LIABILITY OF INTERNET SERVICE PROVIDERS

There are various kinds of services connected with the Internet, and the liability of the service provider may depend on what is being provided. At one extreme there are the long distance telecommunications providers, at the other there are Internet publishers and other providers of material. In between there are a range of providers such as operators of node computers, Internet access providers, providers of bulletin boards, Usenet group organizers and providers of host computers for Web pages.

In many cases, liability will depend upon how a court faced with a case of first impression analogizes a particular Internet service provider to more conventional categories of information providers. For example, should the service provider be viewed as the equivalent of the telephone company, purely a conduit for information? This might be the right analogy for the telecommunications link provider, but clearly does not fit the publisher. On the other hand, if the provider is viewed as analogous to a publisher of a printed publication, there is a much greater exposure to liability. The provider of a host computer for third party Web pages could be compared to a printer or perhaps a distributor of printed publications. It could also be argued that a Usenet group of bulletin board is analogous to a library, so that the provider should be treated as the librarian.

COPYRIGHT INFRINGEMENT

It can and does happen that material made available on the Internet, either by the operator or one of his subscribers, is the subject of copyright owned by a third party who has not consented to this activity. Can a service provider be liable for copyright infringement?

The Copyright, Designs and Patents Act 1988 lists the copyright owner's exclusive rights as the rights to copy, issue copies of the work to the public, perform, show or play in public and to make adaptations. A transitory copy in computer memory is a reproduction for copyright purposes. However, it seems that there is no exclusive right to transmit the work over a network. There is a right under Section 16(1)(d) to broadcast the work or include it in a cable program service but "broadcast" is limited to wireless telegraphy receivable by the general public, while interactive services are expressly excluded from the definition of "cable program service" (S.7 (2)(a)). There is special provision for remote copying; a person who transmits the work over a telecommunications system (which does not include broadcasting or cable) knowing or reasonably believing that reception of the transmission will cause infringing copies to be made is himself an infringer.

The UK law has a number of statutory limitations on the scope of the exclusive rights, but they tend to be narrowly drawn. There is also liability for secondary infringement, such as importing and distributing infringing copies made by another.

It is clear from the scope of the exclusive rights of the copyright owner that any service provider who uses or knowingly permits others to use his host computer, bulletin board

or Usenet group to store and disseminate unauthorized copies of copyright works is in danger of a civil action for infringement. Infringement may also be a criminal offence, although must be a commercial motive before there is criminal liability for copyright infringement.

There have already been a number of cases in the US which have involved bulletin boards containing copyright material which could be down loaded by those accessing the board.

In *Sega Enterprises-v-Maphia*, 857 F.Supp.679 (N.D. Cal. 1994), the Defendant operated a computer bulletin board on which users were uploading and down loading copies of Sega's copyrighted video games without the authorization of Sega. The evidence showed that the Defendant knew perfectly well what his bulletin board was being used for, and he also distributed and sold video game copiers which could be used to make unauthorized copies of Sega's games. The Court held that the Defendant, in facilitating unauthorized copying, was himself infringing Sega's copyright. For good measure, it also found that his activities had published Sega's trade mark via bulletin board which was a trade mark infringement.

In *Playboy Enterprises Inc-v-Frena*, 839 F.Supp. 1552 (M.D. Fla 1993), the Defendant's bulletin board had distributed unauthorized copies of photographs from the Playboy magazine. The Defendant was held to have infringed Playboy's copyright, even though he claimed that he did not himself put such material on his board and was, in fact, unaware that some of his subscribers were doing so. The Court held that the mere fact that he was making copies available was an infringement of the copyright owner's exclusive right to distribute or authorize the distribution of copies of the protected work. The Court also found that the fact that subscribers were able to view the photographs on their computer screen constituted an infringement of the public display right.

It is not only the small bulletin boards that are accused of copyright infringement. In *Frank Music Corp-v-CompuServe Inc*, (S.D.N.Y.) a case recently settled without admission of liability, CompuServe was sued by a group of music publishers claiming that its bulletin board, which allows subscribers to upload and dawn load music compositions in electronic, form, is an infringement of their copyright.

