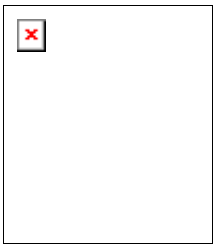

10th BILETA Conference Electronic Communications

March 30th & March 31st, 1995 Business School, University of Strathclyde, Glasgow

Case for Minimal Regulation of Electronic Network Communications

Euan Cameron & Caitriona Hegarty

Keywords: Internet - users - content - nature of use - culture.

Abstract : This paper examines the case for non-regulat of the Internet. Its premise is that the usefulness and flexibility may be damaged if the 'regulationists' have their way. We argue that existing legal controls are as capable for applying within the Internet as elsewhere. Instead it is argued that problems specific to the Internet such as problems of identifying abusers and cross border jurisdiction should be dealt with on a case-by-case basis.

1. Introduction- The Fashion Game

It's a phenomenon - the computer fashion of 1994. It's a revolution - the Computer lawyer's fashion for 1995. It must pose new challenges to the information lawyer in 1996. All sorts of evil will accrue upon It, and within It, if regulation does not keep pace with Its development. Software pirates and pornographers, fraudsters and hackers, virus creators and government spies are but a few of the evil beings lurking if not on the Internet at least somewhere on the global information super highway. It releases vast amounts of information which sits by he roadside just waiting to be accessed.

But hold on; What is "It?" Where is the reality of Its existence and is there any real need to seek regulation? If regulation is to be taken to encompass all legal controls, are there not sufficient in place to govern the complained of activities? Does not the Internet merely replicate non-electronic media of information communication and is there any reason to believe that the laws in question do not equally apply in the electronic media as in other forms of communication. These doubts are emphasised especially by the fact that one area of law after another has succumbed to specialist computer oriented legislation, whether it was necessary or not: computer crime; Copyright and Data Protection to mention just the most obvious examples. In any case are we not in danger of confusing metaphor for reality. The highway may exist in terms of providing the communications infrastructure but the information is not cruising that highway waiting to be picked up. Rather it is waiting at some address (which could either be at home or at an accommodation address) to be accessed. In the end there must be an invitation out onto the highway - an invitation to access - and that invitation needs to be accepted. The information is only on the highway once it is received. Is not the metaphor already being found wanting? The idea of a global web of information is a nice concept but the reality is tied to the actual infrastructure.

The Infrastructure

The Internet as an extra geographical, near instantaneous information zone offers those with access the possibility of browsing, retrieving, accessing, etc. various forms of data. In the mid-'90s perhaps the most valuable raw material is information.

The problem we now face is not how to acquire information, as E-mail has opened the door to a field of opportunity, but how to get rid of information which is no longer essential, mere garbage. Information glut!

Radio, printed media, global television have in the past opened the path to transborder communication. The Internet is an enhancement on past developments. Telecommunications, in whatever format, as a medium is not something inherently demanding of regulation. The Internet as an electronic media has opened up new ways of disseminating information and concluding transactions. As such it poses a threat to the viability of established laws protecting both private and commercial information. So the theory goes.

If it is all a matter of fashion and metaphor, then the history of Information Technology Law shows that we must be most careful in not rushing to quick solutions for perceived dangers. In particular, protective systems are not "natural" rights and there are plenty of lobby groups who would wish to see legal developments which foster their own views. It took the European Directive on Software Protection to even begin to look at the broader issues of balancing issues of monopoly and protection six years after the first "knee jerk" Act in the United Kingdom. There may be issues of

substance which require new legislative interference but they must be carefully identified not just assumed. Difficulties of evidence and procedure must not be confused with issues of substantive law nor should they be allowed to dominate discussion of those issues. For there is much to lose if interference is allowed, in a heavy handed way, to go beyond the absolutely necessary.

Where is the Public Interest ?

There is no natural reason why communication by electronic media should require policing and regulation by national bodies. What needs to be respected is the fundamental right to receive and transmit information which is of value.

Users of the Internet ultimately hold the reins. They either use it or they do not. Every legal limitation in the field of communication can only have a retarding effect on the free marketing environment of the '90s. A balance must be struck which enables those who believe they have something of value to offer to do so whilst at the same time ensuring that all fundamental rights are upheld. How this can be achieved will only come to light once the recent surge of plugging in relents and the dust on the track of the highway settles.

