Winter 1996


Christopher Millard

Robert Carolina

Follow this and additional works at: http://repository.jmls.edu/jitpl

Part of the Computer Law Commons, Intellectual Property Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

http://repository.jmls.edu/jitpl/vol14/iss2/4

This Article is brought to you for free and open access by The John Marshall Institutional Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of The John Marshall Institutional Repository.
COMMERCIAL TRANSACTIONS ON
THE GLOBAL INFORMATION
INFRASTRUCTURE:
A EUROPEAN PERSPECTIVE

CHRISTOPHER MILLARD & ROBERT CAROLINA†

I. INTRODUCTION

A. INTRODUCTION TO THE PROBLEM OF DIGITAL VIRTUAL NETWORKS

Before turning to legal doctrines, it is necessary to review what a digital superhighway is, how it works, and the various actors involved in its operation. This is particularly important in the light of what appears to be widespread misunderstanding about this newest of infrastructures. The most important concept to understand about digital data networks is that they are "virtual networks." This is to say that what appears at first glance to be one seamless network web is, in fact, a series of completely unrelated networks, each potentially owned and operated by different persons. At its lowest level, a data network consists of some type

† Christopher Millard (LL.B. 1980, University of Sheffield; M.A. 1982, University of Toronto; LL.M. 1983, University of Toronto) is a Partner in the Media, Computer and Communications Group of the international law firm, Clifford Chance. His practice has a particular focus on online services and the Internet, hardware and software procurement and distribution agreements, outsourcing transactions, data protection, telecommunications regulation and communications contracts. As a Senior Visiting Fellow of the University of London, he teaches LL.M. courses in Information Technology Law and Telecommunications Law. He is currently Joint Chairman of the Society for Computers and Law, President of the International Federation of Computer Law Associations, and is a General Editor of the International Journal of Law and Information Technology. He may be contacted at Christopher.Millard@CliffordChance.com.

Robert Carolina (B.A. 1988, University of Dayton; J.D. 1991, Georgetown University Law Center; LL.M. 1993, London School of Economics) is a lawyer in the Media, Computer and Communications Group of the international law firm, Clifford Chance. His practice is focused upon the regulation and licensing of computer and telecommunications technology and services, including cross-border transactions. He may be contacted at Robert.Carolina@CliffordChance.com.

The authors gratefully acknowledge the assistance of Mark Ford and Deborah Ishihara in the preparation of this paper. Clifford Chance operates a World Wide Web page at http://www.cliffordchance.com.

269
of underlying physical transmission capacity. Also known as the physical layer, or infrastructure layer, this portion of the network could be miles-long sections of fibre optic cable, a length of copper wire, or even microwave radio transmitters. Historically, this type of infrastructure was owned and operated by a single government ministry, but with the increasing liberalisation of telecommunications markets, there are a growing number of infrastructure networks available for use. On a smaller scale, physical layers could consist of local area computer network cables within an office building.

But the physical layer is not the end of the story. The next layer of a data network (for our purposes) is the "data layer." This layer of the network serves to carve up and package the underlying transmission capacity in a very efficient manner. Again historically, the data layer was often operated by the same organisation which owned and operated the physical layer. Increasing competition and the availability of leased telecommunications capacity, however, mean that a great number of these data layers are operated by third parties who, in turn, lease various physical bits from traditional telecommunications operators. In addition, data layers can be "stacked" on top of one another. Finally, at the top layer of the network we find network users who produce and receive data. Network users do not need to understand the complex interrelationship between owners of various types of infrastructure and operators of data services. For their part, users witness a seamless connection between two or more points.

One important characteristic to understand about data networks is that they are simply a series of computers connected by some type of physical infrastructure. The "transmission" of a message actually involves the creation of an entirely new copy of the message at each and every intervening computer in the chain. Further, these multiple copies are not created simultaneously. Messages can be held in a queue at an intervening computer for seconds, minutes, or possibly hours. The final copy in the transmission chain is the one created on the recipient's computer.

Given the widespread interconnection and interoperability of such networks, it is thus possible to create and operate a massive digital data superhighway which is neither owned nor operated by any single person or organisation. One example of such a network is the Internet, along with the various virtual components which operate on it including the World Wide Web, Commercenet, Gopher and Usenet.

1. This is neither an engineering nor a legal term of art. The term "data layer" is used only for the purpose of distinguishing various data networks from transmission capacity and content producers.
B. THE CARGO PARADIGM

This kind of complex interrelationship should not be unfamiliar to commercial lawyers. A familiar commercial metaphor can be found in the world of cargo shipping. In shipping goods from one point to another, they may be placed on a truck owned by one delivery firm, driven across private and public roads, placed into a container owned by another firm, from there loaded onto a ship owned by a third, unloaded dockside and placed temporarily in a warehouse owned by another. Nonetheless, the whole operation appears to function as a seamless “network” of sorts. As with data networks, the person shipping goods does not necessarily understand or care about the number of different persons involved in handling the goods which are shipped. His only concern is that the goods arrive at the proper destination and in good order.

There are, however, three major differences between these two types of “networks.” The first is that in traditional cargo shipping, the end-to-end delivery time is measured in days, weeks, and months. With digital data networks however, the delivery time is measured in microseconds, seconds, or possibly hours. The second difference is that data networks can only “ship” that which can be transmitted digitally (although it should be noted that this encompasses a great deal including simple text, computer files, voice conversations, still images, and motion pictures).

The third, and probably most important difference, is that an item which enters a cargo shipping network is physically delivered to its destination. There is only one such item, and it can be physically pinpointed at any given moment. By contrast, a data network delivers a copy of the transmitted item, the “original” may or may not be destroyed in the process, and there are innumerable transient (and potentially permanent) copies created in the transmission process. Despite these differences, the cargo shipping metaphor is one of the best currently available for understanding the commercial relationships involved in the operation of data networks.

C. CYBERSPACE AND THE “NO REGULATION” FALLACY

As information technologies have begun to converge, and people begin to speak of universal broadband\(^2\) networks, there have been a number of calls to regulate the use of such technology. By way of example, it is often said that existing data networks (such as the Internet) are “unregulated.” This statement, however, is patently incorrect. There are innumerable laws, statutes and regulations which apply to the develop-

\(^2\) In this context, “broadband” networks are those capable of carrying multiple “large” data messages such as graphic images and full motion video to multiple recipients simultaneously.
ment, financing, and operation of, as well as the content transmitted via such networks, even though most people who use and operate these networks are unaware of many of the various laws which apply to their activities. This is a problem which is compounded by the ease with which such networks, and the traffic on them, span legal jurisdictions. Additionally, some who are aware of the laws in question simply choose to ignore them. Because of the nature of large scale broadband data networks, many of these laws may prove difficult, if not impossible, to police and enforce. Thus networks such as the Internet are not “unregulated,” but in some aspects they may be “unregulatable.”

II. EURO-REGULATION OF GII TRAFFIC

A. EUROPEAN HARMONISATION EFFORTS AND CONVERGING TECHNOLOGIES

Not surprisingly, some of the EU Directives designed to shape a single European marketplace are aimed at suppliers and users of computer technology and services. However, as Europe has been amending its laws and regulations in an effort to create a single market, technology has been changing as well. Unfortunately, many attempts at legal harmonisation do not adequately address the convergence of “multimedia” technologies, and it is clear that the drafters of many laws throughout Europe never envisioned the marriage of computer and telecommunications technology we have witnessed in the past five years. References to “data superhighways,” “global information infrastructure,” and the “Infobahn” are currently in vogue, but no one is quite certain yet what are the “rules of the road” for this information age infrastructure. We will next examine some of the rules which already exist at a European level to regulate traffic on the Infobahn.

B. COPYRIGHT DIRECTIVES

The rules that are most talked about relate to copyright, which is, amongst other things, the right not to have your work copied. From the description at the start of this paper of how data is transmitted over the Internet it can be seen that copyright must be considered at each of the many stages in the transmission process.

