14 INTERNET ISSUES

After studying this chapter, you should understand:

- *the reasons why misuse of the internet gives cause for concern;*
- *the scope and limitations of the legislation that governs the use of the internet at present;*
- *why it is difficult to enact legislation that will effectively regulate the use of the internet.*

14.1 THE EFFECTS OF THE INTERNET

The benefits that the internet has brought are almost universally recognised. 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. In this chapter we shall be looking at three topics – pornography, defamation and 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 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 organisations, 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 criticising 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.

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 in digital form 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 internet service providers (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. Finally, we shall look at the more mundane issue of commerce over the internet and the protection of consumers.

14.2 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.

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:

1. does not modify the information;
2. complies with conditions on access to the information;
3. complies with any rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
4. does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

5. acts expeditiously to remove or to disable access to the information it 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.

These apparently complicated conditions are simply designed to ensure that an ISP that claims to be playing a caching role is behaving in accordance with industry practice.

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:

1. it did not know that anything unlawful was going on;
2. 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
3. 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
4. the customer was not acting under the authority or the control of the service provider.

In the US, ISPs enjoy much broader immunity than in Europe. In effect, even when they are hosting, they enjoy the immunity that in Europe is only granted to ISPs acting as mere conduits.

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. However, this places the ISP in the position of having to judge whether or not material is unlawful. ISPs are not qualified to make such judgements and if they are forced to make them they will play safe, that is, they will usually accept that the material complained about is unlawful and will remove it. The person who posted the material has no legal redress. This means, for example, that if a website is set up to collect and display comments about a major company – be it a supermarket chain, a car manufacturer or a fast food chain – the company can, in effect, censor the comments that appear by complaining to the ISP that the material is defamatory. The ISP, aware that the complainant can deploy an army of expensive lawyers, is likely to play safe by requiring that the material be removed, regardless of whether it is true and in the public interest. There is no easy legal remedy that the owners of the website can use. This is a difficult issue and there is no obvious solution.

A further issue regarding ISPs is the question of anonymous and pseudonymous postings. It is common for contributors to bulletin boards and newsgroups 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 the contributor? In the UK, the ISP is allowed to release the information and can be compelled to do so by a court. In the USA, ISPs cannot in general be required to release the information, although they may be required to do so in the case of serious crimes.

14.3 THE LAW ACROSS NATIONAL BOUNDARIES

How law operates across national boundaries is a difficult and intensely technical topic but one that is very important in the context of the internet. We can only give the most superficial description here.

14.3.1 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 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. The case of Gary McKinnon, discussed in the next chapter, raised issues related to extradition in an acute form.

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.

What does this mean in the context of the internet? 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.

14.3.2 The international convention on cybercrime

In 2001, the Council of Europe approved a draft convention on 'cybercrime'. It deals with child pornography on the internet, criminal copyright infringement, computer-related fraud and hacking. There is an additional protocol relating to incitement to religious or racial hatred, to which signatories to the protocol may also sign up.

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**, can take a long time and is often not at the top of a government's priorities. Governments may be replaced and the incoming government may not feel committed to ratification.

The Council of Europe, which is quite separate from the EU, has 47 members; four countries outside Europe (the USA, Canada, Japan and South Africa) are associated with it. As of May 2013, 39 of these 51 countries have signed and ratified the treaty while 12 have signed it but not yet ratified it. The USA has explicitly indicated that it will not sign up to the protocol relating to hate material because this would be contrary to the First Amendment (see subsection below on the regulation of pornography in other countries)

14.3.3 Civil law

There are some parts of the civil law where the position is reasonably clear cut. Any contract that involves parties from more than one country should, and usually will, state explicitly under which jurisdiction (that is, which country's laws) it is to be interpreted. Where intellectual property law is concerned, there are international agreements to which most countries are signatories so that there is a common framework, even if it can be very difficult to enforce the rights in certain countries.

