# Course: Professional Issues in IT

Course Instructor: Shaharbano

Email address: shahar.bano@nu.edu.pk

# 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 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

Chapter 16

# 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 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 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.