A very important decision recently came out of the Federal Court for the Northern District of California, *Religious Technology Center-v-Netcom On–line Communications Inc.*, 907 F. Supp. 1361. This case is one of a number that have been brought in various parts of the US by the Church of Scientology to try to prevent parts of the works of L. Ron Hubbard being put onto the Internet by individuals critical of that organization. An individual, a former Scientology minister who is now a critic of the organization, posted information to a bulletin board which was distributed to the Internet through Netcom's service. The postings were stored on the bulletin board for three days, while the Netcom system automatically stored all postings for 11 days. RTC sued the individual, the bulletin board operator and Netcom for copyright infringement.

On Netcom's motion for summary judgment, the court held that Netcom was not a direct infringer. The case of *MAI System Corp.-v-Peak Computer* Co., F.2d 511 (9th Cir. 1993), which had held that the creation of temporary copies in RAM by a third party service provider which did not have a license to use the plaintiff's software was copyright infringement, was distinguished. The mere fact that Netcom's system automatically made temporary copies of the works did not mean that Netcom had caused the copying. The court analogized Netcom's situation to that of the owner of a photocopier available to members of the public, where the courts have analyzed the machine owner's liability in terms of contributory rather than direct infringement. The court also had an eye to public policy, stating:

"It is not difficult to conclude that Erlich infringes by copying a protected work onto his computer and by posting a message to a newsgroup. However, plaintiff's theory further implicates a Usenet server that carries Erlich's message to other servers regardless of whether that server acts without any human intervention beyond the initial setting up of the system. It would also result in liability for every single Usenet server in the worldwide link of computers transmitting Erlich's message to every other computer. These parties, who are liable under the plaintiff's theory, do no more than operate or implement a system that is essential if Usenet messages are to be widely distributed. There is no need to construe the Act to make all these parties infringers. Although copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where the defendant's system is merely used to create a copy by a third party … … … The court does not find workable a theory of infringement that would hold the entire Internet liable for activities that cannot reasonably be deterred."

The court also rejected arguments that Netcom was vicariously liable, but sent to trial the issue of contributory infringement.

Other cases brought by the Church of Scientology in Colorado and Virginia have resulted in findings that publication of non-confidential extracts of unpublished works owned by the Church in the context of news reporting and non-commercial public comment were fair use.

It is interesting to guess the likely outcome if these cases had been brought in the UK. For a start, as our detailed "fair dealing" exceptions are much more limited than the US "fair use", the outcome in Colorado, which involved comment rather than current news, would probably have been different. In Netcom's case, a UK court would be faced with the specific provisions of Section 17 of the 1988 Act that copying includes storage by electronic means and the making of transient or incidental copies. Those provisions, combined with the fact that UK court tend to be reluctant to make decisions on the basis of public policy, make it likely that the result here would have been different, at least at first instance. This fact of storage does differentiate most service providers from telephone companies and make them more like publishers.

While a Usenet group moderator or bulletin board organizer might argue that he or she is more like a librarian than a publisher, it would seem unlikely that the statutory provisions

providing certain exemptions from liability for libraries under the 1988 Act and accompanying regulations would apply to what they do. Although a librarian does have the ability to make copies, this is only under controlled conditions which it seems unlikely that the average bulletin board operator could meet.

A highly publicised criminal case was the prosecution of David LaMacchia, a student at MIT. LaMacchia operated a bulletin board service from the MIT computer system which invited users to post commercial software on the bulletin board for exchange with other users. He made no personal gain from these activities, which allegedly cost software publishers over $1 million in lost sales. In the absence of a commercial motive prosecution for criminal copyright infringement was not open, so he was prosecuted under the US Computer Fraud and Abuse Act 1986. Although the Massachusetts District Court characterized LaMaccia's behavior as "heedlessly irresponsible, and at worst as nihilistic, self-indulgent and lacking in any fundamental sense of values", it dismissed the indictment on the grounds that Congress had provided exclusively under the Copyright Act for criminal offences relating to copyright infringement, so a 'back-door' prosecutions under the 1986 Act was not permitted. *United states-v-Lamaccia,* 871 F.Supp 555 (D.Mass.1994).

In the UK, it has been very briefly reported that a video game pirate known as "The Executioner" has been convicted of illegally distributing Nintendo and Sega games in the UK via an electronic bulletin board. Very recently a businessman who ran a very large library of pirated commercial software was jailed for over two years in a trading standards prosecution in Liverpool.