This paper deals with the European face of international superhighway issues, but it should not be forgotten that there are treaties and agreements at a supra-national level which include European countries in their membership. These agreements cover all aspects of the digital superhighway from the laying of submarine cables to rules governing satellites. In the area of intellectual property, it is agreements such as
GATT TRIPs, the Universal Copyright Convention, and the Berne Convention which confer very important rights relating to material transmitted via the digital superhighway.

1. The European Software Directive

The European Software Directive ("Software Directive") aims to ensure that all Member States grant copyright protection to computer programs by classifying them as literary works. It is loosely harmonising in its effect, but there remains significant scope for inconsistency between the national laws of the implementing countries, either because it permits flexibility or because of its inherent ambiguities. The Software Directive does not offer a definition of "computer program," but identifies criteria by which to determine whether or not a computer program will be protected. To qualify as a literary work, the only requirement to be satisfied is that the program must be the author's own intellectual creation: No "qualitative or aesthetic" standard may be imposed.

Article 4 gives the copyright owner the exclusive right to reproduce his computer program "by any means and in any form," "in part or in whole" and whether as a "permanent or temporary reproduction." This exclusive right extends to "loading, displaying, running, transmission or storage of the computer program" to the extent that those processes "necessitate such reproduction." The copyright owner also has the exclusive right to translate, adapt, arrange, alter and distribute his program. One or more of these rights clearly will be infringed if the program is transmitted via the Internet without the consent of the copyright owner.

In principle, a third party requires express authorisation from the copyright owner before he may carry out any of these acts. However, Article 5.1 provides that "in the absence of specific contractual provisions," these acts (with the exception of distribution) do not require the

7. Id. at art. 1.1, 1991 O.J. (L 122) 44.
8. The present state of implementation of the Software Directive is that all EU Member States except Luxembourg have enacted implementing legislation. Luxembourg is in the process of implementing legislation and has a draft law to that effect. Of the former EFTA countries, only Liechtenstein has yet to implement the Directive, but it is thought that it will follow the Swiss implementation in due course.
10. Id. at art. 4(a), 1991 O.J. (L 122) 44.
11. Id.
12. Id. at art. 4(b), 1991 O.J. (L 122) 44.
copyright owner's authorisation "where they are necessary for the use of
a computer program by the lawful acquirer in accordance with its in-
tended purpose . . . ."13 This is somewhat contradicted by one of the
Recitals,14 which states that "the acts of loading and running necessary
for the use of a copy of a program which has been lawfully acquired . . .
may not be prohibited by contract."15 Added uncertainty stems from the
vagueness of the term "intended purpose." Is it the copyright owner's
intention that is material, and further, can "intended purpose" and "use"
be applied to the operation of or retrieval of computer programs via the
Internet?

Article 6 gives the right to decompile another's computer program in
limited circumstances.16 In particular, it provides that "the authorisa-
tion of the right holder shall not be required where reproduction of the
code and translation of its form . . . are indispensable to obtain the infor-
mation necessary to achieve the interoperability of an independently cre-
ated computer program with other programs, provided that the following
conditions are met."17 These are as follows: (a) only lawful users are en-
titled to decompile;18 (b) the information sought must not have been
readily available to a lawful user from another source, e.g., observing,
studying and testing a program whilst making ordinary authorised use
of it;19 and (c) only the relevant part of the program may be
decompiled.20

Restrictions on the uses to which information acquired from decom-
ilation may be put make it clear that it is only permitted in order to
enable a user to achieve interoperability and not, for instance, to allow a
third party to develop a program substantially similar in its expression
to the decompiled program.21

The Software Directive requires Member States to provide appro-
appropriate remedies against activities such as circulating infringing copies of
programs, possessing infringing copies, and possessing or circulating
anti-copy protection devices intended specifically to facilitate "the re-
moval or circumvention of any technical device which may have been ap-
plied to protect a computer program." Under the Software Directive, "the

14. The legal effect of the preamble to a directive, known as the "Recitals," is
uncertain.
16. Id. at art. 6.1, 1991 O.J. (L 122) 45.
17. Id.
18. Id. at art. 6.1(a), 1991 O.J. (L 122) 45.
20. Id. at art. 6.1(c), 1991 O.J. (L 122) 45.
21. Id. at art. 6.2(c), 1991 O.J. (L 122) 45.
term of protection should be the life of the author plus fifty years . . . ."22 However, under a recent directive on the harmonisation of copyright duration, the term of protection will soon be increased to life plus 70 years.23

**GII Issues**

It could be argued that if the right-holder distributes a computer program over a global network, such as the Internet, the action of sending the work is implied authority to network service providers to copy, adapt etc. to the extent necessary for transmission and delivery of the program. It is debatable whether the same is true in the case where the right holder merely makes the program available for retrieval via the Internet. If the use of the program by the lawful acquirer is such that the "intended purpose" and "use" involves communication over a network, it is likely that even without the right holder's authorisation, copyright will not be infringed (at least not by that lawful acquirer and probably not by the network providers).

The decompilation right is a side issue, but one which might become very useful to a software developer who wishes to get his program to interoperate with another program elsewhere on the GII.

Lastly, the definition of "anti-copy protection devices" is so wide that it could be construed as applying to computer "cracker" programs.24 Such programs circumvent "login" programs which are used to protect computer systems and the programs on them. It remains to be seen whether a legislative provision implementing this will be interpreted as regulating the circulation or possession for commercial purposes of programs commonly used to test network security.

2. **Proposed Databases Directive**

The proposal for a directive to harmonise database copyright throughout the EU dates from January 29, 1992.25 The proposal, which was subsequently amended in response to suggestions made by the Euro-

---

22. *Id.* at Recitals, 1991 O.J. (L 122) 43.
European Parliament, builds on the approach adopted in the Software Directive. The draft directive, which has been further amended, has recently reached the “common position” stage, with a proposed deadline for implementation by the EU Member States before January 1, 1998.

The proposal applies to databases in any form defined as “a collection of works, data or other independent materials arranged in a systematic and methodical way and capable of being accessed by electronic or other means.” The proposal requires that databases be protected by copyright if, “by reason of the selection or arrangement of their contents [they] constitute the author’s own intellectual creation.” The copyright protection given by this Database Directive would not, however, extend to the individual works or materials contained within a database. It is interesting to compare this with the US decision in the Feist Publications, Inc. v. Rural Telephone Serv. Co., where the Supreme Court held that a minimum level of originality or creativity used in the selection and arrangement of facts was necessary to obtain database copyright protection; mere “sweat of the brow” was insufficient. Many EU Member States have tended to deny copyright protection to databases unless a high degree of originality is shown and, consequently, the Database Directive would increase the availability of copyright protection for databases in those countries. However, the Database Directive is likely to reduce the protection currently enjoyed in the UK and Ireland where “sweat of the brow” compilation databases may currently be protected by copyright. The Database Directive would not apply to a “computer program used in the making or operation of the database” which can be “accessed by electronic means” nor will it prejudice the application of the Software Directive, the Rental Directive or the Term Directive.