Public interest needs to be protected but the mechanism of regulation may prove to be unnecessarily complex or too fragmentary to prove effective. The issue of what needs to be controlled must be addressed. Is it the use, access or provision of services which needs to be monitored/policed, or is it the resident data waiting for someone to drop in which requires filtration?

Information and Information Technology are interdependent. Without an effective means of electronic communication between users, any potential strategic advantage will be lost. The Internet cannot exist as a valuable entity unless data is freely available to be accessed or used.

2. Some Perspectives from Which to View "The Problem"

May we suggest 4 perspectives from which to view these broad issues; those of 1) the users; 2) the data carried; 3) the nature and use of the highway itself; and 4) the Highway's Culture.

The First Perspective - The Users

There are no doubt many ways in which one could categorise the users. The most basic distinction would be between the (inter-) active and the passive. The latter would appear to raise few issues. To a Software House, the receiver of unauthorised software can be assumed to be a lost sale just as much as the home taper is assumed to be a lost sale to the music copyright owner. Again the Police and prosecuting authorities may feel concern for the receiver of pornographic material but are more likely to have that concern made real by activities away from the keyboard. In any case, the totally passive user is likely to be an unusual presence on any potentially interactive media. The consumer, either for goods or for services or for the joys of participation in the Internet, is likely to feel the need to subscribe to a particular Bulletin Board, or service, or mail list, in order to benefit in even the most passive manner.

This leads to another possible division : between consumers, providers and service providers. The latter phrase is being used to describe those who seek to provide services for the Highway itself. It includes the largest players in the game such as CompuServe and CIX with Microsoft and BT about to break in. There may be issues of monopoly and competition in respect of such players especially if governments become involved but abuses such as riding on the backs of other's copyright present no problems not encountered elsewhere. In particular the compromise contained in the European Directive in respect of decompilation and the use of the fair use defences in United States cases such as Sega v Accolade ((1993) U.S. Court of Appeals) could go some way to preventing the use of incompatibility as a trade weapon.

Consumers and providers come in all shapes and sizes, with many fulfilling both roles. To attempt a categorization of them one needs to also bring in issues of motivation. A linear scale might go from the purely commercial, through barter and the hobbyist motive to the anarchist. It is only with the last named that we reach the character out of control, around whom so much of the hyperbole is centred. The list leaves out the fraudster deliberately. With such a person and such a motive, we are essentially dealing with a distorted commercial motive. The issues are those of security, the potential for detection plus the availability of satisfactory sanctions upon discovery. To this one might add increased opportunity and transborder issues. Security and opportunity seem to be closely linked and it will be suggested that it is for those who wish to use the Internet to provide for the former and to limit the latter. After all, if the global highway proves ill adapted to particular uses, then perhaps one should contemplate not using it at all, rather than risking damage to your correspondents.

Otherwise the provider and the customer in a commercial transaction have the same needs as in any non-electronic transaction which is being mimicked. There may be a need to evolve protocols for establishing the existence of the basic

contractual requirements. But there is no need for these to be government regulated. The providers, or more satisfactorily some representative of groups of providers, can themselves create an appropriate regime.

The Internet service providers may choose to give such protocols and governments may choose to become involved as facilititators but essentially the approach should be consensual rather than imposed. When it comes to questions of proof of transactions then speed and convenience may be different from a conventional transaction, but the need to recognise each other is the same. Additionally, in the end, there must be some physical delivery of any goods involved: We haven't yet the stage of the Star Trek transporter of goods. Services and information delivery are obviously different but, as will be seen, even here an electronic trail will be left to identify the parties involved.

Essentially the same will be true in situations of barter, even in its most intangible form of an exchange of mutually beneficial information. There needs to be some platform upon which such information is made available to others wishing to become involved. Whether it is a Bulletin Board or mailing list or even just some individual's own equipment, the source of information will have a physical presence and what it offers must in some sense be advertised. Certainly steps might be taken to try to disguise the source but the need to contact not only the person with whom one is exchanging, but probably also the service supplier, makes anonymity difficult if not impossible.