A multi-media working party set up by the UK Department of Trade and Industry, comprised of representatives from the media, publishing, music and computer industries, has recently reported and has, inter alia, recommended that a copyright owner who is unable to track down the source of infringements distributed over the Internet should be able to obtain compensation from the service provider or force the blocking of such transmissions. Needless to say, this proposal (which could be seen as toyshop owners voting for Christmas) has caused an outcry from the service providers (who have been cast in the role of Christmas turkeys).

DEFAMATION

The first UK claim for defamation based on distribution via e-mail has already been settled. The Plaintiff alleged that the Defendant placed a notice on a public access computer system, claiming that the Plaintiff had been fired for incompetence. In this case the service provider was not named as a defendant. In a second case, a police crime protection officer who had complained to his local branch of a national supermarket chain about a joint of meat was horrified to learn that the chain had circulated an e-mail message to other stores giving details about him under the heading 'Refund Fraud – Urgent, Urgent, Urgent'. He received substantial damages and an apology in open court from the supermarket chain.

In the US, the issue of the liability of a service provider for defamatory messages transmitted over its services has arisen. In 1991 CompuServe was sued as a result of statements in an electronic newspaper called 'Rumorville' which was prepared and published by a third party and distributed over the CompuServe network, but escaped liability on the basis that its role was equivalent to that of a library or a book shop. *Cubby –v-CompuServe*, 776 F.Supp.135 (S.D.N.Y. 1991). More recently, in *Stratton-Oakmont, Inc.-v-Prodigy Service Co.*, (NY Sup Ct May 24,1995) the plaintiff alleges that messages posted by a (so far) unknown third party on Prodigy's "Money Talk" bulletin board about the plaintiff's public stock offering were libellous and caused it considerable loss. Prodigy sought to escape from the case through a summary judgment motion, arguing that it, like CompuServe, was merely a distributor of the messages and therefore not liable for the content. The court decided that Prodigy was instead a publisher because the evidence showed that it exercised control over the contents of the "Money Talk" bulletin board, including the use of screening software to remove offensive (primarily obscene) postings and the employment of a "Board Leader" to administer the board, and therefore could be liable for any defamatory statements on its board. After this case settled, Prodigy tried unsuccessfully to have the court vacate its judgment. The US Congress has now passed a law (part of the Communications Decency Act discussed below) intended to provide protection for service providers who screen or block offensive material originating from others. This provides, inter alia, that the service provider shall not be treated as the publisher of material provided by another, and that no service provider or user shall be liable for any action taken in good faith to restrict access to or availability of material which he considers to be "obscene, lewd, lascivious, filthy, excessively violent, harassing or otherwise objectionable", even if that material is protected under the US Constitution. It is stated in the Congressional record that one purpose of the provision is to overrule the Prodigy decision.

As the Prodigy case shows, liability of the service provider for defamatory statements posted on the bulletin board or Usenet group may depend on whether he or she is treated as analogous to a newspaper publisher or to a newspaper distributor or librarian. This distinction also applies in UK law. The distributor or librarian, provided they can prove that they disseminated the work without knowing it contained a libel and there were no circumstances under which they should have been suspicious that it contained a libel, will escape liability. On the other hand, a distributor will be liable if he knows that there is a libel in the matter distributed, and may also be liable for deliberately refraining from removing defamatory matter under his control.

The Defamation Act 1996 attempts to clarify liability for defamatory messages transmitted by modern technology. Section 1(1) of the Act makes it a defense for the defendant to show that he was not the author, editor or publisher of the statement complained of, that he took "reasonable care in relation to its publication" and that he neither knew nor had reason to suspect that "what he did caused or contributed to the publication of a defamatory statement." A person who was the originator of the statement but did not intend that it be published is not an "author". A publisher is someone, whose business is issuing material to the public, an editor is a person having editorial responsibility for the content of the statement or the decision to publish. Sub-section (3)

lists certain categories of activities which do not make the person performing them an author, editor or publisher. The categories relevant to the Internet and electronic publishing are © and (e). Sub-clause © deals with case of a defamatory statement published in "electronic form". The exempted activities are processing, making copies of, distributing or selling copies in the electronic medium and operating or providing any equipment, system or service by means of which the statement is retrieved, copied, distributed or made available in electronic form Under sub clause (f) the operator of or provider of access to a communications system is not primarily responsible for statements transmitted or made available by those over whom the operator has no effective control.

