EURIM Briefing No 19

July 1997

In the area of ICT (Information and Communications Technologies) EURIM is a link between Commerce and Industry, Parliamentarians, Whitehall and Brussels

The Regulation of Content on the Internet

Introduction

The Internet is a primary enabler of electronic commerce and other social and commercial benefits, but there is pressure on politicians in most EU states to prevent the dissemination, via the Internet, of illegal content, particularly child pornography. Only a small proportion of the vast content on the Internet is believed to be either illegal or harmful, but the threat to Society is commonly felt to be sufficient to justify the imposition of controls on content. However, care must be taken to ensure that approaches to this problem give people confidence to develop and use the Internet and do not jeopardise legitimate trade.

The Internet is internationally dispersed and it is not realistic, and possibly not desirable, to try to exercise control over content at the point of origination. Control can be applied, however, at the point of access. Efforts can also be made to trace *illegal* content to its source and to its customers. Considerable work has been done by the Commission to identify the issues and propose broad solutions. But priorities have not yet been identified nor have co-operative programmes of content control been put in place.

The problem in most countries is less one of new legislation than of the identification of illegal or harmful content and enforcement of existing laws within Member States and issues of jurisdiction between them, without discouraging use of the Internet for legitimate purposes. Some Member States have nascent trade bodies or the beginnings of voluntary regulatory regimes. Technical solutions which could allow effective control over content at point of access are not yet fully effective or universally available.

Recommendations

EURIM believes that:

- The most practical approach is to develop a pan-European (leading to a global) regime of self-regulation based on co-operation and subsidiarity within the context of a unitary regime for all audio-visual and multimedia content. In particular, financial and organisational support should be given to projects akin to that proposed by the INCORE partnership.
- The UK model of an industry funded self-regulatory body such as the Internet Watch Foundation (IWF) could provide a way forward provided it is given support, resources and legal status akin to those of the Independent Committee for the Supervision of Telephone Information Services (ICSTIS) which addresses a similar problem area, but on a different telecommunication medium.
- Further study into the future relationship between ICSTIS and the IWF is indicated, perhaps in the context of a clearer, wider role for the ITC in content regulation.
- Vigorous encouragement should be given to the development of products and services which allow effective control of content at the point of access so that the promotion of Internet access by children for educational purposes can continue without significant risk of abuse.
- Education of end users about the law and on steps they can take to control access to certain types of material is a vital element of any control mechanism.
- There is a need to clarify existing law relating to the responsibility for generating, disseminating and exploiting illegal material to protect the position of those who, despite reasonable precautions, unwittingly convey, process or provide access to such material.
- The liability for illegal content should rest with those who create it and make use of it, not with those who (unwittingly and despite reasonable precaution) transport, process or enable access to it.
- Priority should be given to the funding, training and co-ordination of law

enforcement resources deployed against illegal content.

Illegal and Harmful Content

1. On 27th September 1996, the EU Telecommunications Council adopted a resolution on preventing the dissemination of illegal content on the Internet. In response the Commission (DGX) produced a communication which, along with the DGXIII Green Paper on the Protection of Minors covers most of the issues (See Appendix A for Communication and Website references and Appendix B for the DGX Communication).

2. The vast majority of Internet content consists of information for legitimate business or private usage. There is no evidence that mis-use is statistically significant but there is strong political pressure for action in view of the growth of the Internet as a powerful influence in social, educational and cultural fields .

3. The areas of mis-use are covered by different legal regimes and instruments at the national and international level, e.g.:

- national security (instructions on bomb-making, - illegal drug production, terrorist activities);
- protection of minors (abusive forms of marketing, violence, pornography);
- protection of human dignity (incitement to racial hatred or racial discrimination);
- economic security (fraud, instructions on pirating credit cards);
- information security (malicious hacking);
- protection of privacy (unauthorised communication of personal data, electronic harassment);
- protection of reputation (libel, unlawful comparative advertising);
- intellectual property (unauthorised distribution of copyrighted works, e.g. software or music)

4. It is important to strike the right balance between ensuring the free flow of information and meeting justified concerns with regard to abuse. There is also a need to consider the legal liability of those who unwittingly convey, or enable access to, illegal or harmful material. Appendix C covers the current, Internet-specific law. Appendix D summarises the case for complete freedom of expression on the Internet.

