

**GOVERNANCE OF
CONTROVERSIAL INTERNET
CONTENT IN THE EUROPEAN
UNION.**

Daniel Dunne.

Minor Dissertation.

Presented in partial
fulfilment of the requirements for the degree of
Master of Arts in European Studies,
University College Dublin, 1997.

Abstract

This dissertation aims to examine EU policy developments in the area of controversial Internet content, with a view to assessing the instrumental capacity of the Union as a putative state in this context, and the implications of the Internet's infrastructure on governance in general. This technical infrastructure and the institutional framework of the Union both set parameters in which any policy must emerge. The institutional framework clearly embeds policy within liberal democratic norms, and also, as regards criminal content, in the intergovernmental structures of Justice and Home Affairs co-operation. Economic interests also impinge on the policy process. The infrastructure of the Internet renders comparisons with traditional media difficult. Volume of data, packet switching, indeterminate terrain and encryption supported anonymity make traditional regulation, allocation of liability and enforcement of policy highly problematic.

Emerging policy on illegal content concentrates on the encouragement of self regulation, while failing to reach a final position on liability. However, the challenges of indeterminate terrain and encryption are not fully faced. The author argues that any sub-global approach to illegal content faces severe and inevitable limits.

A more feasible policy emerges in response to the problem of 'harmful content', that is, the protection of minors from adult content. The Union's support for the Platform for Internet Content Selection (PICS) entails the promotion of a technical protocol as a global standard, in close co-operation with industry. Yet serious obstacles remain to be bridged if such a protocol is to succeed.

European policy on Internet content conforms to the 'Network Governance Paradigm' whereby the traditional regulatory role of the state is circumscribed and new policy instruments invoked. Such instruments include the promotion of technical standards and the encouragement of self regulation. Global level governance, however, is the best hope for adequate public control of Internet content.

Table of Contents:

LIST OF TABLES.....	IV
1 INTRODUCTION.....	1
AIMS	1
STATEMENT OF ORIGINALITY	2
LITERATURE REVIEW	3
METHODOLOGY.....	9
2 DEFINING THE INTERNET AS A MEDIUM.....	11
WHAT IS THE INTERNET?.....	11
CONFLICTING METAPHORS.....	14
LIABILITY.....	16
TECHNICAL INFRASTRUCTURE	18
3 POLITICAL AND CONSTITUTIONAL CONTEXTS	22
THE EUROPEAN UNION, INTERESTS AND COMMUNICATION	22
CONSTITUTIONAL CONTEXTS : EUROPEAN CONVENTION ON HUMAN RIGHTS	26
JUSTICE AND HOME AFFAIRS IN THE TREATY OF EUROPEAN UNION	28
PROXIMATE POLITICAL CONTEXT	30
4 THE DEVELOPING POLICY CONSENSUS.....	32
DEFINING CATEGORIES OF CONTENT.....	32
THE POLICY-MAKING PROCESS	35
EMERGENT SUBSTANTIVE POLICY.....	38
SELF REGULATION, LIABILITY AND INTERMEDIARIES	41
TERRITORY AND ENCRYPTION.....	42
5 PROTECTING MINORS FROM ADULT CONTENT.....	44
THE EXTENT OF PORNOGRAPHY ONLINE.....	45
FILTERING SOFTWARE.....	46
THE LIMITS OF BLACKLISTING	47
PICS: NEUTRAL LABELLING	49
RULES AND STANDARDS.....	51
SHORTCOMINGS OF PICS	53
IMPLEMENTATION	55
6 CONCLUSION: GOVERNANCE IN A GLOBAL INFORMATION INFRASTRUCTURE ..	57
THE NETWORK GOVERNANCE PARADIGM.....	57
TECHNICAL STANDARDISATION AS POLICY INSTRUMENT	58
CO-OPERATION BEYOND EUROPE	61
THE CHALLENGE OF THE GLOBAL - A SPECULATION ABOUT STATEHOOD	64
REFERENCES.....	67

List of Tables

5.1	The Levels and Categories of the RSACi rating system.	Page	51
-----	---	------	----

1 Introduction

Aims

The aim of this dissertation is to critically evaluate policy initiatives of the European Union in the area of controversial Internet content. I have chosen to use the general term ‘controversial’ in the interests of scholarly detachment, especially in cases where there is a lack of consensus on the particular type of material. These policy initiatives will be studied with a view to assessing the instrumental capacity of public power to govern communication in the new medium. What implications, it is asked, does the new communicative infrastructure have on governance in Europe? How are the actions of the liberal democratic state delimited in this context, including the European Union as a putative state or ‘part-formed polity’?

For the European Union the potential obstacles to this capacity are both political and technical. Politically, a common approach must be found in a context of diversity in national legal and moral cultures, and in the context of the justice co-operation parameters of the Union Treaty. Technically, the infrastructure of the Internet poses

huge challenges for the enforcement of policy. Moreover, difficulties in applying existing norms to the Internet raise issues such as appropriate allocation of liability. These two limiting factors will be examined in detail with a view to assessing the degree of limitation placed on liberal democratic governance in this area. In this light, the prospect for the development of substantial policy instruments is addressed. At the outset it is worth noting that the technical and political issues are intimately interconnected. It is the transnational nature of the Internet that creates the rationale for a transposition of this policy arena from the national to the European level.

Statement of Originality

European Union initiatives in the area of controversial Internet content are a recent phenomenon. They have as yet received little academic scrutiny, save brief accounts in the work of Yaman Akdeniz (1996,1997). This will be the first serious appraisal so far as this writer is aware. Furthermore, scholarly inquiry generally on the ramifications of the Internet on the policies of nation states and on international institutions is in its infancy. This is hardly surprising given that the Internet as we know it is itself such a recent development. Studies are most developed in the US context which one could call the core of the Internet, being the origin of the Internet's 'architecture' and where half of those connected reside. However, the rate of the Internet's expansion and its revolutionary nature as a medium mean, in my view, that this is an important area for research. The fact that the Internet is a precursor to an incipient 'information super highway' brings even greater significance to these inquiries (Saxby 1990, 1996; Gates, 1996). The ultimate development of such a broadband network - allowing high quality video on demand- could see the eclipse of television, rendering the Internet as *the* medium of the twenty first century. I have decided not to focus ethical issues, not only for reasons of space, but also because regulation of controversial content on the Internet raises the same ethical dilemmas and well-rehearsed lines of argument as does controversial content in more traditional media. The practical questions of governance

in the new context, however, raise new issues, and present researchers and politicians alike with a steep learning curve. It is hoped that this present work will be a useful contribution in an embryonic area of research.