The draft Database Directive provides that the author of a database shall have the exclusive right to do or to authorise temporary or permanent reproduction, translation, adaptation, arrangement and any other alteration, and any form of distribution, communication, display or per-

28. Id. at arts. 1.1 and 1.2.
29. Id. at art. 3.1.
30. Id. at art. 3.2.
32. Feist, 499 U.S. at 340.
formance to the public.\textsuperscript{37} The lawful user would be entitled to perform any of the above acts which are necessary to gain access to the contents of the database. Moreover, Member States would have the option to provide additional exceptions, for example in respect of fair use or national security.\textsuperscript{38} Any substantial change to the contents of a database would give rise to a new database, for which the period of protection (the same period that is applicable to literary works) would start again.\textsuperscript{39}

There would also be a new \textit{sui generis} right which would entitle the maker of a database to control the extraction and/or reutilisation of the whole or a substantial part of the database. To qualify for protection, a maker of a database would need to be able to demonstrate "that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents . . . ."\textsuperscript{40}

The \textit{sui generis} right would last for fifteen years\textsuperscript{41} and would apply irrespective of the eligibility of the contents of a database or of the database as a whole for copyright protection.\textsuperscript{42} It would not apply, however, to such of the contents of the database as were themselves protected by copyright. Because there would be a lower originality threshold than for copyright, this new "extraction" right would confer protection upon databases which would not currently be protected in the US or in most Member States. However, individuals not habitually resident and firms not established in an EU Member State would not initially, and might never, benefit from the \textit{sui generis} right.\textsuperscript{43}

The proposed Database Directive also refers to further categories of rights which may constitute additional levels of protection. Thus the Database Directive "shall be without prejudice to provisions concerning in particular copyright, rights related to copyright or any other rights or obligations subsisting in the data, works or other materials incorporated into a database, patent rights, trade marks, design rights . . . unfair competition, trade secrets, security, confidentiality, data protection and pri-

\textsuperscript{38} Common Position (EC) No. 20/95 on legal protection of databases, art. 6, 1995 O.J. (C 288/02) 22.
\textsuperscript{39} \textit{Id.} The full test would be: "Any substantial change, evaluated qualitatively or quantitatively, to the contents of a database, including any substantial change resulting from the accumulation of successive additions, deletions or alterations, which would result in the database being considered to be a substantial new investment . . . ." \textit{Id.}
\textsuperscript{40} \textit{Id.} at art. 7.1.
\textsuperscript{41} \textit{Id.} at art. 10.2.
\textsuperscript{42} \textit{Id.} at art. 7.4.
\textsuperscript{43} Common Position (EC) No. 20/95 on legal protection of databases, arts. 11.1 & 11.2, 1995 O.J. (C 288/02) 22. Acting on a proposal from the European Commission, the European Council would be authorised to conclude agreements with third countries. \textit{Id.} at art. 11.3.
vacy, access to public documents and the law of contract.” It seems inevitable that there will be conflict and confusion in determining the precise application of all of the existing and proposed rights.

**GII Issues**

The database proposal applies to collections of electronic materials accessed by electronic means. It may well be that many of the components of the digital superhighway together with the information it carries will fall within this definition; from router tables, and domain name resolvers to the collection of links presented by HTML pages on the World Wide Web, as well as the vast amount of material made available by information providers. The impact on material transmitted via the Internet would then be considerable.

A computer-generated table is not the result of an author’s intellectual creation and therefore would not attract the protection of copyright under the Database Directive or elsewhere. However, the *sui generis* right to control extraction might still apply. This might have unexpected consequences. For example, router tables are used for commercial purposes and need to be used between the networks that comprise the Internet to allow efficient routing of data. When the proposed Database Directive comes into effect, it would be advisable for network service providers who wish to utilise router tables which fall within the jurisdiction of any EU Member State to enter into an agreement with the owners of those router tables in order to use them. This already looks like a cumbersome result and how this area will develop in practice remains to be seen.

The World Wide Web and Gopher are virtual areas that span the Internet and allow users to display their own information and provide pointers to information elsewhere. An HTML script describing a World Wide Web page can be categorised in a number of ways. It is, as its name suggests, written in a computer language and as such may receive protection as a computer program under the Software Directive. It may attract copyright protection as a literary work in its own right, and as a method of representing a collection of works selected by intellectual

---

44. *Id.* at art. 13.
45. These are large databases which are necessary to route traffic on a data network. Each network operator contributes to the database, and all are given access to it.
46. Hyper Text Markup Language. HTML documents are a kind of “living address book” where clicking on a highlighted entry is the functional equivalent of placing a data “call” to the address described.
47. Although in the United Kingdom, provisions which cater for computer-generated works currently cover computer-generated databases.
48. The fact that selecting these links may not lead to the infringement of copyright of another work is an interesting legal issue which space does not permit us to address here.
creation, it may receive copyright protection as a database under the proposed Database Directive.

It will become very important to understand how these rights interact so that providers of information are able to protect their creations in an environment where copying is instant and prevalent, and are also able to inform consumers of their information as to their rights so that they understand what the limits of their permitted use of that material is.

C. Proposed Data Protection Directives

Privacy and data protection issues have been receiving increasing attention as awareness has grown of the scope for collecting, processing and transferring vast quantities of personal information on the GII. After five years of heated debate and lobbying, on July 24, 1995, the European Council adopted a Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "Framework Directive"). A related Commission Proposal for a Council Directive would deal with the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the Integrated Services Digital Network ("ISDN") and public digital mobile networks. The current text of this proposal is the Amended Proposal of June 13, 1994 (the "Telecoms Directive").

The aim of the Framework Directive and proposed Telecoms Directive is to ensure a high level of protection for personal data whilst preserving the free flow of information within the EU. A detailed analysis of the measures is beyond the scope of this paper, but two of the many issues raised by the proposals are of particular relevance to the current discussion. The first is the requirement that a "controller" of personal data obtain express, informed consent from individuals before processing data about them. The second is the cumbersome regime which would be established to regulate exports of data outside the European Union.

51. For a fuller discussion, see Christopher Millard, Data Protection in DATACOMMS USERS HANDBOOK 79 (1994).

The Framework Directive requires EU Member States to ensure that individuals have certain rights and that standards are set for data quality. The Framework Directive has a number of significant and controversial features. First, with a few limited exceptions, the Framework Directive only permits data to be held relating to individuals with their consent, and such consent must be express, informed, and freely given. Second, the Framework Directive regulates structured collections of manual data as well as data held in computerised form. Third, the Framework Directive will restrict the export of personal data outside the EU to countries which do not have an “adequate” level of data protection.

Personal data is defined as “any information relating to an identified or identifiable natural person” and processing has been given a very wide meaning by the Framework Directive. There are various principles which relate to the quality of data that is processed and the circumstances in which data processing is legitimate. A primary obligation on the person who determines the purposes and means of the processing, the “controller,” is to notify a supervisory authority before carrying out any wholly or partly automatic processing operation.

Article 7 of the Framework Directive lays down the grounds upon which personal data may be processed. "Processing" means performing any operation or set of operations on the data. In the absence of unusual circumstances, such as a legal obligation to disclose, personal data may only be processed in the following situations: (1) where the data subject has consented; (2) where it is necessary in relation to the entering


53. For example, the right to information, the right of access, the right to rectification and the right of opposition.

54. For example, data must be accurate, fairly collected, and stored for specified and lawful purposes.

55. Common Position (EC) No 1/95 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, art. 2(h), 1995 O.J. (C 93/1).

56. Id. at art. 3.1.

57. Id. at art. 25.1.

58. Id. at arts. 2(a) and 2(b).

59. Id. at art. 2(d).

60. Common Position (EC) No 1/95 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, art. 18.1, 1995 O.J. (C 93/1).

61. Id. at art. 7.

62. Id. at art. 7(a).
into or performance of a contract; or (3) where it is necessary in the
pursuit of the "general interest" or "legitimate interests" of the person
controlling the data, unless these are overridden by the interests of the
data subject. The possible application of the terms of the proposed
Framework Directive to the use of the Infobahn leads to some curious
results.

GII Issues

Of particular interest to those who view data superhighways as a
medium of expression is an exception to the scope of the directive pro-
vided in the Recitals for the "processing of sound and image data carried
out for the purposes of journalism or the purposes of literary or artistic
expression . . . in particular the audiovisual field . . . ." For this reason,
Member States would be required to provide an exemption where it is
necessary in order to "reconcile the right to privacy with the rules gov-
erning freedom of expression." The scope of this exception is uncertain.