The hobbyist in this context may be seen as having some of the characteristics of both the barterer and the anarchist. In as much as he seeks communication and information and has no overtly malicious or criminal motivation (apart, perhaps from those criminalised by section 1 Computer Misuse Act 1990), then he is little different from the barterer of information. He may be thought of as pursuing a more individualistic course in seeking information without necessarily involving the consensual process but, nevertheless, the location of his accessing will be traceable. As with some other hobbies, carelessness and enthusiasm may overwhelm discretion and lead to disasters but it is hard to see how regulation could prevent this without destroying the nature of the Internet. The man who flooded his correspondents' e-mail boxes by accidentally sending much larger files than he had intended, at least taught us of the need to seek technical solutions to avoid such future occurrences. The self satisfied enforcers of "netiquette" who choose to "mail-bomb" the naive who infringe their code, may be smug but they are essentially harmless.

The anarchist seeks to cause as much disturbance and chaos as he possibly can, often in the mistaken belief that he can surf with anonymity. Posting e-mail intended to insult and provoke is second nature to this particular user. Individuals and newsgroups are both targets of attack. He may post bait with the intention of triggering a flame war. At best no-one will bite, but it may flare up in a flame war. Even with encryption a trail will be left.

The Second Perspective - The Information

As the resource of the '90s information does not comply with the rules that apply to other natural resources. It can be used by more than one user at any given time. It can be reused without being recycled. The use to which information may be put, if at all, is not readily determinable at the point of access. The value that information generates often depends on the user. Its value may be increased by a reduction in the amount of raw data and an increase in the information being made available through filtering and additional checking. Using the Internet is no different to using a telephone directory. The World Wide Web (WWW) provides the user with a sample of raw data which by user selection may be turned into valuable information. The Web can be reused if necessary for various reasons. Each search will have a different value.

The application of information has inherent qualities. It may be used to gain a competitive edge over rivals. It is a commercial asset but its effectiveness can never be priced. It may fade with time as much information has a limited lifespan. What is vital information today may be of secondary importance tomorrow.

The amount of data out there is staggering. The technical potential for increase in the quantity of that data is incomprehensible. As computing power multiplies and more and more of the world's PCs are equipped for electronic communication, the possibilities seem limitless. Yet there is a degree of illusion too in such a picture: in some senses data actually loses its potency with quantity. It is only when data is extracted in an organized manner or that it is applied to a particular problem that it turns into something useful and/or dangerous. In other words, it is again necessary to access in order to raise the real as opposed to the potential dangers and abuses. This must apply equally to the provider/holder of data as to the consumer of information. In as much as the provider/holder is motivated by the desire that his data finds a useful home amongst the consumers and barterers then, whether that motive is commercial, the interchange of ideas, or even anarchistic, there needs to be a point of access. The acquisition of such access is not only a technical question but also a matter of linguistics and comprehensibility. It is our contention that the very nature of the global highway is such that one can only be concerned with data at the stage at which it is reduced to used information. Some of the technical difficulties can be eased by the development of browsing and organization al tools but to meet like-minded people, or information of use, both sides must advertise their existence. The metaphor is the "Infobahn" but unused trains are of no use to anyone even if they are free of cost. A sliding scale in respect of data might go from that which is extracted and used, to that which is merely available and which is effectively garbled because it is lost in the vast quantity of what is available.

The point is that those asserting their rights or seeking to detect wrongs have "merely" to search for those points of access which the holder/provider must make available when seeking interaction. Should we really concern ourselves with data which is available but garbled and therefore has the mere potential to become information? Is it not just the nature of the beast?

The Third Perspective-The Nature and Use of the Internet

Historically it has been possible to identify two models for networks: open and closed. In the former, the prevalent need is for communication with all comers. The culture is that of the Internet. The desire is access for all who might legitimately seek it. In the latter, the culture is that of strictly limited access for equally restricted purposes. Such systems will tend to have complex protocols and security systems designed to enforce those access limitations. Of course, such a dichotomy is a theoretical model which may never have entirely existed. There are examples of systems which act as a closed system, at least as far as consumers are concerned. The obvious examples are the Banks' ATM systems. Often, however, the distinction is more blurred. The same machines will be used for both external and internal networks so that the fence between the open and closed system will merely be passwords and other methods of controlling access. And often there will be gateways through which the outsider with appropriate permission can pass. The fear, of course, is that gatecrashers can also pass through.

