ALAI 2001 National Report
Session IC
United Kingdom

ALAI 2001 CONGRESS QUESTIONNAIRE
Adjuncts and Alternatives to Copyright

Session 1.C: ***Situating legal protections for copyright-related technological measures in the broader legal landscape: ANTI CIRCUMVENTION PROTECTION OUTSIDE COPYRIGHT***

United Kingdom National Report, compiled by Hubert Best and Rachel Tregear.

Note: This is a wide-ranging questionnaire, and it is not possible to provide an exhaustive survey of all the relevant case law/legislation in relation to every question. However the report is intended to provide a summary of significant and relevant information in response to the questions asked.

The Directive on the harmonisation of certain aspects of copyright and related rights in the information society applies to many of the questions asked. The Directive has not yet been published in the Official Journal although it is anticipated that it will be shortly. Once published Member States will have an eighteen-month period within which to implement its provisions.

A Directive is a piece of European legislation addressed to Member States. Once such legislation is passed at European level each Member State must ensure that it is effectively applied in their legal system. The Directive prescribes an end result. The form and methods of the application is a matter for each Member State to decide for itself. In principle a Directive takes effect through national implementing measures (national legislation). However it is possible that even where a Member State has not yet implemented a Directive some of its provisions could have direct effect. This means that if a Directive confers direct rights to individuals then individuals could rely on the directive before a judge without having to wait for national legislation to implement it (**Case C - 184/89** ***Nimz v Freie and Hansestadt Hamburg*** **1991 ECR 297, 1992 3 CMLR 699, ECJ**). Furthermore if the individuals feel that losses have been incurred because national authorities failed to implement the directive correctly then they may be able to sue for damages. (**Joined Cases C-6/90 and C-9/90** ***Francovich and Bonifaci v Italy*** **1991 ECR I-5357 1992 IRLR 8**) Such damages can only be obtained in national courts.

1. Types of Circumvention

a. Computer Misuse Act 1990

Section 1 of the Computer Misuse Act 1990:
Unauthorised access to computer material
This offence attracts criminal liability

Section 2 of the Computer Misuse Act 1990:
Unauthorised access with intent to commit or facilitate commission of further offences

Copyright, Designs and Patents Act 1988 ("CDPA")
Section 296 CDPA:
Devices designed to circumvent copy protection

Section 297 CDPA:
Offence of fraudulently receiving programmes

This offence attracts criminal liability

Section 297A CDPA:
Unauthorised decoders

Section 298 CDPA:
Rights and Remedies in respect of Apparatus &c for unauthorised reception of transmissions

Telecommunications Act 1984
Section 42 Telecommunications Act 1984:
Fraudulent use of telecommunications system

Section 42A Telecommunications Act 1984
...a person has in his custody or under his control anything...which may be used for the purpose of obtaining or for a purpose connected with the obtaining of a service to which section 42 (1) applies.

Availability of other legal remedies: ***Denco v Joinson*** **1992 1 AE 463** the Employment Appeals Tribunal ruled that the act of an employee in seeking to obtain unauthorised access to information held on an employer's computer constituted serious industrial misconduct justifying summary dismissal.

b. **Data Protection Act 1998 -** Section 55 unlawful obtaining etc of personal data (criminalises the improper use of personal data).

Schedule 1 of the Data Protection Act 1998 contains the 8 data protection principles, which are general statements of acceptable processing practice. In this context the 7th data protection principle is particularly relevant: "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

Section 42 Telecommunications Act 1984: A person who dishonestly obtains a [service to which this subsection applies] with the intent to avoid payment of any charge applicable to the provision of that service shall be guilty of an offence.

Section 297 CDPA

Fraud/conspiracy to defraud: "an agreement by two or more by dishonesty to deprive a person of something which is his or to which he is entitled and an agreement by two or more to injure some proprietary right of his suffices to constitute the offence of conspiracy to defraud" **Scott v *Metropolitan Police Commissioner* 1975 AC 819 (definition given in *R v Bridgeman and Butt*)**

Theft Act 1968 section 15:

(1) A person who by any deception dishonestly obtains property belonging to another, with the intention of permanently depriving that other of it,…..