The Recitals also address the situation where a message containing
personal data is transmitted using a telecommunications or electronic
mail service, the sole purpose of which is the transmission of such
messages. The controller in respect of the personal data in this instance
will normally be considered to be the sender, rather than the person of-
f ering the transmission services, although those offering the transmis-
sion service will normally be considered controllers in respect of any
additional personal data necessary for the operation of the service.

Regarding data exports, Article 26 of the Framework Directive pro-
vides that a transfer of personal data to a country outside the European
Union may only take place if the country to which the data is sent en-
sures an adequate level of protection. This blanket prohibition is sub-
ject to various exceptions which will not be relevant to a great deal of
Internet traffic. Article 27 provides that a Member State may, how-

63. Id. at art. 7(b).
64. Id. at art. 7(f).
the protection of individuals with regard to the processing of personal data and on the free
movement of such data, recitals, 1995 O.J. (C 93/1).
66. Id. at art. 9.
67. Id. at art. 26.
68. Id. at art. 26.1 (1-6) provides that this prohibition will not apply where:
(1) the data subject has given his consent unambiguously to the proposed transfer,
or
(2) the transfer is necessary for the performance of a contract between the data
subject and the controller or the implementation of precontractual measures taken
in response to the data subject's request, or
(3) the transfer is necessary for the conclusion or for the performance of a contract
concluded in the interest of the data subject between the controller and a third
party, or
ever, authorise a transfer of personal data to a third country which does not ensure an adequate level of protection even where the exceptions do not apply provided that the data controller has produced sufficient justification, for example by guaranteeing the effective exercise of the data subject's rights. In such circumstances, it is proposed that the Member State will inform the Commission and the other fourteen Member States in good time of its proposal to grant authorisation for such a transfer. If another Member State objects before the authorisation is to take effect, then the Commission will be obliged to resolve the problem by reference to an advisory committee.

There can hardly be a more stark contrast in the age of the "Global Village" than between the image of a computer user who may, with the press of a button, send a message almost instantaneously to a large number of correspondents around the globe and that of the political process which would inevitably be followed before all the Member States of the European Union could be persuaded to approve such a transfer. In such a situation, it is difficult to imagine most computer users doing anything other than pressing the button without any regard to the legal regime in which they operate.

2. The Telecoms Directive

The amended proposal for the Telecoms Directive would apply to all digital networks and, where possible, to analogue networks as well. Many of the rules would apply to all service providers and all users of telephone services. As the original proposal was criticised for being excessively detailed, the amended proposal aims to simplify its terms, but provides a broad mandate to the European Commission to adopt further measures.

The amended Telecoms Directive proposal is intended to ensure an equivalent level of protection of personal data and privacy in Member States in the communications context and to provide for the free movement of telecommunications equipment and services in the EU. On one level it would regulate the activities of "Telecommunications Organisations," i.e., public or private bodies licensed for the provision of a public telecommunications network or public telecommunication services. Its aim would be to limit the extent to which such persons are entitled to

(4) the transfer is necessary on important public interest grounds, or for the establishment, exercise or defence of legal claims, or
(5) the transfer is necessary in order to protect the vital interests of the data subject, or
(6) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.
hold personal data about their customers. Some of the provisions of the Telecoms Directive relating to such limits would extend to "Service Providers" and some rules could only be implemented by placing restrictions on every user of telecommunications services.

The provisions that concern Service Providers include:

- **Security.** In case of particular risk of a breach of the security of the network, the telecommunications organization must inform the subscribers concerning such risks and offer them encryption facilities.

- **Billing data.** For the purpose of billing, data containing the number or identification of the subscriber station, the total number of units to be charged, the type and duration of the calls made has to be restricted to the persons in charge of billing and such a storage of billing data is permissible only up to the end of the statutory period during which the bill may be challenged.

- **Traffic data.** Traffic data containing the personal data processed to establish calls and stored in the switching centres of the telecommunications organizations must be erased as soon as it is no longer necessary to provide the service required.

- **Directories.** Personal data contained in a directory should be limited to what is strictly necessary to identify a particular subscriber, unless the subscriber has given his consent to the publication of additional personal data. The subscriber shall be entitled, free of charge, not to have his or her sex indicated and to be omitted from the directory at his or her request.

**GII Issues**

The first issue is to determine to whom these rules apply. The Telecoms Directive, including the above provisions, applies to telecommunications organisations. The above rules also apply to "Service Providers" who are defined as "providing services whose provision consists wholly or partly in the transmission and routing of signals on a public telecommunications network, with the exception of radio broadcasting and television," and others who provide telecommunication services over the public telecommunications network.

In the U.K., much of the capacity for the Internet is leased from telecommunications organisations, and thus falls within the given definition.

---

69. *See infra* text accompanying note 73 for a definition of "Service Providers."


71. *Id.* at art. 5.

72. *Id.* at art. 6.

73. *Id.* at art. 11.

74. *Id.* at art. 2.2.
of public telecommunications network, even though the network capacity may not be available to the public at large. In the context of the digital superhighway, the definition of Service Provider would appear to include a network provider, that is, someone who carries Internet traffic. Moreover, most people are likely to have access to the Internet and on-line services via dial-up lines provided by Telecommunications Organisations.

D. PROPOSED EU “DISTANCE SELLING” LEGISLATION

A common position text of a Directive on the protection of consumers in respect of distance contracts (“Distance Selling Directive”) is currently before the Commission. No date has yet been set for the adoption of this Directive. As currently proposed, the Distance Selling Directive covers videotext, E-mail and most other forms of direct marketing including catalogue mail order, newspapers and magazines, direct response television and telephone selling. Some of the main provisions of the Proposal are as follows:

- the consumer must be given certain minimum information both at the time of contract solicitation and at or before the time of delivery;
- consumers must, subject to certain exceptions, be given a “cooling-off” period of at least seven working days;
- where the consumers exercises the right of withdrawal, the supplier is obligated to reimburse the consumer for sums paid; and
- cold-calling through telephone, fax or electronic mail must not be used unless the consumer has given his consent.

E. TV WITHOUT FRONTIERS DIRECTIVE

In identifying legal issues which apply to “convergence” technologies, the entire body of regulation which was originally designed to apply to “television” and “radio” broadcasting activity should not be overlooked. Many people do not think of data networks such as the Internet as a television or radio broadcasting medium, but in fact data networks have been used for a number of years to transport graphic images, sound files, and full motion video. Depending upon the wording of individual statutes, a great deal of network transmission activity may be caught by traditional “broadcasting” regulation.

76. Id. at arts. 4 and 5.
77. Id. at art. 6.1.
78. Id. at art. 6.2.
79. Id. at art. 10.1.
With the advent of direct-to-home satellite broadcasting in the early 1980's, European regulators recognised that they would have to take steps to harmonise European broadcasting rules. One of the more tangible results of this process has been the promulgation of the so-called Television Without Frontiers Directive ("Frontiers Directive"). The Directive addresses issues of promotion, distribution and production of television programmes, TV advertising and sponsorship, the protection of minors and the right of reply. The Frontiers Directive has always been controversial, and is one part of an overall process whereby Europe is coming to terms with the globalisation of media products. One of the most hotly debated parts of this process is how to determine the right balance between open trade and competition in services, and the desire of some European nations to preserve their own unique cultural identity. In essence, many European governments are worried that the mass production of American entertainment products has the potential to displace various entertainment media which can be identified as "European." As a result, the Frontiers Directive mandates that a Member State must ensure "where practicable and by appropriate means" that a broadcaster reserves a majority of transmission time for European programmes.