In as much as we are again playing with metaphors, then there is already a conflict between the Internet - open - culture and the internal - closed - network. That conflict becomes more intense when those who have traditionally used closed systems wish to switch their operations to the super highway. The incentive for commercial organizationto do so is obvious. There are simply more potential customers out there on the Net than will sign up to an entirely closed system. The fact that the customer can communicate from home or business magnifies that opportunity. And, of course, the benefits are far from one way. The consumer will come to relish the freedom from the apparently restrictive nature of the closed system.

There is a price for the provider to pay. The freedom to communicate by roving the highway does make control more difficult. Security may be theoretically the same in that, one must guard the point of access and ensure that internal security beyond that point of access is sound, but it would be foolish to pretend that the risks of unauthorised access are not made greater by the greater openness between the internal network and cyberspace. The question is: who should bear the burden of the extra risk? It is submitted that, when it comes to those who switch from closed systems to the highway, it must be they who take on responsibility. It is unreasonable to expect the service providers to monitor the quantity of traffic involved - although British Telecom recently suggested that they might try - while those who are merely acting as consumers may not appreciate that a balanced decision has been taken in which the risks of an open system have been accepted over the security of a closed system. Of course, the decision may not have been balanced. If the risks are worth accepting commercially then the costs of security and insurance should equally be justified. It is reasonable to expect those switching cultures to bring the security culture of closed systems with them. If that is not possible, they should think twice about the suitability of the highway for their services. It is always tempting to make use of new or enhanced technologies but is it so heretical to suggest that, if there is incompatibility of cultures, the potential user must either accept the consequences of that incompatibility or not use the open system all?

The Fourth Perspective - The Culture of Openness

If consumers stand the risk of finding that commercial providers are making use of facilities that are ill-adapted to the type of transaction for which it is being used, then Internet users may also find restrictions on their assumed rights. Freedom of expression by one user may cause insult or visual injury to another. That is the price of openness. We can either fight for the right to transmit and receive all freely accessible data and face censorship, or try to avoid the problem by standardization as an effective means of self censorship. The user has the ultimate control. There are practical and moral reasons for censorship which do not apply only to electronic communications. In so far as the multi functional Internet is akin to a telephone network, the issue needs to be addressed of whether criminal or perceived anti-social activity must lead to a judicial power to intercept this form of communication to the same extent as telephone conversations. At present, cyber-cops are an invisible presence on the Internet. Anonymity is the best policy as far as resourcing is concerned. If it is not an offence to purchase pornographic material at the newsagents, should it be an offence to make such material available on the Internet. Lets not get cyber-moralistic! The 1994 Criminal Justice Act has widened the definition of publication in the Obscene Publications Act to cover computer transmissions (s.168(1) Sched 9 par 3.) this should be sufficient to police the Net. Child pornographers may by forced into the cyber-underworld but they will not escape detection even if they use encryption. Most criminals leave a trail. Those using the Internet are no different. They may use sophisticated encryption techniques but that in itself involves skill and may be used incorrectly. Anonymity is virtually not reality. There is a need for international co-operation as the Net does not recognise national boundaries. Any fears of a "right-to-tap" need to be averted. Users are not untouchable by and large; they will be able to keep their freedom within the existing law.

3. The Scale of the Danger

Against such perspectives it is submitted that the problems which exist are not those of substantive law but rather are problems of procedure and evidence and sheer quantity. However, the analysis above may suggest that problems of procedure and evidence may be less severe than first thought, while the difficulties of quantity are seen to be either likewise reduced or inevitable and to be accepted and taken into account. The reduction would be by the application of the adage that 'quality is more important than quantity', while it is suggested that regulation is incapable of correcting the problems arising from a surfeit of information.