5. It is clearly the responsibility of Member States to ensure the application of existing laws with regard to the distribution of illegal content. **What is illegal off-line remains illegal on-line**. But, given the highly decentralised and trans-national nature of the Internet, measures to reinforce co-operation between Member States are also required. For example, there is already an international Accord on protecting the rights of children, illustrating the potential for incorporating complex, global issues within national laws, both within and outside the EU. Action is in hand in many countries to control content in ways which conform to local susceptibilities. Appendix E covers some of these.

6. The presence of illegal and harmful content on the Internet encourages attempts to regulate at the national level. The regulation of new Internet services by individual Member States, with the aim of preventing abuse, may create distortions of competition, hamper the free circulation of services, and lead to a re-fragmentation of the Internal Market. This prospect is sufficiently likely to justify Community intervention not only to pre-empt unco-ordinated regulatory action by Member States, but also to create the legal and regulatory stability which is a prerequisite for industry growth. Experience in other fields suggests, however, that it is important to avoid over-legislation. It might be more productive to begin by identifying the basic consumer principles before defining detailed procedures.

Points for Consideration

The main points for consideration by local and regional legislators are:

The application of existing law

The Internet does not exist in a legal vacuum. All those involved (authors, content providers, host service providers who actually store the documents and make them available, network operators, access providers and end users) are subject to their respective national laws. Those who unwittingly and despite reasonable precaution convey illegal material should have their position under the law clarified beyond reasonable doubt. The issue is one of clarification of existing law and of enforcement, not of new legislation.

Illegal content

It is crucial to differentiate between content which is illegal and other harmful content. These different categories pose radically different issues of principle and call for very different legal and technological responses. Priority must be given to the application of resources to combat criminal content - such as clamping down on child pornography or on use of the Internet as a new technology for criminals. However, the task is not easy, because the definition of what constitutes an offence varies from country to country. Moreover, where certain acts are punishable under the criminal law of one Member State, but not in another, practical difficulties of enforcing the law may arise.

Harmful content

Various types of material may offend the values and feelings of other persons (e.g. content expressing political opinions, religious beliefs or views on racial matters). What is considered harmful depends in part on cultural differences and nations differ on what is permissible or not permissible. International initiatives must take such differences into account when exploring co-operation to protect against offensive material whilst ensuring freedom of expression. (For limitations in EU Member States, see Green Paper on the Protection of Minors and Human Dignity in Audio-visual and Information Services, Annex III).

Detection of breaches of the law

While detecting breaches of the law in public applications of the Internet (e.g. the WWW) is straightforward, detection is not easy in private applications (e.g. e-mail). Similarly, while enforcement of the law is relatively easy within national boundaries, it is much more difficult in an international context. There are technical problems which mean that control is most practical at the entry and exit points to the Network (the terminal used to read or download the information plus the server through which the user gains access to the Internet and the server on which the document is published). Thus international co-operation is required to avoid "safe havens" for content that is generally agreed to be illegal.

Chain of responsibility

Internet Service Providers play a key role in giving users access to Internet content. It should not however be forgotten that the prime responsibility for content lies with authors and content providers. It is therefore essential to identify accurately the chain of responsibilities in order to place the liability for illegal content on those who create it. The widespread use of filtering devices at points of access should act as a powerful incentive to content providers to "rate" their content. The structure of the industry is covered in Appendix F.

Trade Bodies and Regulatory Models

In the United Kingdom, a Code of Conduct (Appendix G) has been developed and agreed within the trade association body (Internet Service Providers Association - ISPA), with the support of the Department of Trade and Industry. But ISPA membership does not cover all major providers and although the Code is mandatory for members, the range of sanctions is limited. ISPA needs enhanced government support and encouragement if it is to achieve recognition as the authoritative voice of the industry.