**GII Issues**

It is not entirely clear whether parts of the Frontiers Directive might apply to various advanced broadband network services. The Directive definition of "television broadcasting" specifically excludes "communications services providing items of information or other messages on individual demand such as telecopying, electronic data banks and other similar services," but it is not clear from this description what exactly is being excluded. The exclusion would appear to apply to video-on-demand services, but point-to-multipoint video distribution via an experimental multimedia backbone would probably be caught by the Frontiers Directive. In addition, it bears repeating that individual Member State implementation can go beyond the terms of the Frontiers Di-

---

81. The French are among the most vociferous proponents of this "cultural imperialism" argument.
82. Council Directive No. 89/552/EEC, art. 4.1, 1989 O.J. (L 298) 26. The Directive excludes time for news, sports events, games, advertising and teletext services from this calculation. *Id.* The definition of a "European programme" is so wide, however, that many projects financed by non-European sources can now be classified as European if they are produced in an EC Member State. *Id.* at art. 6.1.
83. *Id.* at art. 1(a).
84. Such MBONE projects are already well advanced in both the US and the UK.
rective itself—the Directive merely sets a base-line requirement for regulation.85

III. UK REGULATION OF GII TRAFFIC

A. DEFAMATION

Defamation which takes place in the context of computer networks has received a great deal of popular attention in the press.86 Court actions have been filed in the United States and Australia with at least one, Cubby, Inc. v. CompuServe, Inc.,87 proceeding to final judgment. An English law analysis of cyberspace defamation must consider a number of difficult issues.

First, one has to determine whether to characterise the defamation as libel or slander.88 This is an important point in English law because a plaintiff is required to prove special damages in order to recover on a claim of slander. No proof of special damages is required in a libel action. Older English cases held that unscripted words spoken over the radio did not contain a sufficient quality of permanence in order to constitute libel, and were thus classified as slander.89 Presumably, a message posted to an electronic bulletin board would be deemed sufficiently “permanent” to be counted as libel. The situation with messages in the context of more advanced network services such as Internet Relay Chat or various point-to-multipoint audio and video transmissions could be less certain.90

Next, one must determine whether the defamatory remark has been “published.” The law requires publication to a third party before defamation liability will attach, and it is arguable whether such publication occurs if the remark is merely available to a number of persons connected to a network. A plaintiff could face the daunting task of proving that

85. In fact, implementation of the Directive has proven highly contentious.
88. “Libel” is generally considered to be defamation which occurs in print, while “slander” is normally thought of as defamation which is spoken.
89. The law was specifically changed to characterise defamation delivered in such broadcasts as libel. Broadcasting Act, 1990, § 166 (Eng.); see generally Defamation Act, 1952 (Eng.).
90. But see the discussion below in section III D, infra, on whether some transmissions via data networks might constitute a “programme service” as defined in the Broadcasting Act 1990. Any defamatory remark published in the course of any programme included in a “programme service” will be characterised as libel rather than slander. See Broadcast Act, 1990 (Eng.).
some third party connected to a network has actually read the defama-
tion in question.\textsuperscript{91}

Quite apart from the question of liability on the part of the person
who authors a defamation, there is a serious concern about liability at-
taching to distributors of defamation. Under English libel law, news
vendors, booksellers and distributors are able to take advantage of an
"innocent dissemination" defence if the distributor can prove that he was
not negligent in the act of distributing the defamation.\textsuperscript{92} Presumably,
network operators and service providers will be able to take advantage of
this defence. Demonstrating that the defence applies, however, could
prove a daunting task for any Internet service provider given the regu-
larity of vitriolic exchanges which occur in the context of certain Usenet
news groups. Courts have indicated that the defence will not apply if the
distributor knew, or should have known, that a newspaper was "of a
character" that was likely to contain libel. If the Usenet system is con-
sidered as a whole, it is a system which undoubtedly contains defama-
tory statements which are published on a daily (probably hourly) basis.
Alternatively, if a court looks at each of the 10,000-plus news groups as
an individual publication, network operators might be able to escape lia-
bility if they refuse to accept or redistribute feeds from those groups
which have attained a reputation for containing defamatory remarks.\textsuperscript{93}

In 1994, United Kingdom academic Dr. Laurence Godfrey issued a
libel writ in London against the author of allegedly defamatory remarks
which were posted to a Usenet news group.\textsuperscript{94} The case recently settled.
Significantly, the defendant in the action was a Swiss academic and it is
believed that he "posted" the remarks in question while physically situ-
at ed in Switzerland. Had the case proceeded to trial, the court would
have had to grapple with difficult issues of where "publication" actually
took place. Under a traditional analysis, the alleged defamation may
have been "published" in every country in the world where there is a
computer capable of browsing Usenet news groups. This raises the pos-
sibility that jurisdictions with fairly rigorous defamation laws (like Eng-
land) could play host to litigation by parties from around the world
seeking to redress harm to their reputation.\textsuperscript{95}

\textsuperscript{91} See Nick Braithwaite & Robert Carolina, \textit{Multimedia Defamation}, \textit{International
Media Law} 20, March, 1994. It is recognised, of course, that this will not be a problem in
some cases.

\textsuperscript{92} Sun Life Assurance Co. of Canada v. W.H. Smith & Co. Ltd., 1933 All ER 432
(Court of Appeal); and Emmens v. Pottle, 16 QBD 354 (1885).

\textsuperscript{93} Examples of such news groups are \textit{alt.flame}, or many of the groups detailed
\textit{alt.fan}.*

\textsuperscript{94} Rich, supra note 86, at 22.

\textsuperscript{95} See Michael Smyth & Nick Braithwaite, \textit{First UK Bulletin Board Defamation Suit
Brought}, The Nat'l L. J., September 19, 1994 (on file with the author). Note that parties
will only be able to recover damages based upon the harm to the reputation which they
A Bill to amend the law of defamation is currently before the United Kingdom Parliament.\textsuperscript{96} If enacted, the Bill would establish a general defence for a person who can show that "he was not primarily responsible for the publication of the statement complained of and that he did not know, and having taken all reasonable care had no reason to suspect, that the acts involved or contributed to the publication of a statement defamatory of the plaintiff."\textsuperscript{97}

More specifically, the Bill provides that certain categories of person shall not be regarded as primarily responsible for the publication of a defamatory statement, including:

(c) [In the case of a defamatory statement published by electronic means, a person involved only
   (i) in processing, making copies of, distributing or selling any electronic medium in or on which the statement is recorded, or
   (ii) in operating any equipment by means of which the statement is retrieved, copied or distributed . . . ]\textsuperscript{98}

Early signs are that the Bill may attract cross-party support. However, even if the Bill is adopted, uncertainty is likely to remain as to how an online service provider or Internet access provider can discharge the duty to take "all reasonable care" to avoid publishing defamatory material.

B. COPYRIGHT

1. General Framework

In the United Kingdom, protection of authors against copying is regulated by the Copyright, Designs and Patents Act of 1988 ("CDPA"), as amended to reflect a series of EU directives which attempt both to recon-

\textsuperscript{96} "An Act to amend the law of defamation and to amend the law of limitations with respect to actions for defamation and malicious falsehood." Draft of a Defamation Bill (Eng. 1995) (on file with the author).

\textsuperscript{97} Id. at Clause 1(1). This principle is elaborated in Clause 1(5) and (6) as follows:
   (5) In determining for the purposes of subsection (1) whether a person took all reasonable care, regard shall be had to the extent (if any) to which he is in fact responsible for the content of the statement or the decision to publish it.
   (6) In determining for the purposes of subsection (1) whether a person had reason to suspect that his acts involved or contributed to the publication of a statement defamatory of the plaintiff, regard shall be had to whether the nature or circumstances of the publication, or the previous conduct or character of those primarily responsible, were such as to give cause for suspicion that his acts might involve or contribute to the publication of a defamatory statement.

\textsuperscript{98} Draft of a Defamation Bill, supra note 96, at 2.
cile the differing copyright regimes in Member States and to regulate, or
at least keep pace with, some of the changes taking place in information
technology. Unfortunately, despite these efforts, the law as it stands
either fails to address or fails to clarify some of the issues raised by the
emerging data superhighway. A fundamental question that arises in re-
lation to network operators is whether merely by following the instruc-
tions of their customers to transmit messages, they may incur liability in
respect of infringing material contained within those messages.