Substantive Law

So are there substantive legal principles which are unable to cope with the Internet regime? Let us take copyright as an example. The fear is the widespread dissemination of unauthorised copies of works whether they be standard literary or artistic work etc., or the seemingly more apposite software copyrights which in this context are really no different. The type of infringement we are dealing with is that of the most basic variety - we are talking of literal copying. The processes by which the Internet's functions are fulfilled - electronically displaying information, downloading and uploading - are all going to be caught by the sort of extended definition of copying contained in legislation such as the UK's Copyright, Designs and Patents Act 1988 or the European Directive on Software Protection of 1991. Such provisions extended the definition of copying to include temporary storage in the computers temporary memory, the object being to ensure that permission is required in order to make use of computer programmes. However a side effect of that desire is to effectively cover almost all activities within a network as they usually involve taking a temporary copy to the local workstation. Only if the workstation is being used as a dumb terminal would one have a situation where, arguably, no additional copy was made. Such passive viewing may be perceived as harm by the owner but, in as much as the usage is not authorised, there must be a copy held somewhere, either at a local fileserver or a remote site providing services, such as a Bulletin Board or a Gopher. To the extent that harm is done, not so much by any individual copy as by the presence of an authorised copy in a place from which it can be accessed, then provisions dealing with indirect infringement can be made to apply e.g. authorising infringement. Of course, once the offending item has been downloaded the more subtle forms of infringement might occur - translation, adaption, incorporation in another work: in particular, in relation to a programme, it may be decompiled and then included in a new and rival product. However the salient features still exist:

- there has been an unauthorised literal copy created by downloading as an intermediate stage in the creation of the rival product;
- the problem is one of proving derivation just as it is in any other type of work;
- there are debates as to what degree of derivation or incorporation is permissible without breaching the copyright, but that debate exists irrespective of the process by which the unauthorised copy is created;
- the harm is only clearly in existence when the rival product makes itself known e.g. when it is brought onto the market.
- At that stage the "victim" can begin the normal processes of proving infringement. If those processes of proof include such swift procedures as, in this country, the Anton Piller order, then it is submitted that this is as much as any right owner can expect. A plea to be able to interfere in anticipation that some non-specified harm might occur at some future time, is fraught with dangers of stifling competition. Indeed far too often it seems as if the Anton Piller order, when not being used to police exact literal copies being illegally sold (e.g. piracy), is used for just such an undesirable purpose (see ZS Associates v Nosis - Unreported, 1994)
- The same four salient features could also be identified in the other obvious example of infringement which would involve derived works: the inclusion in a multimedia work of works, or parts of works, copied without authority via the Internet. Again, the problem is one of scale: there is already a problem from the voracious appetite of, for example, a hypertext system for information. The temptation to match that technology to the vast amount of material available on the Internet may prove too much for some. But of course this is simply infringement, it raises no copyright issue. Admittedly there may be additional issues to be raised as to how much can be taken of any one work without it amounting to a "substantial taking", but these are simply the problems which already exist in compiling a hypertext system. There may also be problems with works which are licensed to be on the Internet. To what extent does the author who is permitting the dissemination of his work via the Internet and its downloading thereby permit its use in derivative works? Again, such issues arise in respect of traditional works of reference.
- Indeed, the pressure is not so much that there may be activities which are not caught by current rules as to infringement but, rather, that the current regime is too restrictive; that the need for permissions stifles the use of the technology's potential. Already in respect of Hypertext products this can be a problem. But equally, it is a problem with all large databases which seek to be authoritative. Computer capacities have lead us to debate such issues with or without the Internet. The global highway brings problems of enforcement not of substantive law. It may bring the need to evolve new strategies for exploitation. As the Internet dilutes the value of some types of work because of the availability of large quantities of rivals (the fate of academic articles for example?) then the means of exploitation may need to change. Just as the existence of libraries led to pressure for collective rights, so might the existence of Internet "libraries". But the significant point is, that this can be left to the rights owners acting under the pressure of increased competition and taking advantage of the opportunities provided by the infrastructure.