(2) For the purposes of this section "deception" means any deception (whether deliberate or reckless) by words or conduct as to fact or as to law, including a deception as to the present intentions of the person using the deception or any other person.

The decision in ***Re London and Globe Finance Corp. Ltd*** **1903 1 CH 728** defined deception to mean: "to induce a man to believe a thing which is false, and which the person practising the deceit knows or believes to be false"

Forgery - Section 1 Forgery and Counterfeiting Act 1981: A person is guilty of forgery if he makes a false instrument with the intention that he or another shall use it to induce somebody to accept it as genuine and by reason of so accepting it to do or not to do some act to his own or another person's prejudice.

In ***R v Gold*** **1987 3 WLR 803** the defendants gained unauthorised access to BT's Prestel service and then discovered the password codes of various private mail boxes. The defendants were prosecuted under the Forgery and Counterfeiting Act of creating a "false instrument" by entering the customer's authorisation code to enter the system. The critical issue was whether any false instrument had been made. The Court of Appeal decided that password codes are not a false instrument as they are not tangible. For this and other reasons, the Lord Chief Justice concluded that the Act was not intended to apply to the situation which was shown to exist in the present case.

Wireless Telegraphy Act 1949, section 5 (b) (I): it is an offence to use any wireless telegraphy apparatus i.e. a radio receiver, with the intent to obtain information as to the content of any message (whether sent by means of wireless telegraphy or not) which the person is not authorised to receive.

c. See above. Government proposals relating in particular to child pornography and Internet "chat rooms" are expected.

d. See above.

e. **Theft Act 1968 section 1**: A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it….

Problems arise with the theft of information and the issue of whether the information separate from any connection with the tangible object may constitute the subject matter of theft. ***Oxford v Moss*** **1978 68 Cr App R 183** upheld the principle that information is not property. A student took a copy of a forthcoming exam paper from a lecturer's desk, photocopied it and returned the original. The offence of theft had not been committed, as the victim was not permanently deprived of the asset.

f. **Telecommunications Act 1984**

Breach of confidence

g,h. Breach of contract

2 **<u>General tort law</u>**

a. ***University of NSW v Moorhouse*** 6 ALR 207, 133 CLR 21and ***Amstrad Consumer Electronics plc v BPI*** The Times 2 July 1995 - a tort of authorisation could occur if infringement took place (a claim for infringement of copyright - s. 297, 298 CDPA - would probably be the first line of attack).

b. Injunctions are available (governed by general principles of law). Primary infringement of copyright is a strict liability offence. All other offences (including secondary infringement of copyright, computer misuse, theft, fraud, etc.) all require varying degrees of knowledge and intent.

3 Broadcasting law, cable and satellite regulations, protection of encrypted services or broadcasts, protection of conditional access services

a-e. These services and devices are covered by sections 297A and 298 of CDPA, and attract civil and criminal liability as provided by UK copyright legislation.

f.1. The Conditional Access Directive has been implemented. The provisions are in the copyright regime - sections 297A and 298 of CDPA.

***R v Bridgeman and Butt* 1996 FSR 538** - case under section 297A CDPA
In brief, BSKYB make satellite TV transmissions, and a smart card is required to decode these transmissions. The defendants were caught offering to provide unauthorised smart cards and were prosecuted with the offence of conspiring to commit a criminal offence under section 297A of the CDPA. On the basis that there was a right to be infringed and that the production of the unauthorised cards was to take place in England and that the direct victim of the intended fraud was to be a UK resident company, the conspiracy was indictable in England and Wales even in the absence of intended use or intended use of cards in the UK.

***BBC v Hi Tech Xtravision* 1991 1 WLR** - case under section 298 CDPA. BBC arrange satellite transmissions for reception outside the UK. BBC licensed manufacturers in the UK to produce decoding equipment and agreed to license equipment provided by these manufacturers. Hi Tech Xtravision manufactured decoders in the UK and began to sell them outside the UK at prices substantially lower than the officially licensed decoders. The case concerned whether section 298 CDPA could be used to restrain the manufacture in the UK of equipment only for sale and use outside the UK. The House of Lords said it could.