In many cases, the plaintiff will have some choice about where to take action. Very often the decision will be taken on practical grounds – there is little point in taking action in a country in which defendant has no legal presence or few assets and it is probably unwise to take action in a country where the legal process is well known to be lengthy and expensive.

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 on his website, which is hosted by the ISP, an accusation about a French politician. 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, take action 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, a country where, in any case, the law is not renowned for bringing cases to a rapid conclusion. The politician will probably opt for action in England, on the grounds that, in such cases, English law is much more sympathetic to the person claiming to be wronged than is American law. It may still be necessary to persuade the English court that this is a matter that it can properly consider.

One concrete example is that a court in New Zealand recently ruled that an organisation based in New Zealand could take action in a New Zealand court against an Australian newspaper that, it was claimed, had published defamatory statements about it on its website in Australia.

14.4 DEFAMATION

Consider the following scenario. A university provides internet services for its students and allows them to mount personal web pages. One student, who is a passionate fan of Llanbadarn United football club, believes the referee in their last game made a bad

decision that caused them to lose the match. He believes that the decision was so obviously wrong that the referee must have been bribed. He puts a statement on his web page saying that the referee is corrupt. Someone draws the referee's attention to this allegation. The referee believes that his reputation has been badly damaged by this and he wants compensation.

This situation is covered by the law of defamation. Defamation means 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 (including email).

There can be little doubt that, on the face of it, the statement in question constitutes libel. The first issue to consider, however, is who should the referee take action against. He could sue the student, but the student probably doesn't have enough money to pay any damages that might be awarded. Can he also sue the university, which presumably could pay damages?

The Defamation Act 1996 states that a person has a defence if he can prove that:

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

(Presumably, this is intended to read $a \vee (b \wedge c)$.)

The author, the editor and the publisher of the libel can all be held responsible. If the allegation had been published in a traditional student newspaper, printed on paper and sold to students and others through newsagents or the students' union, the referee would have been able to sue the publisher of the newspaper – probably the students' union if it had a separate legal existence, if not, the university – and the editor. This is reasonable because everything published in the newspaper is directly under the control of the editor, who is the agent of the publisher.

When the libel is published on a web page, on the university site, the university can reasonably argue that it cannot possibly vet everything that every one of its 10,000 students puts on their personal web page. It is not, in fact, publishing the pages, it is only providing an infrastructure that allows students to publish their own web pages. In the terminology used in the 2002 Regulations it is acting in a hosting role. Provided therefore that it removed the offending material, as soon as it had reason to suspect its presence and that the student was not acting under its authority or control, the university cannot be subject to an action for damages.

ISPs receive a significant number of complaints, many apparently from companies. As we have already stated, given the cost and management time involved in defending a libel action, it is not surprising that in these circumstances ISPs make no attempt to assess whether a complaint is justified. Instead, they immediately remove or block access to the offending material, with the result that they can avail themselves of the

defence that the 2002 Regulations provide. This may not always be in the public interest. There may well be occasions when allegations of corruption, for example, are justified and that it is in the public interest for this to be publicised. In such circumstances, in suppressing the allegations, the ISP is carrying out a function that more properly belongs to the courts.

Despite the provisions of the 2002 Regulations, there are many areas of uncertainty regarding the position of ISPs and also many practical problems with complying with the law. We have given a very simplified picture here. The reader who wishes to pursue the matter further is referred to the Law Commission report referenced in the Further Reading section at the end of this chapter.

Because so much material on the internet originates in the US, it is appropriate here to say a little about the position there. US law relating to defamation is much more favourable towards authors and publishers than is the law in the UK. The First Amendment to the United States Constitution guarantees a right to free speech that the US courts have always been eager to defend. The result is that many statements that might be considered defamatory in the UK would be protected as an exercise of the right of free speech in the USA. This is particularly the case where the defamatory statement refers to a public figure. In this case, to succeed in a libel action, the public figure needs to show not only that the statement was factually incorrect but also that it was made maliciously or recklessly.