There are two types of infringement of copyright in the United King-
dom: primary and secondary. Secondary infringement deals mainly with
the possible liability of distributors. As this is the most obvious way in
which network operators may be found liable for copyright infringement,
we shall look at this first.

2. Secondary Infringement

An essential characteristic of secondary infringement is the require-
ment of actual or imputed knowledge. That is to say, secondary infringe-
ment only takes place if the infringer knew or had reason to believe that
an infringement had taken place.

Most of the conduct constituting secondary infringement relates to
the use of infringing copies. A network operator will not be liable for
secondary infringement unless the material being transmitted already
infringes copyright. Secondary infringing conduct includes possessing
and dealing with infringing copies and facilitating infringement by
transmitting the work by means of a telecommunications system. Network operators may be caught by the “possessing and dealing” provi-
sions, but the more clear case is that of “transmission.”

The CDPA provides that “copyright in a work is infringed by a per-
son who without the license of the copyright owner transmits the work
by means of a telecommunications system (otherwise than by broadcast-
ing or inclusion in a cable programme service), knowing or having reason
to believe that infringing copies of the work will be made by means of the
reception of the transmission in the United Kingdom or elsewhere.”

This is likely to cover the activities of network operators, provided, as it

100. Id. § 23.
101. Id. § 24(2).
102. Possessing and dealing with infringing copies includes possessing, exhibiting or
distributing infringing copies in the course of a business. Id. § 24(1). In this context, pos-
session includes possession by persons performing a service in relation to the article. Id.
However, it may be that the meaning of “in the course of a business” is restricted to a
business which deals with that type of article, in which case the network operator would
not be caught by this provision. Id.
103. Id. § 24(2).
says, they know or have reason to believe that copies of the work will be made.

It is an open question as to when the knowledge requirement described above will be met. Would it be sufficient for a software house to issue a letter to a network owner stating that in all probability, the network was being used for the purpose of creating infringing copies? Would it be sufficient to produce evidence that a specific customer was using the network in this manner? Would it be sufficient that the network operator knew that the material being transmitted was sourced from a copy of the material from a neighboring network, which was unlikely to have received explicit permission to copy the work? The authors' view is that network operators should not be held to have the requisite knowledge unless and until they receive very specific and detailed information concerning the activities of a specific customer. Even at this point, there are probably valid policy reasons for not holding network operators liable.\footnote{104}{See CBS Songs Ltd. v. Amstrad Consumer Electronics plc., 2 All E.R. 484 (1988) (holding that the manufacturer of twin-deck cassette tape recorders was not liable for the activities of those who purchase the machines).}

3. Primary Infringement

The question of primary infringement deserves special consideration. If a message sent on the instructions of a customer infringes copyright, then the customer will be liable for primary infringement under the CDPA. What is of concern to us is that, as the law stands, the network operator may well find himself liable to the same degree as the customer for primary infringement.\footnote{105}{See Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla 1993) (holding bulletin board operator strictly liable for primary infringement of copyright in image data file even if he had no knowledge of the file's passage through his computer). The US position may, however, be less harsh given the potential application of "common carrier" status to certain network operators.}

An important distinction between primary and secondary infringement is that, unlike secondary infringement, primary infringement is not dependent on any intention or knowledge on the part of the defendant—primary infringement is a strict liability matter. Thus a defendant who makes infringing copies of a work at the request of another in the mistaken belief that the other is either the owner of the copyright or a licensee, will have no defence to infringement proceedings.

The CDPA provides a list of "acts restricted by copyright," each of which constitutes a primary infringement of copyright unless it is done with the license of the copyright owner.\footnote{106}{CDPA, supra note 99, § 16(1).} These acts include copying the work; issuing copies of the work to the public; performing, showing or
playing the work in public; and broadcasting the work or including it in a cable programme service. We shall look at these in turn.

i. Copying

The term copying does not have just one definition: its meaning varies according to the type of copyright work in question.

Copying of a literary, dramatic or musical work is defined as "reproducing the work in any material form."\(^{107}\) An artistic work may be copied from one form into another. Thus, for example, the copyright in a painting may be infringed by the making of a sketch\(^{108}\) or by taking a photograph.\(^{109}\)

It is primary infringement of the copyright in a film or sound recording to copy the work by making a photograph of the whole or any substantial part of any image forming part of that film. Taking one still from a film and publishing it as a photograph is primary infringement. The meaning of copying in relation to a broadcast or cable programme is normally presumed to be the same as for films or sound recordings.

The position with regard to computer programs is quite complex. As computer programs are within the definition of literary works, unauthorised reproduction of a program in any material form will constitute an infringement. However, there is an exception to this general prohibition on copying to cover the making of necessary back-up copies.\(^{110}\) "Necessary" could be narrowly defined to mean the making of a single back-up copy in order to protect against damage to the original copy or could involve a number of copies. In addition, unless prohibited by contract, a lawful user of a program may make a copy of it for any purpose other than back-up or decompiling provided that the copying is necessary for his lawful use.\(^{111}\) The question is: Would the term "lawful use" cover the activities of a network operator?

As a separate issue, there is an argument, not yet tested in the United Kingdom, that the screen display generated by a computer program is a copyright work in its own right. In the United States case of Digital Communications Assoc. v. Softklone Distrib. Corp., Inc.,\(^{112}\) it was held that copying the screen display is infringement of the copyright in the screen display regardless of whether the codes of the programs used to produce the screen display are similar or in the same language.

---

107. CDPA, supra note 99, § 17(2). It does not, however, include the copying of a two-dimensional work into three-dimensional form. Id. § 17(3).
110. CDPA, supra note 99, § 50A(1).
111. CDPA, supra note 99, § 50C.
Additionally, if the coding for the program is copied, this may amount to an infringement of the copyright in the screen display. This may be relevant to the case of network operators, as they may find themselves liable for infringement of the rights in the display without ever having displayed the images that can be reproduced from the information that they have copied.

**ii. Issuing Copies of the Work to the Public**

The equivalent infringing act in the Copyright Act of 1956 was “publishing the work.” This meant the publishing of the unpublished. That is to say, infringement could be committed only by the person who first issued copies to the public without the consent of the copyright owner. It would not be committed by any subsequent distributor. This is endorsed in the CDPA, which provides that “issuing copies of the work to the public” means “the act of putting into circulation copies not previously put into circulation, in the United Kingdom or elsewhere.”

However, if new copies are made, the person who issues them to the public will not be exempt from primary infringement by virtue of the fact that other copies have been issued with the copyright owner’s consent. Hence, it would seem that even if the person supplying a copyrighted work to the network operator for distribution is properly licensed by the copyright owner to do so, the network operator may still be liable for primary infringement if new copies are circulated by him as a result of transmission.

**iii. Performing, Showing or Playing the Work in Public**

If the work is a literary, dramatic or musical one, performing, showing or playing the work in public will constitute primary infringement. “Performing” includes “any mode of visual or acoustic presentation, including presentation by means of a sound recording, film, broadcast or cable programme of the work.” This would seem to cover the activities of network operators.

In the case of a sound recording, film, broadcast or cable programme, the playing or showing of the work in public is restricted by copyright. No definition of what constitutes “playing” or “showing” is provided, but it is quite possible that a network operator may be construed as doing either one.

---

113. Copyright, Designs and Patents Act, 1988, § 18(2) (Eng.).
114. Id. § 18(2)(b).
115. Id. § 19(3).
The CDPA provides that it is an act restricted by copyright to include, in a broadcast or cable programme service, a literary, dramatic, musical or artistic work, a sound recording or a film. Again, it is likely that the activities of network operators would be caught by this provision.

C. DATA PROTECTION

Data protection in the United Kingdom is regulated by the regime established by the Data Protection Act 1984 ("DPA"). Broadly, the DPA regulates the activities of people who control the contents and use of computerised data ("Data Users") insofar as the data over which they exercise control contains information relating to a living individual who can be identified from the data (this type of information is termed "Personal Data" under the DPA).