***British Sky Broadcasting v Lyons* 1995 FSR 357** - case under section 298 CDPA. The Defendant in this case imported, sold and supplied smart cards not authorised by the plaintiffs, which enabled the plaintiff's programmes to be shown without their consent. The Defendants claimed that section 298 CDPA, which gave rights only to persons who provided or sent signals from the UK was a quantitative restriction contrary to Article 30 of the Treaty of Rome which discriminated against non-UK transmitters. The judge granted summary judgment and refused to make a referral in respect of the Euro Defence.

Rationale for protection is in Recital 6 (internal market) of the Directive.

Yes, conditional access legislation could be applied to services provided through the internet and other networks. The definition of "transmission" at section 297A includes any programme included in a broadcasting or cable programme service…and information society service..which is provided from a place in the United Kingdom or any other service.

4. Telecommunications Law

a.1. Sections 42 - 46 of the Telecommunications Act 1984 covers fraudulent use/access of a telecommunications system (section 42), interception by the operator of a public telecommunications system (otherwise than in the course of duty) (section 45).

Section 42A covers "anything ..which may be used for the purpose of obtaining or for a purpose connected with the obtaining of a service to which section 42 (1) above applies. But this section does not cover unauthorised decoders as defined at section 297A (4) CDPA.

Summary of relevant provisions
Section 42 Telecommunications Act 1984:
Fraudulent use of a telecommunication system

Morgans v DPP **HL 2000 2 AE 522**: Defendant charged with 5 charges of offences contrary to section 1 (1) of the Computer Misuse Act 1990 and with two charges of fraudulent use of telecoms system contrary to section 42 of the Telcommunications Act 1984

R v Levitz, Mbele and Vowell **1989 Crim LR 714**

Section 42A Telecommunications Act 1984:
Possession or supply of anything for fraudulent purpose in connection with use of telecommunication system

Section 43 Improper use of public telecommunication system

Section 44 Modification etc of messages

Section 45 Interception and disclosure of messages

2. No

3. Section 45 (2) of the Telecommunications Act 1984 details the circumstances in which interception by the person running the public telecommunication system is authorised:

(a) court order/criminal proceedings
(b) warrant, authorisation, notice under the Regulation of Investigatory Powers Act 2000 ("RIP")
(c) in compliance with any requirement imposed ..in consequence of the exercise by any person of any statutory power exercisable by him for the purpose of obtaining any document or other information
(d) in pursuance of any duty under RIP, Police Act 1997…etc.

RIP introduces a new interception regime. Interception is only permitted in specified circumstances, and it must be shown that the interception is necessary and justifiable. This legislation includes private networks (with exceptions).

4. These are criminal offences and prosecutions are brought by the Crown Prosecution Service.

OFTEL (Telecoms regulator) have told us that more recent legislation (Data Protection Act 1998, RIP) would probably now be used in preference to the above provisions.

b. Section 42 A Telecommunications Act 1984

5. **<u>Computer Crime</u>**

a. Issue arises of whether computer related conduct should be regarded as requiring technology specific legislation or whether it might be satisfactorily regulated through the application of general criminal law provisions.

Computer Misuse Act 1990 is the major computer specific criminal statute in the UK, intended to supplement provisions of general criminal law.

1980s Law Commissions identified that the act of obtaining unauthorised access to data held on a computer did not in the absence of further aggravating conduct constitute a criminal offence. This

and the decision in ***R v Gold*** **1988 AC 1063 (see above)** created a perception of vulnerability to computer hackers.

Sections 1-3 of the Computer Misuse Act cover unauthorised access to computer material (basic offence), unauthorised access with intent to commit or facilitate commission of further offences (ulterior intent offence) and unauthorised modification of computer material.

b. Section 1 of the Computer Misuse Act 1990:

A person is guilty of an offence if:
(a) he causes a computer to perform a function with intent to secure access to any program or data held in any computer;
(b) the access he intends to secure is unauthorised; and
(c) he knows at the time when he causes the computer to perform the function that this is the case.

The way of getting unauthorised access is not defined.