Suppose that an internet site in the USA, hosted by an American ISP, contains a statement about someone living in the UK that would be considered defamatory in the UK but not in the USA (a statement accusing a British politician of corruption, for example). The person who is the subject of the statement can reasonably say, 'I am British. I live in the UK. This statement can be read by anyone in the UK. Surely, I am entitled to the protection offered by British law'. The author of the statement and the ISP can both say, 'We live in the United States and we are governed by its laws. We understand those laws and we comply with them. We cannot be expected to know the law as it exists in all the other countries of the world and we cannot be expected to comply with those laws'. The complainant may be able to take action in the UK against the ISP, provided the ISP has a legal presence in the UK, but only in respect of the circulation of the defamatory statement in the UK. A court in the United States will not enforce British law over such matters.

This is a case in which the global nature of the internet magnifies an issue. American newspapers and magazines do not contain much material about British politics nor do they have a very wide circulation in the UK. If the statement had appeared in an American newspaper or magazine, it would not have achieved a wide circulation in the UK. But it is nowadays more likely that such a statement will be made on the internet and it is more likely that it will then be read in the UK.

All these considerations apply to defamatory information published on other social media, as two recent cases involving tweets on Twitter show.

Lalit Modi, the former Chairman of the Indian Premier League (a cricket league) tweeted an allegation that New Zealand cricket star Chris Cairns had a history of

match fixing. Although the tweet initially went to only 65 people, it was picked up by the cricket website cricinfo, where it was read by a further 1,000 or so readers. Cairns sued both Modi and cricinfo for damages to his reputation. cricinfo quickly acknowledged the libel and settled out of court, paying £7,000 in damages and around £8,000 in costs. Modi however refused to withdraw the libel and was ordered to pay Cairns £90,000 in damages. This was confirmed on appeal in October 2012. Note that the legal action took place in London rather than in India or New Zealand.

In November 2012 the BBC Newsnight programme made allegations that a high-profile Tory politician had been involved in the sexual abuse of young boys at a children's home in North Wales. The programme did not specifically name the politician in question but there had been tweets on Twitter before the programme was broadcast alleging that Lord McAlpine was the politician involved. After the broadcast, Sally Bercow, the wife of the Speaker of the House of Commons, tweeted 'Why is Lord McAlpine trending? *innocent face*'. It proved that there was no substance in the allegations and the BBC agreed to pay substantial damages. Mrs Bercow, however, who had some 56,000 followers on Twitter claimed that her tweet was just a neutral enquiry. The judge in the High Court held that the innuendo was clear and that the damage to Lord McAlpine's reputation was potentially severe. Mrs Bercow was forced to pay substantial damages and costs.

14.5 PORNOGRAPHY

More or less every country has laws concerned with pornography. Beyond this simple statement it is almost impossible to generalise. What is considered pornographic varies widely from country to country. What is accepted as normal by everyone in one country may be considered pornographic in another country. In some countries the possession of pornography may be a criminal offence, in others possession is not an offence but distribution and/or publication are. We are not concerned here with what should or should not be considered pornographic or what should or should not be prohibited. We are concerned simply with a country's ability to enforce the laws that it has chosen to enact.

Until the early 1980s, a country could expect to enforce its laws regarding pornography reasonably effectively. It was a comparatively simple matter for the police to stop the sale of material that was regarded as pornographic. It was easy to prevent cinemas showing films considered pornographic; again this could be done by the police. And, apart from a few areas near its borders, the only television broadcasts that could be received in the country would be ones that were broadcast from within the country and could therefore be controlled.

Three developments changed this. It became possible to broadcast television programmes via satellite, which meant that programmes could be broadcast from one country to be received in another. Secondly, the advent of the internet meant that individuals could receive pornographic material, in the form of images or text, in a way that was extremely difficult for the authorities to detect. In other words, pornography became available in an intangible form. And finally, the advent of the digital camera

allowed photographs to be produced without the need for externally provided development services.