Literature Review

There is a vast array of literature available on subjects relevant to this dissertation, much of it in the form of online documents. However a relatively small amount of this is of a serious scholarly nature, and rarely transcends the polemical. Some of the more cogent contributions of this type, which focus on discrete areas of policy, will be critically evaluated in the main chapters of this study when the pertinent issues arise. The present review will focus on scholarship which offers general theoretical accounts of direct relevance to this research.

Authors in the legal field have produced by far the most considered reflections on Internet content regulation, and regulation in general. A new discipline of 'cyberlaw' has been born, with some of its journals are now published exclusively in cyberspace, for example the *Journal of Information Law and Technology*. Of some significance for this study is the fact that some of these authors (e.g. Saxby, Perritt and Reidenberg) have been engaged by the European Commission as advisors, following its practice of creating 'epistemic communities' (Wallace and Wallace, 1996), making this an important pool of discourse. It should be noted that many of the contributions go beyond merely legal considerations and extending into the wider political impact of the Internet. Some of the contributions are of central relevance to the questions about governance raised in this study.

A. Michael Froomkin (1997) argues that the net effect of the continuing internationalization of the Internet will be to promote liberal democratic values of openness and freedom. However, in a liberal democratic context, the Internet allows

for a process which Froomkin calls 'regulatory arbitrage'. This process means that communicants can avoid domestic regulations by virtue of the Internet's decentralised architecture, structuring their communications or transactions to take advantage of foreign regulatory regimes. This encourages free speech and makes censorship very difficult, especially given the availability of anonymous remailers and encryption software, which Froomkin explains in depth. Regulatory arbitrage 'reduces the policy flexibility of nations by making certain types of domestic rules difficult to enforce'. It is shown that totalitarian governments - a range is surveyed - will incur high costs if they seek to aggressively filter content, reducing the economic and intellectual value of being connected considerably. In liberal democracies the inability to enforce a ban on anonymous Internet communication will impose real costs in untraceable libel, and hate speech.

Froomkin's contention that the Internet will promote liberal democratic values of openness and freedom is supported by the work of Christopher Kedzie (1996,1997). Kedzie argues (1997) that there is empirical evidence that information interconnectivity is a 'powerful predictor of democracy'. Kedzie roots his strongly statistical argument in a conjunction of Samuel Huntington's (1991a,b) and Alvin Toffler's (1980) diverse notions of the 'third wave'. Toffler's concept based on the information revolution is combined with Huntington's wave of 'transition of some thirty countries from nondemocratic to democratic political systems' (1991a: xiii).

Henry Perritt (1996) examines the current law (in this case, United States law) and applies it to the novel situations encountered in the 'Information Superhighway'. In common with others, for instance Kaspersen (1996), Professor Perritt compares the Superhighway to a network of roads. Vehicle accident law translates into an examination of laws ranging from defamation to misleading advertising. Network access providers are compared to those who paint lane markings on the roads and with those who ensure that the ends of the roads meet so that drivers can pass from one

highway to another without worrying that the uneven road surfaces will cause the car radiator to jump through the bonnet. Civil dispute resolution and procedure, criminal law and International law are addressed. Perritt's approach is that the current law can deal with the Information Superhighway 'with no more difficulty than it had dealing with ocean commerce, international civil aviation or telecommunications when they were new' (1996:31). The author contends that 'intermediaries', that is access providers, should not face sanctions for activities they cannot prevent. Private dispute resolution systems currently emerging are examined in a positive light (1997:164) but it is conceded that conventional judicial sanctions must be available, enforced by state coercion. Perritt sees a role for the embryonic International Criminal Court being discussed under UN auspices (1997: 189). Ultimately both private and public international institutions must emerge to effectively police cyberspace (1997: 192).

Victor Mayer-Schönberger and Teree Foster (1997) examine the restriction of free speech on the 'Global Information Infrastructure' (GII) by various national regimes. They argue that the GII places constraints on both regulators and free speech absolutists, the latter affected by the consequences of national laws being imposed on international audiences. For governments 'an escalating national de jure regulation of speech meets a pervasive de facto futility of enforcement.' Some global system of regulation is advocated, and it is argued that the international law concept of *jus cogens* could form the basis of such. For Mayer-Schönberger and Foster liability must lie with the originator of the communicative act and not with the carrier or receiver.

David Johnson and Professor David Post (1997) argue that Cyberspace requires a system of rules quite distinct from the laws that regulate physical, geographically defined territories. Cyberspace challenges the law's traditional reliance on territorial borders; it is a 'space' bounded by screens and passwords rather than physical markers. Professors Johnson and Post argue that 'taking Cyberspace seriously' as a unique place can lead to the development of both clear rules effective legal institutions. Post (1995)

addresses the question as to who will make and enforce the rules that will govern cyberspace. He examines various 'controllers', or points from which rules can issue, ranging from technical network protocols, to private organisations like universities, to Congressional statutes. These controllers vary in their ability to enforce whatever rules they choose to adopt, depending on the existence of conflicting higher-level controllers, and on the possibility that those who are subject to the rules can change jurisdictions to seek a more favourable rule set. The Internet allows a relatively easy change of jurisdiction, or 'exit', from any given controller, leading to the unprecedented - and unpredictable - situation of a 'free market' in rule sets.