A-G's Reference (No 1 of 1991) 1992 3 WLR 432: AG sought the opinion of the Court of Appeal on the question: In order for a person to commit an offence under section 1 (1) of the Computer Misuse Act 1990 does the computer which the person causes to perform any function with the required intent have to be a different computer from the one into which he intends to secure unauthorised access to any program or data held therein?
The Lord Chief justice answered in the negative.

c. These could be offences under section 297A CDPA etc. See above.

d. Yes the person obtaining or seeking to obtain access to any programs or data must know that this is not authorised - Section 1 (c) of the Computer Misuse Act 1990.

Section 17 (5): access is unauthorised when the user is not himself entitled to control access of the kind in question to the program or data; he does not have the consent to access of the kind in question to the program or data from any person who is so entitled.

e. A number of cases have been brought under the Computer Misuse Act 1990. In particular the case law has clarified that the Act covers misuse of facilities by authorised users.

R v Bignall **1997 Times 6 June:** a police officer obtained access to data held on the police national computer in order to identify the owner of a motor vehicle. The information was sought for the police officer's personal interest. Once the conduct was discovered the officer was charged under section 1 of the Computer Misuse Act 1990. However it was held that no offence had been committed under that Act

R v Bow Street Magistrates Court ex parted Allison **1999 4 AER** -This case concerned the application by the US authorities for the extradition of the applicant to face charges inter alia of securing unauthorised access to the American Express computer with the intent to commit theft and forgery. It was also alleged that the applicant had caused unauthorised modification to the contents of the computer system. Following the decision in Bignall it was held that a section 1 offence had not been committed. On appeal the House of Lords rejected the notion that misuse of access rights could not incur criminal sanctions. Therefore misuse of facilities by authorised users will expose them to the risk of criminal prosecution.

f. Yes the Act is intended to supplement existing criminal law provisions. It is not possible in this report to detail every aspect of criminal law which could apply in this context. This is only a summary of some of the provisions of criminal law which could be relevant.

Section 3 (6) of the Computer Misuse Act 1990 is intended to avoid any possibility of overlap between the Computer Misuse Act 1990 and the Criminal Damage Act 1971.

Cox v Riley **1986 83 Cr App Rep 54 -** in this case an employee deleted computer programs from a plastic circuit card which was required to operate a computerised saw. It was held that property had been damaged.

R v Whiteley **1991 93 Cr App Rep 25 -** in this case the defendant was convicted of causing damage through gaining unauthorised access to the Joint Academic Network System and deleting and amending a substantial number of files. It was held that the alteration of magnetic particles on the disk impaired the value and usefulness of the disk and constituted damage.

The attempt to exclude Criminal Damage Act 1971 in the computer context may not be effective. It is suggested that damage to data held on a computer disk might still be regarded as adversely affecting its physical condition.

Other possible offences include: conspiracy to defraud, theft, forgery, fraud ***R v Bridgman and Butt*** **[1996] FSR 538**

Ian Lloyd in his text book on Information Technology Law says "it may well be that an attempt by a software producer to include anti-copying devices which would have the effect of causing software to stop working in the event an attempt to copy was detected, would constitute the offence of extortion."

6. **<u>Unfair Competition law</u>**

a. ***BSkyB V Lyons*** [1995] FSR 357. The defendant attempted to raise a euro defence: section 298 CDPA a quantitative restriction contrary to Article 30 discriminating against non UK transmitters. The Judge granted summary judgment and euro defence failed. In interpreting and applying Article 36 of the Treaty of Rome it was for the national legislature to determine the conditions for the protection of a right like a transmission right but these conditions should not amount to an arbitrary discrimination or a disguised restriction of trade between member states.

European Commission Press Release 24 March 2001 EU starts procedure against IMS Health in Germany

The case involves the analysis of sales information for the health care industry.

IMS Health group an American group are accused by NDC a rival of having sewn up the German market so efficiently that NDC and AzyX Geopharma another rival cannot compete. In the past year or so both have tried to launch products only to be told by potential customers that they want the presentation of the drugs data based on the IMS system, which is protected by copyright and called the 1860 brick structure. IMS successfully sued NDC and AzyX Geopharma in Germany for copyright infringement as they copied some elements of the drugs database.