So far as service provider are concerned, this legislation still leaves the possibility that they could be regarded as 'publishers' and therefore not able to use this defense. Even if an operator is held not to be primary responsible, he must still prove that he had no reason to suspect that he was disseminating a defamatory statement, having taken "all reasonable care". If he monitors the contents of the board, like Prodigy, is he expected to monitor for at least obviously defamatory statements; on the other hand, is failure to monitor a failure to take' all reasonable care'? Section 1(5) provides some very general guidance; in considering whether a defendant took reasonable care, the extent of his responsibility for the statement or the decision to publish it, the circumstances of the publication and the previous conduct of the author, editor or publisher of the statement are to be taken into account. These considerations are very dependant on individual circumstance and not very helpful in formulating general guidance for service providers. It would seem at the very least that a provider giving access to sites which are notorious for "flaming" messages, or sites provided by those with a past history of making defamatory statements, cannot just shut their eyes and plead ignorance.

One question that arises under UK law is whether a defamatory message in an electronic medium constitutes libel or slander. On the basis that the material is stored, even if only temporarily, in an electronic form, it would seem more akin to libel, and it should be noted that earlier legislation makes broadcasting defamatory words libel rather than slander. If temporary storage is sufficient to be fixation under copyright law, it would seem consistent treat it as sufficient to make the message libel. Interesting questions could arise on the issue of publication, which requires that the defamatory statement is made known to a person or persons other than the plaintiff himself. It would seem unarguable that placing such a message on a public access computer system or sending it by e-mail to a third party would constitute publication, but suppose instead the message was sent by e-mail, instead only for the plaintiff, but in fact sent in such a way that it could be accessible by others. Is this the equivalent of sending a letter in an unsealed envelope, where the defendant may not be liable on the basis that he could not reasonably anticipate that someone would read a letter in an envelope addressed to another, or is it more akin to making the statement on a postcard, where the message can be readily read by others than the addressee? Given the growth of emails, it is surely only a matter of time before this issue falls to be decided.

PORNOGRAPHY

There has been a great deal of concern expressed in the press and elsewhere about the spread of computer pornography, in particular, how it is readily available to children and young teenagers. Access by children to "top shelf" magazines and adult films and videos can be controlled by parents and by newsagents and cinemas. However, parents may not be aware of what can be accessed from their own home, and are likely to be less computer literate than their offspring. The magazines available on most newsagents' shelves are constrained by the criminal law to contain only "soft" pornography. Publishers of pornographic material on the Internet are not so restrained and there are reports of "hard" pornography obtained from the Internet, involving such things as extreme violence and bestiality, circulating amongst school children. There is also a great deal of obscene material involving children; recently a man was convicted in Manchester for the possession of a large number of pornographic images relating to children downloaded from the Internet, and others have been arrested for similar offences.

The UK Obscene Publications Act 1959 covers material, which has the effect such as to tend to deprave and corrupt. There has been a great deal of case law on what constitutes obscenity. A major factor in determining whether accused material is obscene is whether it would, taken as a whole, tend to deprave and corrupt the type of persons who may get hold of the material. Children are regarded as particularly at risk. Whereas conventional printed "hard" pornography can only be obtained in general under very controlled circumstances, electronic pornography on the Internet can be accessed by anybody with the right equipment, and it is notorious that teenage boys are very proficient at carrying out this sort of access. The prosecution should have no problem in convincing a jury that much of the "adult" material on the Internet is obscene in those circumstances. The Act was extended by the Public Order Act 1994 (the "1994 Act") to cover the transmission of electronically stored data which, when converted to a form viewable by humans, produces obscene images.