There is a second aspect to the problem of pornography. This is the problem of unsolicited pornography sent to people who find it offensive. This, however, is part of the wider problem of spam, which we deal with in the next section. In this section, we are concerned with the problems that a country faces in enforcing its laws against pornography, in the face of internet users who are willing receivers of it.

There is one important difference between laws regarding defamation and laws regarding pornography. In most instances of defamation, any legal action will be under the civil law and will be initiated by the person or organisation who is the target of the defamation. In most cases concerning the publication of pornography, action will be under the criminal law and will be initiated by state prosecution services on the basis of information provided by the police.

14.5.1 The law in the UK

In England and Wales, the law relating to pornography is based on the Obscene Publications Acts of 1959 and 1964. The 1959 Act repealed both existing legislation and the common law offences relating to obscene material. It created a criminal offence of publishing an obscene article, whether for profit or not, and the 1964 Act extended that offence to include possessing an obscene article with a view to for publication for gain. It is not an offence simply to possess an obscene article. In the context of these Acts, 'article' is to be taken to mean any type of article 'containing or embodying matter to be read or looked at or both, any sound record, and any film or other record of a picture or pictures'. The definition of publishing was amended in 1994 so that it explicitly includes the transmission of electronically-stored data.

The 1959 Act states that 'an article shall be deemed to be 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, see or hear the matter contained or embodied in it'. Although the Act has been modified by subsequent legislation, some intended to bring it provisions into line with the world of computers and the internet, the definition of obscenity has not been changed. However, its interpretation has changed considerably; much material that would almost certainly have been found by a court to be obscene at the time that the Act was passed would now be regarded as quite acceptable.

Two important features of this definition are that the effect is to be 'taken as a whole' and that it is the effect on 'persons who are likely... to read, see or hear' the material that matters. The 'taken as a whole' provision means that a prosecution under the act cannot be based simply on a short excerpt, possibly taken out of context. Thus a 400-page novel, five pages of which contain graphic and explicit descriptions of sexual activity, must be judged as a whole. The Act also states explicitly that a defendant should not be found guilty of an offence if it is proved that publication is 'for the public good on the ground that it is in the interests of science, literature, art or learning, or of other objects of general concern'. Furthermore, it is explicitly states that 'the opinion of experts as to the literary artistic, scientific or other merits' of the article can be taken into account. The effect of these provisions has been that, starting with the famous case of *Lady*

Chatterley's Lover, attempts to prosecute works that have any literary or artistic merit at all have proved unsuccessful and have now been abandoned by the authorities.

The phrase 'tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it' is potentially of importance in relation to the internet. In the 1980s, pornographic material was usually purchased in printed form from newsagents, where it was kept in a less accessible position and not sold to under-18s. Thus, those who were likely to read or see the material were likely to be adults who were deliberately looking for it. It could be argued that when the same material is posted on the internet, younger people are much more likely to gain access to it, possibly unintentionally. This could mean that material that a court would not judge to be obscene when it is printed and sold in a newsagent becomes obscene when it is posted on the internet, because it is likely to be seen or read by a larger group of people.

The position regarding child pornography is very different. The Protection of Children Act 1978 and subsequent legislation make the simple possession of indecent, that is, sexually explicit, material involving children a serious criminal offence. It is much easier to prove in court that material is sexually explicit than that it tends to deprave or corrupt. And mere possession is an objective fact in a way that possession with a view to publication is not. For these reasons, prosecutions under the Protection of Children Act are much more straightforward than prosecutions under the Obscene Publications Act. Sections 63 to 67 of the Criminal Justice and Immigration Act 2008 introduce provisions making mere possession of certain other types of obscene material – so-called 'extreme pornography' – an offence, thus simplifying prosecutions related to such material.