Joel Reidenberg¹ (1996) also examines the issue of rule-making, pointing to the 'emergence of a complex mix of rule-makers' (1996: 926). Governance in global networks should be seen as a mix of state, technical, business and citizen forces. Though national borders have less meaning in an 'Information Society', states retain a critical ability to influence rule making. They can provoke the creation of network standards mainly through incentives or allocations of liability on service providers, but also through technical standardisation. States retain physical power over persons and infrastructure and thus can exercise control over key network 'situs' points. A key example of state action in the European context for Reidenberg is the CompuServe case in Germany which we will deal with below. For Reidenberg, global communications networks challenge traditional sovereignty paradigms. Territorial borders 'disintegrate'. In the new situation 'the identities of the rule makers and the instruments used to establish rules will not conform to classic patterns of regulation.' A new paradigm is postulated:

[A] new network governance paradigm must emerge to recognise the complexity of regulatory power centers, utilise new policy instruments such as technical

¹I am very grateful to Professor Reidenberg for posting me his indispensable article.

standardisation to achieve regulatory objectives, accord status to networks as semi-sovereign entities, and shift the role of the state toward the creation of an incentive structure for network self regulation. (1996: 930)

Professor Clive Walker, while dealing with the substantive issue of fair trials in the 'new audio-visual media' seeks to 'identify the problematic capacities they have developed in relation to established forms of regulation, both national and international' (1996: 519). Problems arise from the new modes of information transfer and from the consequent inability of traditional forms of governance, whether national or international, to respond effectively to them, he argues (1996: 520). This delimitation of traditional regulatory powers is associated with the tendency towards transnational media configurations, and can be seen as part of a general dialectical decline in the operational structures and concerns of sovereign nation states.

The discourse of postmodernism (which might be linked here with economic analysis in terms of post-Fordism (Jessop, 1994) ...) would suggest a trend towards fragmentation within the state and the emergence of 'bubbles of governance' at local, regional, international and global levels along side the semi-sovereign state (Rhodes, 1994; Jessop, 1994: 274).

Walker goes on to maintain, however, that fragmentation does not necessarily mean loss of power and authority, and that the case made for the 'hollowing out' of the state (Rhodes, 1994) is contestable. A more accurate view he contends is that the fragmentary state can respond to challenges by more imaginative forms of governance. These could deal with post-modern and post-Fordist changes in ways which reach beyond the traditional mechanisms of the sovereign nation state, and the state could maintain for itself 'crucial functions in terms of managing the political linkages in governance.' In a later article (1997) Walker reiterates his case arguing that one can expect a trend towards 'governance' rather than the 'government', in which the role of

the nation state is not exclusive but ‘may need further sustenance by the activation of more varied levels of power at second hand’.

Yaman Akdeniz (1997) draws on the work of Reidenberg and Walker in his survey of the regulation of pornography and child pornography on the Internet. He argues that there is no settled definition of pornography in a multi-national environment such as the Internet. Cultural, moral and legal variations all around the world make it difficult to define ‘pornographic content’ in a global society. Akdeniz is the only author to date who comments on the European Commission’s contributions. Following the Commission’s Green Paper (1996b) he discusses two different issues within one context: the regulation of harmful content such as pornography and regulation of illegal content such as child pornography. He avoids any conflation of the two issues, arguing that ‘any regulatory action intended to protect a certain group of people, such as children, should not take the form of an unconditional prohibition of using the Internet to distribute certain content that is freely available to adults in other media’. A case study of the regulation of child pornography in the UK is undertaken. Influenced by the writings of Reidenberg and Walker, Akdeniz proposes a multi-layered solution for the regulation of pornographic content on the Internet. This ‘may involve the on-line users, Internet Service Providers, codes of practice, self-regulatory bodies, technical solutions, the Government, and the European Union in the near future’ (1997: 2). However the role of the European Union is not analysed in any depth. For Akdeniz the Internet is a ‘complex, anarchic, and multi-national environment where old concepts of regulation, reliant as they are upon tangibility in time and space, may not be easily applicable or enforceable’ (1997: 15). For this reason, he regards the wider concept of governance as being more suitable. He goes on to treat of the rationale for, and complex difficulties involved in particular policy instruments such as the Platform for Internet Content Selection (PICS) which I will also treat of below.

The above literature presents a starting point for research. There is a consensus among many of the authors on the fact that the Internet poses huge problems of enforcement for the traditional nation state. Whether understood in terms of 'safe havens', David Post's concept of 'exit' or Froomkin's 'regulatory arbitrage', the traditional congruence between national territory and functionality is under challenge. Professors Walker and Reidenberg have made an important contribution in postulating new types of governance in this new context. I will refer to the consensus emerging from their arguments as the argument for a 'network governance paradigm'.

Methodology

Central to this enterprise is an attempt to elicit a clear understanding of the Internet as a medium and the implications of its structure on communications policy in a liberal democratic context. If regulatory arbitrage is as significant as Froomkin maintains, what can the state do at a European level that does not suffer from the same drawbacks as national action? To what extent do European initiatives conform to the paradigm advocated by Reidenberg and Walker? Is the European Commission 'managing the political linkages' in governance, as Walker would have it, and activating more varied levels of power at second hand? The contributions of the European Commission are assessed in terms of their technical cogency and in terms of their success in attaining a feasible and implementable common position. To what extent does policy rely on incentives to access providers or allocations of liability, or on promoting technical standards? As regards regulatory arbitrage, what is Europe's role on the global stage?

This study will begin with chapters on the two major shaping influences of European policy on Internet content, namely the nature of the Internet itself and the pre-given structures of European governance. Chapter 2 introduces the Internet, its history and its uses. A discussion as to what metaphor is appropriate to it as a medium is undertaken. The difficulties posed by the technical architecture of the Internet for

would be regulators are dealt with, in particular difficulties related to the allocation of liability. In Chapter 3 the various contexts in which European policy making in this area takes place are examined. Political and constitutional contexts are examined with an emphasis on the different interests at play. In Chapter 4 the categories of illegal and harmful content, as adopted in European policy are critically evaluated, and the different issues of principle and technique which these raise will be introduced. European level initiatives with regard to illegal content, including justice co-operation, are critically assessed. Substantive policy and the policy process are both addressed with a view to answering some of the questions above. Chapter 5 deals with the issue of protecting children from adult content, evaluating the Union's role in promoting the Platform for Internet Content Selection (PICS) standard. In my concluding chapter I will examine the evidence to ascertain whether Reidenberg's network governance paradigm is borne out in this context. I will also offer some speculations on the prospects for global instruments of governance in this area and Europe's role in the promotion of such.