An offence is committed under the 1959 Act if the defendant publishes an obscene article, even if not for gain, or has an obscene article for the purposes of publication for gain. Publication consists of any kind of distribution, sale or performance. The amendment introduced by the 1994 Act means that the Internet service provider may be prosecuted even though the obscene material was put on the internet by a third party without the service provider's consent. There is no requirement under the Obscene Publications Act that the defendant must have actually have had an intent to deprave or corrupt, although it is a defense for the defendant to prove that both he had not examined the article and had no reasonable cause to suspect that it was of such a nature that his publication of it would constitute an offence under the Obscene Publications Act. As both these facts must be provided, it is not enough for an Internet service provider to simply shut his eyes to what is going on; he must have no reasonable cause to suspect that pornography of any kind is being transmitted using his service. Given the open nature of most Usenet groups, it would seem that this condition could not be satisfied unless the service provider did in fact inspect what was being placed on his computer. Some companies are already using software to monitor material for possibly obscene matter.

There are also special provisions covering child pornography. The Protection of Children Act 1978 (as amended by the 1994 Act) makes it an offence to take, make, permit to be taken, distribute, show, posses intending to distribute or show, or publish any indecent photograph or indecent pseudo-photograph of a child. The 1994 Act amended the definition of photograph to include "data stored on computer disk or by other electronic means which is capable of conversion into a photograph". The term "pseudo-photograph" was introduced by the 1994 Act. Pseudo-photograph means an image, whether made by computer-graphics or otherwise, which can be resolved into an image, which appears to be a photograph. Further, if the impression conveyed by the pseudo-photograph is one which is difficult to classify as either an adult or a child, but the predominant impression is that the person shown is a child, then it shall be treated as such. This is intended to cover computer-generated and manipulated images.

Both a person or company may be charged with an offence under this Act and the penalties are very similar to those under the Obscene Publications Act. However, the material covered by the 1978 Act must be "indecent", which is different from obscene. Indecency occurs at a lower level of offensiveness than obscenity, particularly where children are involved. Most people would consider indecent photographs of children, which imitated the widely accepted "Page 3" photographs of adult women. There are two potential defenses; the first is similar to that under the 1959 Act, that the defendant did not see the image and had no knowledge or suspicion that it was indecent. It is also a defense that there was a legitimate reason for possessing or distributing the image.

The Criminal Justice Act 1988 also regulates the area of child pornography, providing a summary offence of possession of an indecent photo of a child. The 1994 Act has amended the Act in a similar way to the amendments to the Protection of Children Act. The defenses under the 1978 Act are available. A further possible defense is that the image was not requested and was not kept for an unreasonable length of time after receipt.

The Telecommunications Act 1984 provides that it is an offence to send any message by telephone originating in the UK, which is grossly offensive or of an indecent, obscene or menacing character. This extends to data transmitted by a telephone line and therefore catches the use of the Internet. However, the ambit of the Act is to catch the originator of the material rather than the person distributing it. Therefore, it is unlikely that the Internet service provider will be caught by this provision in the Act but the originator of the material will be caught.

The Indecent Displays Act makes a person guilty of an offence if he publicly displays matter. Those caught are the person making the display, and any person causing or permitting the display. For matter to be displayed, it must be visible from any public place; this would include for example, Internet terminals in public libraries, "cyber-cafes" etc. However, Section 1(3) makes it clear that payment of a fee to view the material has the effect of making that material not on public display. Hence, a Web site, entered only via a subscription mechanism or an adult bulletin board with similar pay-access will not

be covered. The Act specifies the format of any warning to be used. Once again, bodies corporate may face liability as well as individuals.

Parliament is currently considering the Sexual Offence (Conspiracy and Incitement) Bill, which is aimed at the child sex tourism industry. This makes it an offence to conspire or incite others in the UK to commit sexual offences abroad. Amendments added at the Third Reading provide that an act of incitement is to be treated as done in the jurisdiction if the message is either sent or received here by any means of communication. This means that the foreign poster of an Internet message constituting incitement under this statute could be prosecuted if he came to this country.

Public concern about Internet pornography in the United States has recently caused the US Congress, by overwhelming majorities in both houses, to pass the Communications Decency Act of 1996. This Act makes it a crime to transmit over a communications network any "obscene, lewd, lascivious, filthy or indecent" material knowing the recipient is under 18 or that the material could be available to the under-18s. Mere access providers are not liable, and it is defense to show that good faith actions to restrict or prevent access to indecent content by minors have been taken. Those taking such actions are protected against litigation from third parties based on those actions. The legislation is strongly opposed by Internet users and civil liberties groups, and a Federal court in Philadelphia has held that it is unconstitutional in light of the First Amendment: this decision is being appealed to the Supreme Court.