The DPA provides that a person shall not hold personal data unless that person has complied with the formalities necessary to effect a registration under the DPA with the Data Protection Registrar. A failure to register as required under the Act is an offence and can result in liability for the person or company that fails to register. Although there are various exceptions to the registration requirements, these are very limited in scope. It is probable that most Data Users who should have registered have failed to do so. Even the Data Protection Registrar, whose raison d'être is to keep the register, estimates that more than two-thirds of all United Kingdom Data Users have failed to register as required.

The DPA also regulates the categories of people to whom personal data may be disclosed and the countries to which personal data may be transferred, and the Data User must include details of all such types of disclosure and transferee countries in his registration. Once an entry has been made, operating outside the scope of the registration or failure to comply with eight "Data Protection Principles" may result in civil enforcement proceedings and, ultimately, in criminal sanctions.
Application of the DPA to Internet-related activities is problematic. The gulf between legal theory and operational practice is most clearly illustrated in the section of the Act dealing with the transfer of personal data from country to country. For the purpose of illustration, suppose that a company based in London is correctly registered to hold particular categories of personal data, and to be able to disclose the data to a subsidiary in Belgium. If an employee of the UK entity sends an e-mail message via the Internet to a colleague in the Belgian subsidiary, can he be satisfied that he has complied with all the provisions of the DPA? Even if he is confident that he is allowed to reveal the contents of the message to the intended recipient, at the point when the message is given to a data network operator, the UK-based employee will have made a disclosure not only to the network operator but also, perhaps unwittingly, to any person who intercepts Internet traffic. The DPA provides that it is an offence knowingly or recklessly to make an unauthorised disclosure of personal data. The informed user of a data network will be aware of the risk of messages being intercepted. This raises the possibility that sending unencrypted messages could be viewed as reckless for the purposes of the DPA. Continuing with the example given above, given that the message may pass through several other countries on its way to Belgium, the person sending the message should probably register for data transfers to all countries of the world.

D. United Kingdom Broadcasting Act

The United Kingdom regime of broadcast regulation is contained primarily in the Broadcasting Act of 1990. Among other things, the Broadcasting Act regulates the television transmission and content of “licensable programme services.” The Broadcasting Act defines a “licensable programme service” as a “service consisting in the provision by any person of relevant programmes with a view to their being conveyed by means of a telecommunications system . . . .” The term “telecommunications system” is defined so broadly as to encompass nearly any transmission medium. A “relevant programme” means a “television” programme which does not consist “wholly or mainly” of “non-representational images,” that is to say the programme is not “wholly or mainly” text-based. There are other exceptions to the definition of “li-

---

122. This paper only examines the position regarding “television” regulation. Similar restrictions apply to the broadcast of sound.
123. Broadcasting Act, 1990, § 46(1) (Eng.).
124. The term is given the same meaning as in the Telecommunications Act 1984. Broadcasting Act, 1990, § 202(1) (Eng.).
125. Broadcasting Act, 1990, § 46(5) (Eng.).
126. Broadcasting Act, 1990, § 2(6) (Eng.). The exclusion of wholly or mainly text-on-screen services was included with a view to excluding teletext services, a type of primitive
censable programme service" intended to cover business-to-business transmissions, but these clearly would not extend to cases where private individuals are able to download graphic images from remote file servers. Interestingly, there is an exemption which appears to have been drafted for video telephones and teleconferencing systems. Unfortunately, the Broadcasting Act does not define “television,” but the videophone exclusion may indicate that the term should be viewed in the broadest possible manner.

Arguably, any graphic or motion picture file resident on an open access Internet file server could be viewed as a licensable programme service, since millions of people are capable of receiving this image for non-business purposes. What regulations are there then, for such activity?

Under the Broadcasting Act, anyone who wishes to provide a licensable programme service must make an application to the Independent Television Commission (“ITC”), together with a fee. Any person who provides such a service without a license is guilty of an offence and liable to pay a fine. Any person who provides a licensable programme service must comply with the ITC code of practice, which gives guidance in relation to: Violence and sounds of violence, particularly “when large numbers of children may be expected to be watching . . . .”; programmes appealing for donations, matters concerning standards and practice.

bulletin board system broadcast in parallel with television signals and capable of reception on a properly equipped television. Nearly all televisions sold in the UK are capable of receiving teletext transmissions.

127. The definition does not apply to services where the receiver has a business purpose in receiving the transmission. Broadcasting Act, 1990, § 46(1)(a) (Eng.).

128. Broadcasting Act, 1990, § 46(2Xc) (Eng.). In fact, the exemption is said to apply to “a two-way service,” that is:

[A] service of which it is an essential feature that while visual images or sounds . . . are being conveyed by the person providing the service there will or may be sent from each place of reception, by means of the same telecommunications system . . . visual images or sounds . . . for reception by the person providing the service or other persons receiving it (other than signals sent for the operation or control of the service).

Id. Arguably, this may exempt a number of “television-like” activities which occur on data networks, but the use of the term “essential feature” as well as the operation and control signal qualification make the application doubtful.

129. Examples would include any GIF, TIFF, PICT or similar file containing graphic images, or MPEG files containing motion picture images. Many such files are available currently via the Internet as well as private commercial information services although, admittedly, the transfer rate is quite slow for most users.

130. Broadcasting Act, 1990, § 13 (Eng.).

131. Id. § 7(1)(a).

132. Id. § 7(1)(b).
for programmes, what may be included in programme advertise-
ments, and provisions regarding the control of advertisements. The Broadcasting Act itself lays out further requirements. "[N]othing is included in its programme which offends against good taste or decency or is likely to encourage or incite to crime or to lead to disorder or to be offensive to public feeling." There are restrictions regarding religious programmes, restrictions regarding subliminal messages and other means of influencing the minds of persons watching without their being aware of it, and restrictions on the programme provider expressing his/her views and opinions on matters of political or industrial controversy or which relate to current public policy. A license holder must retain, for a period not less than 90 days, a recording of every programme included in the licensed service and must produce such a recording to the ITC on request.

This body of regulation is probably not in the mind of the computer science student who electronically mails a copy of his vacation photographs to three or four friends around the United Kingdom. It may also not occur to an individual who loads a promotional motion picture file on his server for public consumption.

E. Other Content Regulation

Many other laws and regulations may have an impact on the content of various types of transmission. An obvious example is the various national restrictions on the importation, possession, and distribution of pornography. This is one area which has received a great deal of atten-

133. Id. § 8.
134. Broadcasting Act, 1990, § 9 (Eng.).
135. Id. § 6(1)(a).
136. Id. § 6(1)(b).
137. Id. § 6(1)(c).
139. Id. § 6(1)(e).
140. Id. § 6(4).
141. Id. § 11.
142. This type of activity might be exempted as a “two-way” service.
143. In this case, one could argue that the “two way service” exemption would not apply if the receiving party did not have a camera attached to his or her computer which could generate moving picture images. Alternatively, would it be enough to trigger the exemption that the computer is capable of reverse mailing the same MPEG file? As with most multimedia regulation, there are more questions than answers here.
Companies with significant computer networks should be especially cautious in this regard as a number of jurisdictions impose quite harsh penalties on those who distribute or possess pornographic images. Intellectual property rights other than copyright may also be supplemental. The protection applicable to trade marks confers rights which are relevant in the context of material distributed via the digital superhighway. Moreover, rights in relation to confidential information and trade secrets may be as significant in cyberspace as elsewhere.

Existing domestic legislation can also be applied in surprising ways. Section 43 of the Telecommunications Act of 1984 provides that it is an offence to send a message over a public telecommunications system which is grossly offensive or of “an indecent, obscene or menacing character . . . .”