2 Defining the Internet as a Medium

What is the Internet?

Simply put, the Internet is a network of computers. Loader defines the Internet as ‘a collection of networks and gateways that use the IP protocol suite, and function as a single, co-operative virtual network’ (1997:229). Encyclopaedia Britannica (1997) describes the Internet as a ‘network connecting many computer networks and based on a common addressing system and communications protocol called Transmission Control Protocol/Internet Protocol (TCP/IP).The technical protocol referred to began on the ‘Arpanet’, initially sponsored by the US Defense Department's Advanced Research Projects Agency (ARPA), established in 1969 to provide a secure and survivable communications network for organisations engaged in defence related research (Froomkin, 1997). Researchers and academics in other fields began to make use of the network, and eventually the National Science Foundation (NSF), which had created a similar and parallel network called NSFNet, took over much of the TCP/IP technology from ARPANET and established a distributed network of networks capable of handling far greater traffic. NSF continues to maintain the backbone of the network (which carries data at a rate of 45 million bits per second), but Internet protocol development is governed by the Internet Architecture Board, while the Internet Network Information Center (InterNIC) administers the naming of computers and

networks (Encyclopaedia Britannica, 1997). Thus has the TCP/IP protocol evolved into the standard for world-wide communication of digital information. The digitisation of information, that is, conversion into binary code, is the foundation of the entire information revolution. Both audio-visual information and text can be converted into this format (Saxby 1990, 1996; Gates, 1996). While the traditional telephone wire is the typical carrier of Internet services, amateur radio, cable television wires, spread spectrum radio, satellite, and fibre optics all have been used to deliver digital information using the same protocol.

The Internet is growing exponentially (Froomkin, 1997). In 1983 there were around 200 computers on the Internet's precursor, the 'Arpanet'. As of January 1993, there were more than 1.3 million computers with a regular connection to the system. In January 1996 there were about 9.4 million Internet host computers. Access doubles approximately every year. As Michael Froomkin says (1997): 'at this rate of growth, the Internet cannot help but penetrate deeply into the general population of industrialised countries.'

The two most successful Internet applications have been electronic mail, known as E-mail)and the World Wide Web. The Web is a user friendly system for retrieving information in the form of pages. Written in HTML (Hypertext Mark-up Language), web pages contain hypertext 'links'. Browsing programs ('browsers') such as Netscape's Navigator or Microsoft's Explorer present a graphical interface which allows for easy navigation of the web. The hypertext links inserted by document authors refer the reader to other documents using addresses known as Uniform Resource Locators (URLs). A mouse click on a link refers the user to remote documents, images, sounds, or even movies that have been made Internet-accessible. A Web browser can retrieve data via File Transfer Protocol (FTP), Gopher, Telnet or newsgroups (discussion groups), as well as via the HTTP (Hypertext Transfer Protocol) used to transfer hypertext documents (Froomkin, 1997). E-mail - one of the original uses of the Internet

- remains a vital application. An estimated 25 billion e-mail messages were exchanged in 1995 (Froomkin, 1997). In the landmark judgement against the Communications Decency Act (CDA) judges grouped Internet communications into six categories:

- One-to-one messaging (such as 'e-mail')
- One-to-many messaging (such as 'listserv')
- Distributed message databases (such as 'USENET newsgroups')
- Real time communication (such as 'Internet Relay Chat'),
- Real time remote computer utilisation (such as 'Telnet'),
- Remote information retrieval (such as 'ftp', 'gopher', and the 'World Wide Web')

(US District Court for the Eastern District of Pennsylvania, 1996)

The Internet is an open architecture, meaning that one computer system can connect to others simply by adhering to the TCP/IP standards. It is not necessary for users of one computer system to use the same hardware or software as another computing system with which they wish to communicate, or even to know the nature of the hardware and software in the other system (Perritt, 1995). It has a 'distributed architecture', in the words of Henry Perritt (1995). This means that different parts of the eventual bundle of information content and related services desired by users may be supplied by different Internet nodes, operated by different persons or entities (Perritt, 1997: Fig. 1). As a communication medium the Internet is non-hierarchical, interactive, and global. Anyone with access can freely publish material which is then available globally and indefinitely. So in contrast with traditional centralised media the Internet has a many-to-many aspect as a medium. It is interactive as opposed to passive.

Conflicting Metaphors

In seeking to address the question as to what policy instruments are either desirable or feasible a clear understanding of the nature of the Internet is the fulcrum on which the answers must turn. Firstly, the Internet must be understood as a communication medium in some meaningful terms. Secondly, the technical infrastructure of the Internet must be understood in order to gauge which policy instruments are feasible.

On the first question: how does the Internet compare with the traditional media? Crucially do its communications fall into the private or public sphere? To what extent do analogies to print publishing, broadcasting and one-to-one communication by telephone or post apply? Print publishing is traditionally subject to very weak regulation (Commission, 1996b, annex 3) The answers to these questions impinge on what can be taken as desirable regulation, taking cognisance of privacy rights and questions of liability.

Jonathan Wallace and Mark Mangan, in the context of a libertarian argument against the ill-fated CDA, present a survey of communications revolutions from the invention of writing through printing to electronic communications. This yields fascinating insights. Each revolution prompted scares and the first attempts at regulation were inevitably misplaced and based on false understandings of the new medium (1996: 193-233). Wallace and Mangan, in conclusion, argue that the best metaphor by which to understand the Internet is the following: 'Cyberspace is a constellation of printing presses and bookstores' (1996:228). However this analogy fails to take adequate account of the more private elements on communication on the Internet. The closest analogy for E-mail, for instance, must surely be traditional mail. It is this private element which was emphasised in one of the judgements against the CDA. Judges maintained that 'the Internet may fairly be regarded as a never-ending world-wide

conversation' (Cunningham, 1996). The range of types of information on the Internet renders both approaches limited, I believe. That range stretches from private text exchanges right through to moving images and sound events which approach the status of traditional television programming, for example the recent participation of a large audience in viewing pictures relayed from the Mars exploration mission. Interestingly, those with a strong civil liberties orientation tend towards the printing analogy. Like Wallace and Mangan, Britain's National Council for Civil Liberties (Bird, 1996) takes such a view in its response to the Commission's Green Paper On The Protection Of Minors And Human Dignity In Audio-visual And Information Services (hereinafter 'The Green Paper'). The NCCL is particularly concerned with discounting analogies to film and computer games, the latter as we shall see below being relevant in the development of the PICS standard.

