dismantled this platform by leveraging digital forensics to trace Bitcoin transactions and uncover hidden server locations. Ross Ulbricht, the creator, was convicted and sentenced to life imprisonment. This case demonstrated the effectiveness of digital forensic techniques in addressing internet-enabled criminal networks.

Defamation Act

► Prior to 2014, the UK law on defamation would have allowed the referee to start a case based or damage to reputation.

► However, the Defamation Act 2013 modified the situations where a case can be brought. It is now necessary to show that there is a case of 'serious harm', which means that there is, or is likely to be, serious financial loss.

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 sexual content 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.

Legislation in the USA

► The CAN-SPAM Act allows ISPs to sue for damages in certain cases and several ISPs have initiated successful court action against spammers. In 2005, Microsoft won a $7.8 million civil judgement against Robert Soloway for sending spam through MSN and Hotmail services and Robert Braver, a small ISP in Oklahoma, was awarded over $10 million in a judgement against Soloway. It is not clear whether either claimant actually received the money awarded. In 2008, Soloway was sentenced to 47 months imprisonment and ordered to pay $700,000 on email fraud and related charges.

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 complaint and then take the action necessary to enforce the law.

► In most cases, use of the internet is not charged on the basis of individual communications but on the basis of data transfer limits, so there is no recording of

individual emails and it costs no more to send an email from Australia to the UK than it does to send an email to one's colleague in the next office.

► Furthermore, spoofing (forging the sender's address on an email) and relaying (using other people's mail servers to send your spam) are easily achieved.

COOKIES AND USER TRACKING

► Cookies are items of data that can be stored in a browser when a user accesses a site. A cookie might be used by the site that the user is visiting (e.g. to handle login information or analytics information to monitor site usage). Some sites use third-party cookies, which can be used to track users across different sites.

► The PECR also cover the use of cookies. There are requirements to inform users that cookies are being used and to provide an option to decline cookies being stored in the browser. If a user declines the use of cookies, this may have an impact on what functionality is available

► As a result of the PECR, websites that use cookies started to add statements to inform users of this fact, with an option to accept the use of cookies or decline the use of cookies.

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.

1) 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.

2) Section 2 of the Act is concerned with gaining unauthorized access to a 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 transmitted diseases, with a view to black mailing 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.

3) 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

"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 cybercrime, 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.

Data Protection, Privacy and Freedom of Information

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.

It was designed to protect individuals from:

1. the use of inaccurate personal information or information that is incomplete or irrelevant;
2. the use of personal information by unauthorized persons;
3. 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.

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

The 8 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.

1) 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.

2) 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.

3) 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."

4) 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.

5) 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). Procedures to ensure that all data is erased at the appropriate time are needed, and this must include erasure from backup copies.

6) Sixth data protection principle

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

7) 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.

8) 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. (1) 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.

(2) 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:

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

The 1998 Act also gives data subjects the right:

1. to prevent processing likely to cause damage and distress;
2. to prevent processing for the purposes of direct marketing;
3. 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;

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 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:

1. to establish facts, for example, on what date a specific order was placed;
2. to ensure that the organization's regulations and procedures are being complied with;
3. to ascertain or demonstrate standards which are or ought be to be achieved;
4. to prevent or detect crime (whether computer-related or not);
5. to investigate or detect unauthorized use of telecommunication systems;
6. to ensure the effective operation of the system, for example, by detecting viruses or denial of service attacks;
7. 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);
8. 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.