14.5.2 The regulation of pornography in other countries

The First Amendment to the US Constitution famously states that:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

The clauses about freedom of speech and of the press have been enthusiastically defended by the courts since the 1950s. In particular, attempts by individual states to enact provisions against pornography have been struck down as unconstitutional by the Supreme Courts of the states themselves and an act of Congress that would have made the internet subject to much stricter control than other media was struck down by the Federal Supreme Court. As a result, despite the fact that much of American society is very conservative in its attitude to sexual matters, there is little legal control over pornography.

Within Europe, the level of legal control over pornography covers a wide spectrum, with some countries, such as Denmark and Sweden, having very few controls whilst others are as restrictive or, in some cases, more restrictive than the UK. Quite often, controls are limited to material that depicts violent, non-consensual sexual acts. Worldwide, the range is still broader, ranging from countries in which the depiction of a woman in a

modest one-piece bathing costume would be unlawful to countries in which there are apparently no restrictions whatsoever.

Notwithstanding this wide variation in the control of pornography in general, there is wide (though not universal) international agreement that child pornography should be banned. Some ambiguity can arise because of differences in the age of consent from country to country – pictures involving 14-year olds might be regarded as child pornography in one country but not in another. And, indeed, a painting of Romeo and Juliet could be considered to be child pornography, since Shakespeare's play explicitly states that Romeo is 14 and Juliet is 13. But despite this ambiguity 'at the boundary', there is generally a clear understanding of what constitutes child pornography.

14.5.3 The Internet Watch Foundation

In the UK, the Internet Watch Foundation (IWF) was set up in 1996 to monitor and, where desirable and possible, take action against illegal and offensive content on the UK internet. It has the support of the UK government, the police and the internet service providers. It can act against material on the web that contain:

- images of child sexual abuse, originating anywhere in the world;
- adult material that potentially breaches the Obscene Publications Act in the UK;
- non-photographic child sexual abuse images (e.g. cartoon material) hosted in the UK.

When originally founded, the IWF's remit included material inciting racial hatred, but this has now become a police responsibility, for which there is a dedicated website. Obscene adult material was added to the IWF remit at the same time as responsibility for material inciting racial hatred was transferred to the police. The restrictions to the UK for adult obscene material and non-photographic material reflect the fact that there is no international agreement that such material should be banned.

The IWF operates a 'hotline' through which members of the public can report any internet content that they believe may be illegal. The IWF will locate and assess the material. If the material is considered illegal and falls within the IWF remit, the IWF will pass the information to the police and inform the ISP that is hosting it in the case that the material is hosted in the UK. If it is hosted abroad, the IWF will inform all its ISP members so that access from the UK can be blocked. If images of children originating in other countries are involved, it will also inform Interpol and the police in the countries concerned.

The IWF receives around 20,000 complaints per year, of which about a third relate to material that is assessed as being potentially illegal. In the first full year of IWF operation, 18 per cent of the illegal material was traced to sources within the UK. By 2003, this had been reduced to one per cent and it has remained at this low level; furthermore, it is typically removed within 60 minutes of being reported.

In the UK, the provisions of the Electronic Commerce (EC Directive) Regulations 2002, discussed in the section on the effects of the internet, apply to pornography as well as

to defamatory material. This means that ISPs will not be subject to criminal action in respect of pornographic material on sites that they host provided that:

- they did not know of its presence;
- they removed it when they became aware of its presence; and
- those responsible for publishing it were not under the ISP's authority or control.

If ISPs were left to deal directly with complaints from the public, they would inevitably feel they have to remove all the material complained about, regardless of whether it is potentially illegal, in order to keep their immunity from prosecution. This, however, would lead to legitimate public complaints that private companies were acting as internet censors. Having the complaints routed through the IWF, means that an ISP only receives those that the specialised staff at the IWF believe relate to potentially illegal material. Complaints about material that is offensive to the complainant but not potentially illegal never reach the ISP. Although this is not a perfect solution, it is a reasonable one and has proved to work well in practice.