However, the primary issue is not how the industry itself is organised, but whether regulation of content on the Internet should be voluntary (i.e. self-regulation within existing law) or imposed (by the State or by some other recognised authority), and how such a regulatory regime should relate to the industry. Appendix H is a summary of regulatory regimes in the UK and the options for content regulation on the Internet.

In a number of Member States, information service providers have already set up systems of self-regulation: indeed, the Commission welcomes this general movement and is encouraging a European network of associations of ISPs. INCORE (Internet Content Rating for Europe), a loose association of industry, government, police and user interests, is evidence of the sort of co-operation which could further be extended to the wider international level, but it lacks formal recognition and public funding. The UK Government supports INCORE but is not itself a partner in the project. Industry self regulating bodies, which face common problems, could usefully co-ordinate their approach, in particular regarding technical solutions.

In the UK, the voluntary regulatory body is the Internet Watch Foundation (IWF) which is funded by a number of providers and has parallels with ICSTIS. The IWF is not independent from the providers (as is ICSTIS from the Premium Rate Telephone Service industry) and lacks the credibility and influence which formal recognition and legal status could give. The IWF is an attempt at voluntary regulation and deserves to be afforded recognition and status similar to that of ICSTIS. The ICSTIS model is at Appendix I. It is beyond the remit of this paper to consider whether ICSTIS and the IWF should exist as separate bodies in future, or, indeed, whether their natural home might be within a restructured ITC (as suggested in EURIM Briefing 13).

Suitably strengthened, the ISPA-IWF model is one which other countries could be encouraged to adopt as the foundation for a network of international regulatory regimes, offering co-operation between the authorities and providers to ensure that control measures are effective and not excessive.

Methodology and Technology

The concept of tagging classification codes to material is described in the DGX Communication (Appendix B) and in detail in the Safety-Net Foundation proposals (Appendix J). The issues associated with the

universal application of codes such as PICS include how content classifications are to be defined and applied.
International co-operation is required if such problems are to be overcome.

Convergence Issues
Whatever action is taken to regulate content on the Internet, the convergence of media and means of presentation will require a convergence of regulatory regimes. The control of audio-visual content on TV, for example, should be compatible with that of content on the Internet if the regimes are to be even-handed.

Related issues, which although critical in their own right, are not central to this study, include IPR, Security and Data Protection. They are summarised at Appendix K.

Schedule of Appendices

A. *Summary of Website addresses.* A useful source of quick reference to the key locations dealing with the subject.

B. *DGX Communication.* This is the key document, a study of which will provide the reader with most of the underlying arguments relating to policy.

C. *Summary of existing, Internet-specific UK law.* The summary does not cover common law provisions as it might affect the Internet. It focuses on the law as it is developing specifically for the Internet.

D. *Summary of Conflicting Views.* This study has not confined itself to a consideration of the arguments in favour of some form of control of content. There are opposing, usually libertarian, views, which are summarised here

E. *International Activity.* The Internet is not a national phenomenon and any changes in national legislation aimed at improving control of content must be harmonised, so far as is possible, with similar activity elsewhere. This Appendix summarises the major international activities

F. *ISP Industry Structure.* A (possibly over-simplistic, but nevertheless useful) portrayal of the key elements in the chain from content provider, through service provider, network operator, local loop operator, down to the end user.

G. *ISPA Code of Practice.* Not all service providers are members of ISPA, but this Code is a major advance.

H. *Summary of Content Regulation in the UK and Options for the Internet.* A succinct description of current models and processes

I. *The ICSTIS Model.* A fuller description of how ICSTIS is organised and operates, included because of its possible relevance to the way that the IWF might develop.

J. *The Safety-Net Foundation R3 paper*. An industry proposal for addressing, in the UK, the question of illegal material on the Internet, with particular reference to child pornography.

K. *Related Issues.* A summary of important issues (such as IPR and Security) which have a bearing on any discussion of content regulation on the Internet.

These Appendices are on the EURIM website at: http://www.eurim.org/.