The various Internet media, principally [the] world-wide web, comprise mainly a text message supported by images and layout, like the pages of a magazine. Sound, and especially video clips, are greedy of bandwidth and unlikely to become the dominant part of it. The material conveyed is therefore not fictional drama or dramatised documentary, and only a little of it conveys game-playing. It is generally news, factual, hobby and 'chat' material, most resembling a spread of newspapers and magazines - in fact it resembles a much wider spread of small personal/organisational newsletters, and particular 'channels' are consumed entirely by choice where one adult usually has strong control of the receiving 'set'. If it resembles anything else it would be individual phone & fax conversations (although it is the published aspect which causes most concerns). Film, and particularly computer games, are a very poor model for the Internet and bear little resemblance to it. (Bird, 1996:10)

There is much that is questionable here. Bandwidth, as I have argued above, is likely to increase with technological developments. The inconvenience of downloading large

video or sound files is just that. Many Internet users put up with it. And while games are only one aspect of the Internet, content is not confined to the categories listed, but rather, runs the gamut of human interest. As I will argue in chapter 5 below, pornography in various forms is easily accessed.

The European Commission's 'Communication', I believe indicates a balanced understanding of the radically challenging nature of the new medium, rejecting the analogies based solely on publishing offered above.

A unique characteristic of the Internet is that it functions simultaneously as a medium for publishing and for communication. Unlike in the case of traditional media, the Internet supports a variety of communication modes: one-to-one, one-to-many, many-to-many. An Internet user may 'speak' or 'listen' interchangeably. At any given time, a receiver can and does become content provider, of his own accord, or through 're-posting' of content by a third party. The Internet therefore is radically different from traditional broadcasting. It also differs radically from a traditional telecommunication service. This constant shift from 'publishing mode' to 'private communication mode' - two modes governed traditionally by very different legal regimes - constitutes one of the main challenges of Internet regulation. (Commission 1996a)

Liability

One of the reasons why the question of analogies is so relevant is due to its impact on questions of liability for network and service providers. The traditional situation in the field of telecommunications is one of minimal liability, the provider of the means of transmission being seen simply as a neutral carrier. However, in such media as television and radio there has been a greater weight of legal responsibility involved. Essentially the development of digital technology is producing a phenomenon of

‘convergence between telecommunications and audio-visual’ media (Kaspersen, 1996), producing new quandaries in terms of allocating liability. The question of liability is given heightened importance due to the fact that, rightly or wrongly, network and service providers are seen as gatekeepers with some power over the content carried on their networks. Henrik Kaspersen of the Commission’s Legal Advisory Board also points out (1996) the difficulties involved in pursuing sanctions against Internet users responsible for misuse of the medium. These include difficulties in locating and ascertaining the real identity of such users, difficulties finding the necessary evidence of their acts, and the difficulties involved in pursuing cases across national boundaries. Thus the role of network and service providers in the governance equation is a crucial one. Kaspersen maintains that:

Both for the purpose of the identification of the perpetrator and for the removal of the illegal information the co-operation of the network service providers is indispensable. ...Technically, all the data traffic with or by the user passes the system of the access provider. (1996:1)

An access provider is a commercial organisation which allows a user to have access to the resources of the whole network during a fixed quantity of time per week or month for a set fee. Unsurprisingly, the degree to which access providers should be liable is a controversial one. They can claim to be nothing more than the transporter of data over the network, denying any responsibility for its content and refusing any obligation to act in cases of misuse. Any policy concerned with the regulation of controversial Internet content must come to some consistent position on this question of liability.

Some of the theorists covered in the literature review have dealt with the liability issue from diverse perspectives. Henry Perritt (1997) contends that ‘one of the by-products of jurisdictional uncertainty is that intermediaries become even more attractive targets than in the past for criminal prosecution and civil lawsuits’. He echoes Kaspersen in

maintaining that ‘Intermediaries (network access providers) may be easier to identify than originators of harmful content. Furthermore ‘intermediaries’ may be perceived as having greater financial resources and:

...may be more easily subjected to judicial jurisdiction because they have physical or virtual presence in many more places than content originators, making it easier to execute judgements against them or to use forfeiture as a criminal penalty. (Perritt, 1997)

Ultimately, according to analysts like Perritt (1997), Post (1995) and Reidenberg (1996) this subjection to liability puts access providers in a rule-making position. According to Perritt (1997), ‘an intermediary who responds to a threat of civil liability by refusing to handle controversial material is in effect engaging in a rule-making function.’

Technical Infrastructure

Turning to our second question; how can the infrastructure of the Internet be understood so as to give clear indications on the technical limits of policy? Firstly the scale of accessible material is massive, meaning that scale in itself limits the feasibility of monitoring, in contrast with traditional media such as television. Secondly, the form in which information is transferred under Internet protocols makes it highly unamenable to monitoring. This entails a system known as ‘packet switching’, a method by which messages are subdivided into smaller standardised packets which are then routed independently to their destinations via an indeterminate number of intermediaries (Froomkin, 1997; US District Court for the Eastern District of Pennsylvania, 1996). This decentralised, anarchic, method of sending information appealed to the Internet's early sponsor, the Defense Department, which was intrigued by a communications network that could continue to function even if a nuclear war destroyed a large fraction of the system. Packet switching ‘makes it difficult for anyone,

even a government, to block or monitor information flows originating from large numbers of users' (Froomkin, 1997)