THE ICRA

The Internet Content Rating Association (ICRA) was an international, independent organisation whose mission, it claimed, was 'to help parents to protect their children from potentially harmful material on the internet, whilst respecting the content providers' freedom of expression'. Its board included representatives from the major players in the internet and communications markets, including AOL, BT, Cable and Wireless, IBM, Microsoft and Novell. Despite its claim to be international, it was largely US-based.

The ICRA provided a framework that enabled content providers to label their sites or individual pages systematically with labels that described the nature of the content under such categories as nudity and sexual content, bad language, violence, use of drugs and alcohol, and so on. The ICRA also provided filter software, which could be used to control which sites and pages could be accessed. A user could download and install this software and then configure it to allow access only to webpages and sites that satisfy particular labelling criteria. This allowed parents discretion about how they controlled their children's use of the internet. Some parents might be quite unconcerned about their children viewing material involving nudity but might feel that they want to protect them from violent images, a common view in Sweden, for example. Others might take the opposite approach.

ICRA failed. It failed because it could not persuade enough sites to label their contents using its system and because it could not persuade browser developers to make their products read and act on the ICRA labels. For a much fuller analysis of the causes of the ICRA failure, see the paper referred to in the Further Reading section.

There are many other internet filtering products, some at least of which are useful in appropriate situations. They may be used by parents to control the amount of

time their children spend playing online games or using social media; they may be used by employers to prevent employees using work time to surf the net; and they can be used to block what may potentially be dangerous software, such as viruses. However, many filtering products aimed at blocking access to offensive material are linguistically naïve and result in harmless material being blocked. Typically this arises because an innocent word – often a place name or a personal name – contains a string of letters that are in other contexts an obscenity. Examples include Scunthorpe (a town in Lincolnshire) and Cockburn (a common Scottish surname). The local history website RomansInSussex.co.uk, which was specifically aimed at school children, was blocked by the filtering software used in many schools because the URL contains the substring 'sex'.

14.5.4 Future developments

As we have seen, the IWF has been very effective in blocking child pornography, even if the press and politicians have failed to appreciate what has been achieved. The effectiveness of the IWF's work is the result of several factors:

- There is general international agreement that this sort of material should be suppressed.
- Sites that supply the material are not attractive to advertisers. Thus, in order for such a site to be profitable, it must charge its customers. Since the payments will be necessarily electronic the customers can be traced.
- Prosecution is comparatively straightforward.

These conditions, in particular the first, do not apply in relation to other types of pornographic material and there is little likelihood of effective action being taken against them in the same way. In some countries, for example, representation of the naked body is regarded as pornographic and is forbidden by law; in other countries, paintings and sculptures by great artists, depicting the naked body, are considered to be among the countries' greatest artistic treasures. Novels that are enjoyed as great literature in some countries are banned as pornographic in others. In some countries, homosexuality is illegal and so is the depiction in text or images of homosexual relationships; in other countries, the rights of homosexuals are guaranteed by law and any discrimination is illegal. Furthermore, constitutional provisions guaranteeing freedom of speech and expression will often lead to a country tolerating pornographic material that most of its population would find extremely offensive, and more general considerations of individual freedom make it unlikely that many countries would want to make simple possession of pornography illegal.

There is, however, increasing concern about pornography on the internet, whipped up by the populist press and politicians looking for bandwagons to climb on. In response to this, in a speech delivered on 22 July 2013, the UK prime minister announced that the government had signed an agreement with the country's four largest ISPs (BT, TalkTalk, Virgin and Sky) under which all broadband connections will be automatically fitted with a 'family friendly' filter unless customers specifically request that the filter not be activated. The prime minister stated explicitly that the purpose of the agreement was

to protect children from viewing inappropriate material. He was unable or unwilling to be specific about the type of material that would be blocked.