Because of the First Amendment, the USA has probably the world's most highly developed case law on what constitutes obscenity. One factor that must be considered in determining whether something amounts to obscenity and therefore unprotected speech is local community standards. What might be considered utterly shocking and depraved in rural Arkansas may be merely titillating in Los Angeles. This sensible test has been undermined by a recent successful prosecution for obscenity in Tennessee of a bulletin board operator based in California, for material that might not have been considered obscene by a California jury. The possibility of being prosecuted in a jurisdiction with very strict standards (such as Saudi Arabia) for material which would probably not offend in its place of origin must be a great concern to the major service providers.

SPREADING VIRUSES

It is evident that a single user on the Internet could accidentally or deliberately spread a virus worldwide, potentially affecting tens or hundreds of thousands of machines. This happened when a Cornell University student Robert Morris, carrying on what he characterized as a "harmless experiment", initiated a type of virus known as a "worm" on the Internet. Although the virus caused no permanent damage, it infected over 6,000 computers and took thousands of man-hours to eradicate. Morris was prosecuted under the US Computer Fraud and Abuse Act and he was convicted despite his assertion that he had no malicious intent to cause damage to a "federal interest computer" which is a requirement of the CFAA.

The extent of liability of the service provider will undoubtedly depend on whether the presence of the virus on its bulletin board was deliberate or accidental. In Morris' case there is no doubt that the creation and placing of the virus into the system was deliberate, even though Morris did not intend the harm that he in fact caused. In the United States, in addition to the Federal statute, a number of States have introduced legislation to deal with deliberate introduction of viruses into a computer, computer system or network. There has been at least one successful conviction, under the Texas statute, of a disgruntled employee who placed a virus into his employer's computer system, which destroyed a large number of vital records.

In the UK, Section 3 of the Computer Misuse Act would seem to cover deliberate introduction of viruses. Under that Section, the crime is committed if a person does an act which causes unauthorized modification of the contents of any computer, and at the time of doing the act, he intends to modify the contents of the computer and by so doing either impair its operation, prevent or hinder access to any program or data or impair the operation of program. These factors are likely to be present in the case of deliberate infection by a virus. The perpetrator must also know that his act is unauthorized, but this requirement is unlikely to cause the prosecuting authorities too many problems.

It is likely, however, that most cases of infection by a virus will be purely accidental, perhaps as a result of a virus being contained in a piece of public domain or shareware software legitimately placed on a bulletin board for down loading. These circumstances clearly would not bring criminal liability under either the Computer Fraud and Abuse Act or the Computer Misuse Act. If, as is likely, there is no contractual relationship between the bulletin board operator and the user, the most obvious cause of action in which a civil claim could be brought is negligence. However, there would be considerable hurdles to be overcome for such an action to be successful. Firstly, is the service provider under any duty of care at all and, if so, what standard of care applies? It is more likely that an operator of a commercial service will be held to owe a duty of care than a hobbyist who merely makes a system available at no cost to the bulletin board users. The standard of care could range anywhere from a cursory examination to a requirement that every piece of software be run through state of the art virus checkers before being made available on the bulletin board. It is almost impossible to predict how a court would view these matters, and a decision may very well depend on the facts of the first case that reaches the courts. Another hurdle is that, under UK law, purely economic loss cannot be recovered in an action for negligence. There must be some kind of "physical" damage. It is clear that, besides the economic loss that may be caused by damage to software or records, elimination of the damage can be costly, as is shown in the Morris virus case. However, is this the kind of damage that is recoverable under existing case law?

A plaintiff may be tempted, because of the problems over duty and standard of care under negligence, to instead use product liability law as the basis for his claim against the software supplier. In the UK this claim would be under the Consumer Protection Act. That Act has the advantage that liability is not to be based on fault, causation rather than negligence is the primary criterion for liability. However a liability is imposed on a "producer" of a "product". While a producer is defined so as to include an importer, it is

most unlikely that a bulletin board operator would come within the definition, except where the operator is also the author of infected software. The question whether software transferred to the user in electronic form is a "product" is also wide open.