Thirdly, the Internet engenders a new space - 'cyberspace' - which presents regulators with an indeterminate terrain:

Cyberspace does not merely weaken the proposition that the effects of conduct taking place at a particular geographical location are felt primarily by persons at or near that location, it renders it virtually unintelligible; it does not merely render geographical boundaries ever more permeable, it obliterates them entirely, because geographical location itself is both indeterminate and irrelevant for transactions on the net. (Johnson and Post, 1997b)

There is no relationship between machine addressing (the location a computer in the virtual space created by the TCP/IP Protocol addresses and domain names) and the physical location of the machine and its user (Johnson and Post, 1997a, b). At present, while there is a convention of whereby many addresses include country signifiers (e.g. '*.uk', '*.ie'), no countries legally stipulate that machines within their geographic boundaries use such a signifier. Moreover, there are no registries that can prevent individuals holding such a country designator from assigning that designator to machines in other countries, nor is there a means of limiting the use of technical protocols such as the Telnet protocol to access the Internet from other Internet access points (with other addresses). Nor is the use of non-country-specific designators (e.g., '*.com', '*.org') restricted in any way (Johnson and Post, 1997b: note 6). In addition to the addressing problem location is rendered indeterminate by the features of some Internet interactions. Johnson and Post (1997b) instance distributed databases (such as Usenet newsgroups) which 'have no single place of existence at all, but are aggregates of information stored on a large (and constantly changing) number of individual

machines at any time.’ And location is irrelevant in the sense that network servers are equally accessible from everywhere. A Web site in any corner of the network can be accessed with equivalent transmission speed and message quality from any other corner of the network, and therefore the effects of whatever information is available at that site are felt simultaneously and equally in all jurisdictions, independent of their ‘distance’ from one another. Needless to say, this indeterminacy of location in cyberspace poses grave problems for those who would govern content. Besides the difficulties in locating transgressors there are problems which arise from the externalities of any policy implemented (which Post and Johnson call ‘spillover’). This raises issues of legitimacy, since in such a situation many of those affected by a policy would have no say in its making.

Lastly, the availability of anonymous remailing facilities (Froomkin, 1997; Perritt, 1997) allows Internet users to avoid being held responsible for the contents of the messages they send. The effect is to make both censorship and information export restrictions ‘nearly impossible to enforce’(Froomkin, 1997). Anonymous remailing is made possible by encryption technology. Digital information is highly amenable to encryption, a process whereby information is encoded using mathematical algorithms. The information is then only readable with the correct ‘key’, a password in effect. A process known as public key cryptography was invented in the 1977 by mathematicians Rivest, Shamir and Adelman. Their RSA algorithm did away with the need to exchange codebooks or keys before the sending of a message (Campbell, 1997b). The security of encrypted information depends to a large degree on the length of the key used, and RSA encryption with a key length of 112 bits (strong encryption) is apparently uncrackable. Any policy aimed at the regulation of communication on the Internet must face this issue. Some governments have been keen to either limit public access to strong encryption, or to oblige users to leave copies of their keys with ‘Trusted Third Parties’ (Campbell, 1997b). But the interests at stake for governments are complicated

by the fact that strong encryption represents a 'holy grail' in terms of security of electronic commerce.

Given these elements in the information infrastructure presented by the Internet - volume of data, packet switching, indeterminate terrain and encryption supported anonymity - its governance poses a huge challenge for would be regulators. Froomkin (1997) concludes that any effort to censor the Internet organised at the national level (or below) is likely to fail. He cites John Gilmore's pithy comment in order to summarise the situation: 'the Net interprets censorship as damage and routes around it.'

3 Political and Constitutional Contexts

The European Union, Interests and Communication

A hypothesis which this research seeks to test is that the Internet limits the instruments available to the liberal-democratic state to control communication. The view of the state being taken here is a fairly neutral, instrumentalist, one. The state is looked at as an instrument through which policy goals may, or may not be achieved. This allows a certain distinction between means and ends. The state is a powerful instrument, with potential to enforce policies whether positive or negative. State regulations in the communications arena may inspire acceptance or rejection, depending on one's viewpoint and the circumstances. Policy may be aimed towards the enforcement of hegemonic mores, towards the protection of children, consumers, or 'human dignity'. But the crucial issue in this study is the enforceability of policy.

Of course the state is more than a neutral instrument of policy. As an institution it is intertwined at times with specific interests. But in order to understand the interests that influence the state at a European level, it is necessary to ask what is meant when one treats the European Union as a state. The European Union is a unique case in this regard, since it cannot be called a state in the traditional sense of the word. For instance it does not hold the classic monopoly on instruments of coercion. Authors refer to a 'part-formed', or 'would-be' polity (Lindberg, 1970), and to 'putative'

statehood. Streeck and Schmitter refer to the Community's 'quasi-state' or 'nonstate' (1991: 142).

The union is a mix of supranational and intergovernmental elements. The key to understanding the interests at play in this framework is to look at the institutions of the Union. The European Commission, the Union's policy entrepreneur, is a supranational body, bound to seek the overall European interest. The Commission has an interest in expanding its own supranational political territory:

...the move of organised interests onto the European scene was expected to be further accelerated by European bureaucrats who, in their search for a constituency, would be more than willing to promote interest organisation on a scale coterminous with their supranational jurisdiction. (Streeck and Schmitter, 1991: 134)

This view is offered in the context of neo-functionalist theory of 'spill-over' (Hass, 1958). In that theory supranational interest-group formation was expected to serve as an indispensable substitute for popular identification with the emerging political entity, above and beyond the nation state. As it turns out, the relationship between the managers of European collective interests and European bureaucrats has been very intimate, a relationship smoothed by similarity among the personnel. Both groups are 'appointed rather than elected, both experts and technocrats, both susceptible to a cosmopolitan lifestyle, and both professionally interested in the smooth management of complex interdependencies ...' (Streeck and Schmitter, 1991:134)

The European Parliament, like the Commission, is a supranational body. Like the Commission, it has been concerned with the expansion of its own political territory, having won increased powers in successive treaties. Its case for increased powers is strengthened by the fact that, in contrast to the Commission, it is the Union's only

democratically elected representative body. It confers legitimacy, and brings democratic accountability to the Union. Charged with pursuing the will of the Unions citizens, the Parliament sees itself as representing the public interest. It has a strong record of promoting human rights and it is worth pointing out that its make up, a social-democratic led majority, often its influences policy emphases, as shall be seen below.