It has been suggested that search engines should block searches that include terms from a forbidden list. If implemented, this will certainly run into the 'Scunthorpe problem' mentioned above. What is more, it would effectively ban searches looking for legitimate websites covering medical information about aspects of sexual health. In practice, anyway, it is not necessary to use obscene terms in a search in order to find pornographic material on the web.

The prime minister also said that it was wrong that material that would not be allowed in a newsagent's shop was available on the internet. Although we may sympathise with this sentiment, we must recognise the advent of the internet has made it almost impossible to stop this happening – it could only be achieved by censorship of cross-border internet traffic on a scale so massive as to be completely unacceptable to society as a whole as well as so demanding of resources as to be unaffordable.

14.6 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'. Any regular user of email will be familiar with spam. We find our mailboxes filled with emails offering Viagra, penis enlargement treatments, incitements to visit pornographic sites, advertisements for dubious financial investments and so on. It is estimated that around half of the traffic on the internet is spam. Internet users find it irritating and often offensive. If they respond to any of these invitations, they may also find themselves defrauded and their bank accounts raided. It is easy to miss important emails in the welter of spam. Some spam carries viruses. The effectiveness of the internet is much reduced by the load of spam that it carries. Not surprisingly, there is considerable pressure on governments to legislate to eliminate or at least alleviate the problem and a number of organisations have been set up specifically to fight spam.

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.

Most of these methods require constant vigilance, however, and are more suitable for use by organisations than by an individual. Furthermore, they carry a real risk that genuine email will be mistaken for spam and rejected.

The problem of spam is perceived as being of the utmost importance by the industry and substantial efforts are being made to develop technical solutions but these need to be backed up by effective legislation.

14.6.1 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.

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

- Unsolicited email can only be sent to individuals (as opposed to companies) if they have previously given their consent;
- Sending an 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.

In the UK, the enforcement of the regulations is in the hands of the Information Commissioner. The maximum penalty is a fine of £5,000 in a magistrate's court but the matter can be taken to a higher court, where an unlimited fine can be imposed.

The directive is widely seen as a step in the right direction. Its main weakness, however, is that it can only be effective in relation to spam sent from within the EU; it is estimated that some 90 per cent of the spam received in the UK originates in the USA. It has also been criticised because it does not prohibit the sending of spam to companies and because the penalties are felt to be too light.

A second weakness in the UK legislation is the difficulty of enforcing it effectively. Since it is not an offence to send unsolicited email to companies, it falls to individuals to take action against UK spammers. Few individuals are prepared to make the effort that this involves, particularly as any damages awarded will inevitably be comparatively small. Furthermore, if the spammer is a company it may frighten the individual off by threatening to fight the matter to the highest court. In one case, after judgement had been given in favour of the complainant, the company repeatedly delayed payment of the damages and costs until it suddenly disappeared. (See the Further Reading section.)

14.6.2 Legislation in the United States

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; 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.

These provisions means that email users will have to respond to every piece of spam they receive, asking for no more to be sent. Dishonest spammers will be able to use these messages to confirm the validity of the email addresses. In Europe, it is the responsibility of the spammer to get the recipient's permission before sending the spam; in the USA it is the responsibility of the recipient to inform the spammer that they don't want to receive the spam.

The law actually has some very good provisions, mostly the technical ones that require valid return addresses and make it illegal to forge other routing information that accompanies each message. Coupled with some changes in the architecture of internet mail handling and increased anti-spam vigilance by ISPs and network operators, these could, over time, have real impact on spam volumes.

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. Other large-scale spammers have also been successfully prosecuted, many of the cases involving both spamming and other criminal activities. Despite these cases, there is little sign of a decrease in the overall amount of spam originating in the USA, which accounts for nearly 20 per cent of all spam worldwide.

14.6.3 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. On the face of it this should act as a model for preventing spam; indeed, the CAN SPAM Act specifically requires the Federal Trade Commission to produce plans for such a register within six months. Unfortunately, the technical differences between the internet and the telephone network mean that this model is unlikely to work with spam. 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, although this is not effective when the direct marketing call originates from overseas.