- Similar points could be made in respect of other aspects of substantive law alleged to be under threat from the Internet. In respect of crime, there is no more doubt that material distributed on the Internet is pornographic than there is for material distributed by any other medium. The problem of defining pornography is certainly not Internet specific. Likewise, in respect of viruses and criminal damage, crimes which have been developed to cope with interference with individual computers and internal networks are just as capable of dealing with the same problem on the Internet. Again, if one thinks of issues of Data Protection, then there can be little doubt that allowing personal data out onto the information highway would be in breach of one's data protection obligations. In particular, most systems have restrictions on transborder flows of data. Also, the various Data Protection Acts tend to provide quite a good model for communication in that the onus for security is placed on the holder of personal information who is required to achieve reasonable levels of security for such data.
- **Procedure and Evidence**
- Wherever one looks, the problem is seen to lie, not with the scope of the substantive law, but rather with the fear that it can be enforced. The feared difficulties are those of evidence and procedure. However, the earlier analysis suggested that those difficulties are exaggerated. Situations where the greatest harm can be done are situations where it is possible to trace the machine from which the harm is being done. Further, anyone who wishes to take advantage of the interactive possibilities of the Network will leave evidence of their locale. Thus, it is primarily a question of the will to detect the wrongdoer. Once Sega became aware of the Maphia Bulletin Board, then it was a relatively easy matter to gather evidence that its games were being exchanged via that Board (see Sega v Maphia (1994) F.Supp 670). Nor was there any real problem with the substantive law and the procedures to seize evidence via the Californian equivalent of our Anton Piller was perfectly satisfactory. Likewise the leading U.S. case on viruses actually involved the release of a "worm" onto the Internet that proved traceable to its origin. (U.S. v Morris (1991) 928 F 2d 504)
- Of course, it would be naive to assume that that would always be possible. But if the perpetrator has sufficiently covered his trail, it is hard to imagine what regulation could do about it. More relevant may be the difficulty of knowing who is behind the machine which is traced and whether civil and criminal responsibility can be imposed on the owner. It may seem reasonable to assume that the owner should take responsibility for security, but when one thinks of the computer laboratories of a large educational institution, one begins to wonder. However, at least those controlling Bulletin Boards and gophers, and those wishing to make commercial use of the Internet, will identify themselves.
- **Regulatory Structures**
- **Case For Regulation**
- The nature of information technology does not necessitate special consideration of a regulatory infrastructure. We believe that the tenor of the arguments thus far raised lead to a conclusion that only minimal regulation is required. Advocates of regulation perceive certain needs for and advantages in its implementation:
- to produce safeguards which reduce the risk to computerised information systems. Public authorities will only show cursory interest if there is no damage limitation;
- to encourage the creation of open information systems with a guarantee of security and protection. Legitimate access to information and browsing of information is permissible and desirable. Regulation can ensure increased openness compared with traditional data handling;
- to secure an open system with reduced risks will encourage enhanced use and extend the capabilities of that system; and
- without it technology will continue to run ahead of appropriate regulation if, and for so long as, those in a position to influence change allow it to do so. Electronic communication has opened another gateway to transborder commercial, economic, political and social relations. The culture of the '90s is one of on-line communication. Its development runs the risk of running out of control unless, and until, a global perspective is formulated and adopted.
- Internet growth in the US has now started to settle, whilst in Europe it is still in its infancy. The opportunity to curtail such an unruly beast must be seized. It is argued that the question is not what action is appropriate, but who should take the initiative.
- **The Case for Minimal Regulation - Cultural**
- Regulation may be a solution. However, communication law has traditionally distinguished between the service provider and the facility user. In the context of the Internet it may prove difficult, and probably ineffective, to continue to base regulation solely on the clearly defined roles of the user and the service provider/information facilitator.
- If the right to communicate and transfer information across borders is to be upheld, the regime must be defined fairly liberally. Regulation should be kept to a minimum: sufficient only to meet the needs of security and protect privacy. Information flow should be unrestricted to the fullest extent consistent with legitimate privacy concerns. Fears in the early days of the data protection debate, that advances in technology would place individual privacy at risk by permitting unhindered flow and use of personal data, have proved unfounded. Abuses have proved to be limited. Self-regulation, coupled with legal controls, are an effective mechanism. The benefits of the transmission of personal data to the data subject have been duly recognised. If unwarranted restrictions are placed on the collection or use of such data, individuals could be denied some or all of the advantages which they have come to expect in the age of communication, where information is perceived as an essential ingredient.
- **The Case for Minimal Regulation - Practical**