Attempts by these two supranational institutions to enhance their own status as incipient organs of sovereign government are limited by the existence of the intergovernmental Council of Ministers. Streeck and Schmitter see this as a strong 'centrifugal centre' in the Union's quasi state. No comparable barrier to central state formation and state growth has ever been present in a traditional nation state. (1991:142). Above all, the Ministers in the Council pursue the perceived interests of the respective member states, or more accurately, the member governments. The national pull in the community is strengthened by the fact the procedure of governance based on Directives, which must be nationally enacted and nationally enforced (often with different degrees of enthusiasm). According to Joel Reidenberg (1996: 925) directives do not in themselves create supranational rights that can be invoked by citizens, however the developing role of the European Court of Justice (a third supranational institution of the Union) should not be overlooked.

A complex mix of interests is at play in the European Union, complicated by of competition between the constitutive institutions. As Streeck and Schmitter describe the situation:

Together with the member states, regional and supranational political entities share in the diffuse and fragmented sovereignty of the Community, blending into a highly interdependent but incompletely unified, loosely coupled, and diverse institutional complex - the new type of state that is the European Community. (Streeck and Schmitter, 1991:153)

The European Union as a state is closely identified with both liberal democracy and capitalism. As we shall see below, liberal democratic norms are integrated into the Union's structures. Liberal democracy and capitalism do not logically necessitate each other (though the protection of property rights is crucial), but on a practical level there is substantial dovetailing between the two. In the European context, it has been argued that the integration project is closely linked with a capitalist project of deregulation:

In the 1992 compromise, the project of European integration became finally and formally bound up with a deregulation project. (Streeck and Schmitter, 1991: 149)

European Union Telecommunications policy is highly developed. Indeed the Internet is seen as instrumental in developing economic growth in the services industries. This is closely allied to the aim of completing and maintaining the single market and the free movement of goods and services. What is to be drawn from this is that beyond the interests of policing and justice, other interests are likely to impinge on the outcome of any policy designed to regulate Internet content.

But how do these limit the state's room for manoeuvre? Froomkin, having surveyed the situation in Asian non liberal democratic regimes concludes that totalitarians will fare worst in this new world, as they will be forced to choose between, on the one hand, limiting access and paying a substantial price in economic growth (Kedzie, 1996) or, on the other hand, letting go of their control of information, a traditional tool of social control (Froomkin, 1997). However, while for Froomkin the promotion of openness and free speech by the Internet is tantamount to the promotion of liberal democracy this deduction is questionable, since social control is not the only goal involved in the regulation of communication. The protection of individual rights, something integral to liberal democracy may also involve the regulation of communication, and is one of

the aims involved in the policies under review in this study. Thus while the free speech promoted by the Internet may undermine authoritarian regimes, it is possible that the infrastructure may at the same time limit liberal democratic governance in areas concerning individual rights. What of the states ability to protect, say children and minorities? The fact that the European Convention on Human Rights (ECHR) is a constraining influence in Europe is an important factor. The state is working in a rights-based context. This means that there are legal constraints on policy as well as those dictated by economic interest (Froomkin, 1997).

Constitutional Contexts: European Convention on Human Rights

An important constitutional context is provided by Title VI of the Treaty of European Union (TEU) which sets out the provisions for Justice and Home Affairs co-operation. It states that co-operation in all the listed policy areas ‘shall be dealt with in compliance with the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950’ (Treaty of European Union, 1992). The regulation of Internet content involves these fundamental rights in particular rights to free expression and privacy, which as we shall see below, must delimit any policy. In fact the European Convention is binding on all member states who are signatories and thus circumscribes regulation norms of the traditional media in Europe. Policies on Internet content regulation take place in this context of foregoing content regulation in the more traditional media in national regimes and to some extent at a European level. Existing media regulation takes place in the convention framework. Article 10 of the European Convention on Human Rights reads:

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers. This

Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary. (Council of Europe, 1993)

This principle has been incorporated into the TEU (TEU Article F(2)), community law as expressed by the European Court of Justice, and into the constitutions of the member states where a written constitution applies (Commission, 1996b). The UK has recently announced its intention to incorporate the convention into domestic law (Adonis and Wintour, 1997). As is apparent in Article 10 the principle of freedom of expression is not an absolute one. Restrictions by the state are allowable but are however, as stated in the green paper, 'circumscribed by a very precise set of combined criteria that have been clearly enunciated by the ECHR' (Commission, 1996b). Restrictions must be: prescribed by the law (transparency, to the exclusion of the arbitrary); necessary, that is to say they must meet a genuine social need and respect the values inherent in a democratic society; and must pursue legitimate objects that are defined exhaustively; these include the protection of public health and morals, which are of particular relevance to the protection of minors and human dignity. Thus any restrictive measure must be necessary, not just useful or reasonable. 'Its mandatory character can be deduced only from a detailed analysis of its effectiveness and the extent of the interference. The test is one of the proportionality of the restriction.' (Commission 1996b)

The principle of respect for privacy is enunciated in Article 8 of the Convention:

Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights or freedoms of others. (Council of Europe, 1993)

Restrictions are allowed on much the same terms as in the case of freedom of expression. Restrictions on the principle are possible (for instance to identify and punish private communications for criminal purposes), though once again the proportionality test, as developed in the case law of the European Court of Human Rights, must be passed. The Commission argues in its green paper (Commission, 1996b) that in the absence of common rules these principles constitute a highly significant 'European core'. Beyond these core principles the legal regimes in the Member States 'vary greatly and reflect differences in cultural and moral standards'. In its green paper the Commission sees the proportionality test as a 'powerful factor for convergence' between the Member States.