Furthermore, it is a criminal offence to send a message or messages over a public telecommunications system which are intended to cause annoyance, inconvenience or needless anxiety. In the UK, many users of the Internet use the public telecommunications system either for modem access or over a leased line, and in this case it would seem that “flaming” and “spamming” could be criminal activities.

Other examples of content regulation include various broadcasting “blackouts” imposed for policy reasons. The most famous example in the United Kingdom was the ban on broadcasting the voice of any official representative of the Sinn Fein political party due to its alleged involvement in the promotion of terrorism. Courts around the world have also imposed various broadcast bans for the purposes of ensuring a fair trial for the accused in a criminal matter. In a less dramatic vein, securities laws in many jurisdictions regulate investment advertisements and advice.

F. JURISDICTIONAL ISSUES

Which laws will apply to the transactions on the GII? As a general rule, under English law, parties to a contract are free to choose which law will be applicable to the contract. In a case where the users are all subscribers to a service, the terms and conditions of their subscription

145. Telecommunications Act, 1984, § 43 (Eng.).
146. “Flaming” is a term of art describing vitriolic comment from contributors to material available via the Internet, often as a result of a breach of the network’s informal rules as to content (“netiquette”). “Spamming” is the process of deluging multiple Usenet groups with a single message.
may well specify the jurisdiction to be applicable to consequential retail
transactions. However, the Contracts (Applicable Law) Act 1990148 pro-
vides that even if a foreign jurisdiction is chosen for a consumer con-
tract,149 the foreign law will only apply to the extent that it will not
deprive the consumer of any protection he would receive under “the law
of the country in which the consumer has his habitual residence . . . .”150
Where there is no express choice of law, a consumer contract will be gov-
erned by the laws of the country in which the consumer is habitually
resident.151

It is impracticable to consider all the possible consumer protection
laws before making a sale. If the consumers are part of a defined group,
for example because they sign a subscription agreement, then that
agreement should specify the jurisdiction in which future transactions
will take place. If there is no such provision, or no such agreement then
the consumer should be warned, at the point of sale, that as a condition
of sale a certain jurisdiction will be used. Consumers will still be af-
forded their national consumer protection laws where the country is a
signatory to the Rome Convention, and where the country is not, the
country's own laws will determine how the transaction is treated.

We have dealt with jurisdictional issues relating to the retail trans-
action itself, but they also apply to the other transactions which com-
prise a home shopping service, for example, the contracts which bind the
parties who provide or convey the advertising information, the orders,
the payment and the goods. The jurisdiction applying to these contracts
will depend on the facts of the situation, the choice of law clauses in the
various contracts, the location of the parties and the location of equip-
ment attached to the network. We shall follow the approach adopted
earlier in this paper and divide the legal issues into infrastructure and
content. Although, in practice, legal advice covering a home shopping
service will need to be sought for many different jurisdictions, by way of
example we shall deal with those issues as if they were all subject to UK
law.

148. This implements the provisions of the Rome Convention signed by the UK on De-
cember 7, 1981.

149. For these purposes, a consumer contract is one where goods or services are sup-
plied to an individual outside his trade or profession. Contracts (Applicable Law) Act,
1990, art. 5.1 (Eng.). Different rules apply where a consumer is not involved.

150. Contracts (Applicable Law) Act, 1990, art. 5.2 (Eng.). In addition, the contract
should be preceded by a specific invitation addressed to the consumer or by advertising,
and he had taken in that country all the steps necessary for the conclusion of the contract;
or the other party or his agent received the consumer's order in that country. Home shop-
ping will generally satisfy one of these conditions. Id.

151. Id. at art. 5.3.
G. Advertising Regulations

Advertising regulations which are normally associated with more traditional retail transaction systems may also apply to commercial transactions on the GII. For example, in the UK:

- **Mail Order Transaction (Information) Order 1976**
  This Order provides that adverts should state the name and address of the persons carrying on the business.

- **Business Advertisements (Disclosure) Order 1977**
  This Order provides that those persons who sell goods in the course of a business must make it clear in their advertisements that they do so. This may apply to any “small-ads” section of the BBS.

- **Trade Descriptions Act 1968.**
  It is an offence to use a false trade description for goods offered for sale in the course of a business. In addition, it is an offence for a person in the UK to assist a person in another country who would otherwise be committing an offence under the Act. A BBS provider could thus be liable for a misleading advert placed by a foreign information provider.

- **The British Code of Advertising Practice and Sales Promotion.**
  This is a non-legally binding code of practice which lays down guidelines for the content of advertisements appearing in non-broadcast electronic media and viewdata services. Failure to comply can lead to requirements to withdraw or amend any offending advertisements, adverse publicity, difficulties in placing adverts (since most publishers and media owners have a policy of only disseminating adverts which conform with the code) and ultimately injunctions issued pursuant to the Control of Misleading Advertisements Regulations 1988.

- **The Common Law of Misrepresentation and the Misrepresentation Act 1967**
  If the goods or services were described in a materially false manner, the customer will be able to rescind the contract and obtain a refund of any monies paid. In addition, if the misrepresentation was fraudulent or negligent, the customer may choose to continue with the contract and obtain damages.

H. Consumer Protection Legislation

This section on legal analysis started by considering the particular problem of jurisdiction when applied to retail transactions involving an electronic home shopping service and concluded that the laws of all the countries involved would have to be considered. As an example, we have briefly considered advertising legislation in the UK and must now consider the consumer protection legislation available in the UK. This is a considerable subject in itself and as it applies to a BBS home shopping
service in much the same way as any other retail transaction, only a brief overview of the relevant areas will be given.


  These acts imply certain presumptions and conditions into contracts for the sale of goods and supply of services. Goods are presumed to be “owned” by the person selling them, they should match their description and be of a satisfactory quality as well as being fit for a particular purpose where one is specified.


  This legislation prevents a supplier from limiting his liability in certain circumstances and prevents him from imposing certain “unfair” terms on to a consumer. The regulations also provide that contracts should be expressed in plain intelligible language and that where a term is ambiguous, it will be interpreted in favour of the consumer.

- **Consumer Protection Act 1987 and General Product Safety Regulations 1994**

  These cover the situation where the safety of a product is not such as persons are entitled to expect and the product causes damage. Fault is irrelevant and the persons who may be liable include the producer, importers (into the EU) and ultimately suppliers, where they fail to identify the producer or importer.

- **Consumer Credit Act 1974**

  A home shopping service which offers consumer credit or carries out an ancillary business service such as credit brokerage, must comply with the provisions of the Act where the amount of credit does not exceed £15,000. These include obtaining a license. The content of related advertisements is governed by the Consumer Credit (Advertisements) Regulations 1989 and the Consumer Credit (Quotations) Regulations 1990.

- **Financial Services Act 1986**

  This statute regulates the carrying on of “investment business” in the U.K. Investment business means the business of dealing in investments, arranging deals in investments, giving investment advice, managing assets and establishing, operating or winding up collective investment schemes. Authorisation can be obtained either by becoming a member of one of the recognised self regulating organisations, such as, the Securities and Futures Authority or the Investment Management Regulatory Organisation, or by being directly regulated by the Securities and Investments Board.
IV. CONCLUSION

As can be seen from the discussion above, there is clearly great room for confusion concerning liability for the content of information on a European digital superhighway. As regulators, legislators, and courts begin to grapple with these problems, it may be helpful to cut through the confusion by reverting to the cargo shipping metaphor. At each stage of analysis, policy makers will have to re-visit the question of who should rightfully bear the risks and associated costs of information age rules.

In a different day, policy makers decided that a newspaper publisher should have to compensate an author if it unknowingly printed and distributed his work without permission, or if it published defamatory statements. The same policy makers, however, decided not to hold the drivers of delivery trucks to the same standards of liability, and no one seriously suggests that organisations which own and maintain roads should be liable for infringing copies which pass over them. The authors are hopeful that today’s policy-makers will reach an equally reasonable balance when apportioning liability on the Infobahn.