In most cases, use of the internet is not charged on the basis of individual communications but on the basis of connect time, 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 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. This means there are no reliable records that can be used to identify where the spam really came from and the use of relaying may mean that it is impossible even to determine in which country it originated. In these circumstances, there is little possibility that a prohibition on sending unsolicited email to addresses on a register could be enforced effectively.

14.7 ECOMMERCE REGULATIONS

The basic law regarding selling over the internet is contained in the European Directive 97/7/EC, which was incorporated into UK law by the Consumer Protection (Distance Selling) Regulations 2000. They apply to both goods and services ordered over the telephone or over the internet. Two important aims of the Directive were to ensure 'that consumers should be able to have access to the goods and services of another Member State on the same terms as the population of that State' and to provide 'a new impetus for consumer protection policy'.

The regulations require suppliers to provide the following information before any contract is agreed:

- the name of the supplier and an address;
- a description of the what is being offered;
- the cost, including tax;
- the delivery charge, if any, and the method of delivery;
- the method of payment;
- the customer's right of cancellation;
- any communication costs for concluding the contract (the cost of a premium rate telephone call, for example;)
- how long the offer is valid for;
- the duration of the contract, if it is not a one-off.

The information must be clear and understandable and it must be provided, along with all terms and conditions, either in physical form or in a digital form that the consumer can store. The supplier must fulfil the contract within 30 days of its being made.

The consumer has an automatic right to cancel the contract for up to seven days after the goods are delivered or, in the case of contracts for the supply of services, up to seven days after the contract has been agreed. If the supplier has failed to provide all the information listed above, however, the customer has an automatic right to cancel the contract up to three months and seven days after delivery of the goods or, in the case of services, from the date of the contract. The supplier must reimburse the customer within 30 days of the customer cancelling. (The right to cancel does not apply in certain cases, such as customised products or newspapers and magazines.)

The regulations also stipulate that, if a customer's credit card is charged fraudulently, the card holder must be reimbursed by the card issuer.

In the case of transactions over the internet, the above provisions are strengthened by the EU Electronic Commerce Directive 2000/31/EC, incorporated into UK law by the Electronic Commerce (EC Directive) Regulations 2002. The main additional provision is that the supplier must acknowledge the order by electronic means without undue delay and provide information explaining how to amend any input errors made.

FURTHER READING

The issues discussed in this chapter change rapidly. The best sources of information are therefore usually to be found on the internet but it is important to make sure that you know the date of any article you look at. An article on spamming dated 1997, for example, cannot reflect the current situation. You should also realise that many websites are maintained by small groups of people who have very strong views. You should not assume that what you read is necessarily balanced or even factually correct.

In December 2002, the Law Commission (an official UK body responsible for reviewing UK law) produced a report entitled *Defamation and the internet*. The report is clearly written and (comparatively) easy for a non-lawyer to understand. If you want to know more about this topic it is strongly recommended. It can be found on the internet at:

http://www.lawcom.gov.uk/files/defamation2.pdf

Although it dates from 1997, the following reference is a valuable and comprehensive source of information:

Akdeniz, Y. (1997) 'Governance of pornography and child pornography on the global internet: a multi-layered approach'. In Edwards, L. and Waelde, C. (eds), *Law and the internet: regulating cyberspace*. Hart Publishing, Oxford.

It is also available on the internet:

www.cyber-rights.org/reports/governan.htm

The Internet Watch Foundation:

www.iwf.org.uk

The failure of the ICRA initiative is well documented and analysed by Phil Archer, in a paper to be found on his website:

http://philarcher.org/icra/ICRAfail.pdf

A summary of the UK spam case referred to in the subsection on European spam legislation:

www.scotchspam.org.uk/transcom.html

The Robert Soloway case mentioned in the subsection on spam legislation in the United States is described in more detail online:

www.pcworld.com/article/148780/spam.html