In December 2000 NDC and AzyX Geopharma appealed to Brussels requesting that IMS be forced to license its system to them so as to open the market to competition. The argument is that IMS have abused an "essential facility". The European Commission sent its objections to IMS in March stating that the refusal to licence is prima facie abuse of a dominant position within the meaning of Article 82 of the European Treaty. According to European Competition Commissioner Mario Monti should the Commission's initial opinion be confirmed then IMS

would have to licence the use of the 1860 brick structure on non-discriminatory commercially reasonable terms.

b. The UK Competition Act 1998 came into force in 2000, and was intended to align the UK competition position with the Treaty of Rome. Prior to that, unfair competition as such would have to have been raised as a euro defence (as in BskyB above) and not in the domestic courts. Now there would need to be abuse of a dominant position or an anti-competitive agreement, which involves analysis of the economic position. Market definition would be a significant issue, as in IMS above.

7 Protection of technological measures as such

a. Technical means of protection could be protected by copyright, patent or trade secret.

Patents for software is a controversial topic. Patents Act 1977 and the European Patent Convention 1973 exclude computer software and methods of doing business "as such" from patent protection.

UK Patent Office launched a public consultation on whether patent protection should be extended to include software and business methods. The Patent Office announced on 13 March 2001 that the position would not be changed but called for urgent European action. The European Commission's response to its own consultation exercise is expected shortly.

In point of fact, thousands of software patents have been granted. This has been achieved by crafty wording and time-pressed examiners. Whether these patents will all survive challenge in courts (possibly as being anti-competitive) remains to be seen.

b. No.

8. Other protections

a. This is covered elsewhere in responses.

b. Contracts can provide effective protection between the parties to the contract. Recent legislation (Contracts (Rights of Third Parties) Act 1999) gives enforceable rights to third parties who benefit from the contract, but these rights can be excluded from contracts. There is extensive case law on general contracts which is applicable, including case law on bringing terms and conditions to the attention of the other party, Unfair Contract Terms Act 1977 and much other consumer protection legislation which includes the reasonableness test for contractual terms.

9. Limitations, exceptions, fundamental rights, third parties and public interest

Article 10 ECHR Everyone has the right to freedom of expression…

Article 10 (1) - states that it does not prevent states from requiring licensing of broadcasting, television or cinema enterprises.

Article 10 (2) - the exercise of the freedoms in article 10 (1) carries with it duties and responsibilities.

Freedom of Information Act - replaces the non-statutory code of access to Government Information. FOIA does not have to be fully implemented until 30 November 2005 at the latest. A guide to FOIA is available on the Information Commissioner's website an is an outline work plan showing the proposed activities to be undertaken by her office up to March 2002.

***Hyde Park Residence Limited v Yelland* 3 WLR 215** limits the public interest defence to infringement of copyright. The plaintiff company was responsible for security at the Paris villa which Diana Princess of Wales and Dodi Fayed visited on the day before the car accident in which they both died. The visit was recorded on video tape by security cameras. One of the plaintiff's employees was instructed to take stills from the video tape. He took an extra set for himself and passed them onto a newspaper without the plaintiff's consent. The plaintiff brought an action against the employee, the editor, publisher and printers of the newspaper for copyright infringement. The plaintiff argued that the publication of the photos was "fair dealing for the purpose of reporting current events" and in the public interest. The Court of Appeal held that this was not fair dealing nor in the public interest. There was nothing in the circumstances of the case to require the court to refuse the enforce the copyright.

10. <u>Potential application of the protections surveyed above to copyright works</u>

a. In the UK many of these provisions form part of CDPA, the copyright statute. The Crown commences criminal proceedings, which are controlled by the Crown Prosecution Service, although an aggrieved copyright owner can lay a complaint in the Magistrates Court, leading to criminal proceedings.

b. Yes.

c. As these issues are largely subsumed under UK copyright legislation, this would be the first and principal line of attack. Criminal proceedings need a higher standard of proof, and commencement and prosecution of them are not in the hands of the copyright owner.

d. Article 11 of the WIPO treaty is currently covered, in our view. It is not clear that Article 12 is covered within existing legislation. The Copyright Directive is intended to implement a number of international obligations in the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.