- Regulation of the Internet may prove to be unnecessarily complex and even fragmented. To be effective the model must accommodate further advances in technology and account for the impending deregulation of cable services across Europe, which could result in significant price cuts in global connectivity. The Net in its present format is not a commercial infobahn. The backbone of the Net in the US, NSF Net, has been funded by the US government. But not for much longer, it would seem. The character of the Internet is evolving. Netiquette, which has sought to restrain commercial postings outside the .biz hierarchy, is due to change in 1995. The Net shows all the signs of becoming yet another commercial vehicle. The driving force is not the user who cruises the highway rather it is the vision of the service providers. Netiquette policing of blatant advertising, the ultimate evil of the on-line culture, is due to become a thing of the past. WWW is the perfect candidate to spur commercialization of the Net. Microsoft Network '95, or will it be '96, could have a serious impact on the future if the dream of direct selling comes to fruition. The US Justice Department has already expressed concern. CompuServe has in excess of 2.5 million members (90,000 in UK). It currently provides 2,000 services ranging from software and hardware support for some 700 companies, news, sport and travel information and share price information for some of the leading markets. The potential for commercialization can no longer be ignored. The consumer may be attracted by the capacity to interact rather than be the passive recipient of broadcast advertisements in the global village. Cyber-selling and Cyber-licensing are just around the corner. As the pressure for such use grows then the pressure to evolve standards also grows. However, the nature of the Net is such that those commercial pressures can be relied upon to create those standards.
- If the service of the public interest remains the cornerstone of validity of regulation, it can only be effective if it is kept flexible and unobtrusive to the user. Clear policy objectives must be set which may realistically be adhered to. If standards are set they must be achievable.
- **Telecommunications as a Model for Standards Setting within a System of Minimal Regulation**
- Telecommunications in the UK has already gone through the process of de-regulation resulting in greater choice and flexibility. Is the Internet really that different? Enthusiasm for regulation must be tempered by a consideration of the use to which services may be put and why the Net is perceived as being novel. The attractions include choice and availability of national or supranational services. It enables access to a diversity of opinions and views on virtually any conceivable issue, current or historic which may be explored from a cyberchair or cyber-cafe. As it evolves, it must be commercially viable to remain attractive to the non-academic user.
- Standardization in the telecommunication industry has helped insure against monopolization. Its implementation has been important for governments as a means of monitoring trade and industry internationally and, from the users point of view, in providing guarantees. There has been a relative degree of formal standardization of the Internet. HTML (which is the standard language WWW uses for creation and recognition of hypermedia documents), HTTP and URL's, have become standard on WWW, which is currently the most popular client-server model. Like the OSI model, they stipulate how data, in various forms (words, sounds, graphics) should look within the network. We are now at the stage where further standardization is necessary, not only because of rapid growth, but to ensure the marketability of further developments. No technology will succeed in a mix-and-match world of webbing unless governed by acceptable standards.
- We can assume that there are such commercial pressures on the system which will force standardization . The first half of the '90s has seen an unprecedented interest in the Internet. The Internet is currently popular because the information and services provided are free and it is interactive. It is by common consent considered to be difficult to access, slow, and expensive. Its major rival is the alternative information superhighway cable. If the attraction of the Internet is to be maintained, competition must be met.
- The Internet does not need to be a unified network to survive. It can continue to develop in a piecemeal fashion, put together by a variety of companies with varying interest, so long as the methods of interconnection and communication protocols are standardized. In the not so distant future cable operators will be offering fully interactive services which have the potential to provide what other technologies have failed to do. Cable poses a threat to the Internet which can only be met with standardization.
- **Conclusion**
- The public must be encouraged to embrace change and welcome experimentation. This can only work if there is a regulatory framework flexible enough to allow it to happen and resilient enough to cope with consolidation and even failure. Commercial detail may determine the future of the world's communication system but should not cramp its current growth. The Internet is a flexible body but, at some point in the not so distant future, all the investment will have to be seen to pay.