UNAUTHORISED DISSEMINATION OF CONFIDENTIAL INFORMATION

Some bulletin boards were set up by the same kind of people who tend the carry out computer hacking, phone phreaking or similar activities. This group of people tend to believe that any kind of property rights in information are basically wrong, particularly if that information is owned by the Government or big business, and take great pride in discovering and making available such confidential information. It is, therefore, not surprising that there have been a number of cases in the United States, which involve the publication of stolen proprietary information. For example, *United State-v-Riggs and Neidorf*, 741 F.Supp.556 (N.D II 1990), the defendants had between them hacked into a Bell Telephone Company computer, obtained highly confidential information about that computer company's emergency telephone number system, and had published it in a magazine. They were prosecuted under the 1986 Computer Fraud and Abuse Act, and also under federal statutes dealing with wire fraud and interstate transfer of stolen property. This was the first case, which addressed whether electronic transfer of confidential information from one computer to another across State lines constituted interstate transfer of stolen property; the court found that it did. The court held that there should be no distinction between transferring electronic information on a floppy disk and actually transferring it by electronic impulses from one computer's magnetic storage to another's.

Other Us Cases involve Defense Department information *(United States-v-Morrison*, 859 F.2d.151 (4th Circuit 1988)), law enforcement record *(United States-v-Girard*, (2nd Circuit 1979)), banking information *(United States-v-Cherif*, 943 F.2d.692 (7th Circuit 1991)) and stock market information *(Carpenter-v-United States*, 484 U.S. 19(1987). Besides these federal statutes, which only apply where there has been a transfer across State lines, a number of States have laws, which make criminal the theft of confidential information.

The position in the UK is somewhat different, as there is no legislation specifically directed to dishonest appropriation of pure information. The current law is that information is not property capable of being stolen; this was the holding in the case *Oxford-v-Moss* (1978) 68 Cr. App. R. 183, in which a university student broke into the Examination Committee's premises, studied and made a copy of the exam paper and departed, leaving the original exam paper behind. These activities were held not to be theft.

As regards civil remedies, the bulletin board operator will clearly not be in a contractual relationship with the owner of the confidential information. It is possible that the equitable doctrine, which imposes an obligation of confidentiality in respect of information which the recipient knows or ought to have know to be confidential, and which was imparted under circumstances implying confidentiality will apply. However, it

is obvious that there would be considerable difficulties for the plaintiff in proving that such an obligation existed, particularly in the case of a bulletin board operator who claimed ignorance of what was on his bulletin board. It may be specific legislation covering misappropriation of confidential information will be required as electronic networks grow in importance in this country.

There may very well, however, be criminal liability in some of the more serious case. For example, where the bulletin board is used to publish passwords to allow unauthorized entry into a computer system, the operator may be liable for any offence under the Computer Misuse Act that is then committed. The exact liability will depend on the circumstances. If the operator has actually advertised to a community of people who are likely to carry out computer hacking that passwords are available on his bulletin board, this would amount to incitement to commit an offence under the Computer Misuse Act. In a case involving police radar detectors, it was held that advertising an article for sale, representing its virtue to be that it may be used to do an act which is an offence, is an incitement to commit that offence-even if the advertisement is accompanied by a warning that the act is an offence. To establish incitement, it must be proved that the defendant knew or believed that the person incited has the necessary mens rea to commit the offence, but as the mens rea for an offence under Section1 of the Computer Misuse Act is merely that the defendant intends to secure access to a program and knows that such access is unauthorized, this will probably not be too difficult to establish.

An alternative approach is to charge the bulletin board operator with aiding, abetting, counseling or procuring commission of an offence. In each case, the defendant must have the intention to do the acts which he knows to be capable of assisting or encouraging the commission of a crime, but does not actually need to have the intent that such crime be committed. Which type of participation is most applicable will depend on circumstance; the distinction given by Smith and Hogan is that there must be a causal link for it to be procurement, aiding requires assistance but not consensus nor causation, while abetting and counseling require consensus but not causation.

There is also the possibility of a charge of conspiracy, if the necessary agreement between the operator and subscriber could be demonstrated.

There have also been cases where improperly obtained credit card numbers have been placed on computer bulletin boards, thus facilitating the making of fraudulent purchases using that card number. Here again, if the bulletin board operator knows or ought to known this is going on, he may have liability, as a secondary participant in the crime that is then committed.

In the case of defense information, it should be noted that, in a current case in California, a hacker who obtained information from a defense computer has been charged with espionage, even though there is no evidence that he ever passed the information on or intended to supply it to an enemy of the United States. In the UK, placing stolen Government confidential information on a bulletin board is likely to fall foul of the Official Secrets Act. However, catching the culprit is the main problem; the UK

Government has been unable to prevent Sinn Fein putting information about police and army facilities and security on its Web page based in Texas.

CONTEMPT OF COURT

The international nature of the Internet poses challenges to the system of protection judicial proceedings. A foreign national could publish prejudicial matter, or could attend a hearing subject to reporting restrictions and publish a report on his return home, as has already happened in the Rosemary West case. Although reporting restrictions were not lifted, a transcript of the committal hearing was put on the Internet in the US. The *Spycatcher* case showed the difficulties even without the Internet; although publication was banned in the UK, the book was on sale in the US and it was not difficult for individuals to obtain copies. In these circumstances, the authorities likely to seek to proceed against any UK based Internet service provider though whose service the contempt is published. The law relating to the liability of parties to an offending publication in the print medium is well established, that relating to broadcast media less so. As in the case of liability for defamation, courts faced with an Internet service provider will probably look for an analogy with established categories. The defense of innocent publication is likely to be of importance, although the proviso that all reasonable care must have been taken may cause difficulties.

INCITING RACIAL HATRED

The 1986 Public Order Act (the '1986 Act') created specific offences in relation to racial hatred. The provisions, which are most likely to be relevant to Internet activities are sections 19 and 21. Section 19 makes it an offence for a person to publish or distribute threatening, abusive or insulting written material if either he intends to stir up racial hatred or in the circumstances the material is likely to stir up racial hatred. Section 21 of the Act covers distributing, showing or playing to the public or a section of the public a recording of visual images or sounds to the same effect. If material otherwise within section 19 is merely viewed rather than downloaded, then there may be an offence under section 18 of the Act for displaying such written material, although there is no offence when the material is displayed inside a private home and it is only seen by people in that or another home. It is also an offence under section 23 to possess racially inflammatory material intending to have it made public.

In order to understand the possible applicability of the offences to the Internet we could consider a number of possible scenarios. The first involves an e-mail message sent between two individuals containing racially inflammatory material. There would be no offence under sections 19 and 21 as they both require public display or distribution. If either party is not in a private home then there could be an offence under section 18, and if the sender intends the receiver to then publish the material both parties have committed an offence under section 23.

On the other hand, where a message is sent to a Usenet group containing racially inflammatory material or a Web page is created that contains material that is racially

inflammatory, the public element is present. The person who sends the message or publishes the Web page will have committed an offence. The liability of the Internet host may depend on how it operates. Both sections 19 and 21 (3) provide a defense for an accused who is not shown to have intended to stir up racial hatred if he can prove that he was not aware of the content of the material or recording and did not suspect, nor had any reason to suspect, that it was threatening, abusive or insulting. Of course if a web page or a Usenet group is created specifically for the purpose of disseminating racially inflammatory material then host will be caught. Where an Internet host advertises that it monitors postings then it may well have reason to know and be unable to avail itself of this statutory defense.

The Act also creates liability for corporate bodies or companies. After conviction a court may order the forfeiture of any written material or recording relating to the offence. For an Internet host the consequence of having its equipment seized could be devastating.

What if the Usenet site or Web page is located in a different jurisdiction? A statute will not be treated as having extra-territorial effect unless it specifically states that is does. Such statutes are rare and tend to be confined to those areas of international law such a piracy or hijacking, but recent cases appear to suggest that the courts are moving to a more global view of legal action. This signals the way for at least common law rules on liability for crimes such as incitement, attempts or conspiracy to be justifiable in this country. So, for example, if messages sent on a e-mail are sent with the intention that they should stir up hatred or if a Web page is set up in different jurisdiction with the intention that people in England should read it, this may be actionable as common law incitement. In practice such prosecution is unlikely to happen as it would involve extradition proceedings, which tend to be so difficult as to be reserved for very serious crimes.

CONCLUSION

This paper can provide only a brief discussion of some of the main legal issues connected with the Internet. The development of information superhighways (or autobahns if you prefer the German model) will doubtless pose many challenges to governments, law enforcement agencies and lawyers. Perhaps it might even force the development of a true system of international law.