Justice and Home Affairs in the Treaty of European Union

Another context is the constitutional framework of the European Union itself and the resulting decision making mechanisms. While such areas of policy as free movement of services and common standards come under the ambit of the 'first pillar' of the Union, the highly developed and integrated structures of the traditional communities, Justice and Home Affairs co-operation falls under the 'third pillar' created under Title VI of the (Maastricht) Treaty of European Union (Wallace and Wallace, 1996). Before this

treaty Justice and Home Affairs had not been part of the community framework being handled under the more opaque and informal structures of the 'Trevi' network. This was co-ordinated by the Council Presidency but had little accountability and few links with institutions (den Boer, 1996). Co-operation on justice issues has been spurred by increasingly internationalised processes of which the Internet is but one. Kapteyn (1995) has argued that globalization has enabled a variety of social actors to have access to an international arena as an extension or as an alternative to the state arena. This has generated new kinds of policy issues and new forms of political interaction. Helen Wallace 1996: 17) points out how globalization in the economic and security arenas and in the new 'global issues' such as ecology induces needs for transnational co-operation. Such globalising trends, moreover, have 'weakened the link between national identities and state capacities' (Wallace and Wallace, 1996: 439). To these global issues must be added the regulation of the Global Information Infrastructure. The links between the information revolution and the increased mobility of capital on a global scale should not be overlooked. As one writer describes the situation:

Technology has made us a 'global' community in the literal sense of the word. ..[M]ankind now has a completely integrated financial and information marketplace capable of moving money and ideas to any place on this planet in minutes. (Wriston, 1992: 61-2)

The price for the inclusion of Justice and Home Affairs in the new Treaty was, as Wallace (1996:55) points out, its subjection to a weaker institutional regime. The 'third pillar' is more intergovernmental than the first, and more co-operative. The Commissions role is lighter than in the first pillar, while the Parliament's role is that of offering comment. The key institution is ultimately the Council at whose request the Commission must act. The type of policy (revise this) instrument which co-operation under Title VI can produce differs from those of the traditional communities, leading to conventions rather than directives. All of these restrictions reflect the sensitivity of

justice matters, representing 'high politics' and close as they are to the core of traditional national sovereignty. They impinge closely on the key attribute of statehood in Weberian terms: the monopoly of coercive power. Another reason for the sensitivity of justice issues is the range of differences among national police and legal cultures (den Boer 1996). There are also sensitivities regarding civil liberties and democratic accountability.

Proximate Political Context

The issue of illegal and harmful content on the Internet was first identified as an urgent priority at an informal Council of Telecommunications and Culture ministers held in Bologna on 24 April 1996. The Council requested that Commission produce a summary of the particular problems and challenges posed by the rapid development of Internet, and that it assess, in particular, the desirability of European or international regulation. The Commission set up a Working Party to fulfil this task (Commission, 1996c). Also in April 1996, UNICEF and the Council of Europe organised a joint meeting to discuss the commercial exploitation of children. Here, the Irish Minister of State for European Affairs, Gay Mitchell, called on the EU to investigate controls on the transmission of child pornography on the Internet (Smyth, 1996; Akdeniz, 1996). The Commission's work resulted in the publication of three documents. The first, a Communication on 'Illegal and harmful content on the Internet'(Commission, 1996a) attempts to address controversial content generally. The second document, the Green Paper On The Protection Of Minors And Human Dignity In Audio-visual And Information Services (Commission, 1996b), as its title suggests is confined to the protection of children. Its scope, however, extends beyond the Internet. The third, the Report of the Working Party (Commission, 1996c) contains substantive recommendations, elaborating on some of the proposals of the other two texts 'in practical terms'.

The Autumn of 1996 saw various specialised ministerial Councils (Industry, Justice and Home Affairs, Culture and Telecommunications) discuss subjects relevant to the regulation of Internet content. This shows that the complexity of the topic cuts across narrow functional boundaries. It also reflects political response to heightened public awareness of child protection issues in the wake of Belgian Child abuse scandals which were associated with Internet use. The increased awareness of child protection and justice issues was also obvious in the Irish administration which was President of the Council of Ministers during the second half of 1996. The Telecommunications Council of 27 September had 'a broad exchange of views' on the question of preventing the dissemination, via the Internet or similar networks, of illegal material and in particular material containing, or likely to lead to, violence against or sexual exploitation of children. It noted the transnational dimension of this problem and the consequent need to address it at national, European as well as international level (Commission, 1996c). The Council agreed to extend the Working Party, and politically agreed a resolution based heavily on its report's recommendations.

4 The Developing Policy Consensus

In this chapter I will examine the emerging policy consensus at a European level on controversial Internet content. The impact of the policy making process on the final outcome will be examined along with the substantive policy recommendations. The latter will be critically evaluated as regards the feasibility of their enforcement within the infrastructural parameters of the Internet. I will conclude with a discussion as to whether these policies entail a novel pattern of governance.

Defining categories of content

All of the key policy statements under review are premised on the distinction between ‘illegal’ and ‘harmful’ content and go on to outline the types of content deigned to belong to these categories. This distinction has a large impact on the outcome in terms of the resulting emphases and recommendations. The Communication maintains that the illegal/harmful distinction is ‘crucial’ as:

These different categories of content (illegal and harmful) pose radically different issues of principle, and call for very different legal and technological responses. It would be dangerous to amalgamate separate issues such as children accessing pornographic content for adults, and adults accessing pornography about children.

The Communication later concludes that:

The main weapon for dealing with harmful content is in ensuring that practical means are available to limit access by the vulnerable to such content.

It would seem from this that what the Commission has in mind when speaking of harmful content is content harmful to the development of minors, for instance sexual content, which should not be universally restricted. However, this is at variance with the implied definition of harmful content elsewhere in the same document. Under the rubric of 'Harmful Content' a broader definition emerges:

Various types of material may offend the values and feelings of other persons: content expressing political opinions, religious beliefs or views on racial matters etc. What is considered to be harmful depends on cultural differences. Each country may reach its own conclusion in defining the borderline between what is permissible and not permissible. It is therefore indispensable that international initiatives take into account different ethical standards in different countries in order to explore appropriate rules to protect people against offensive material whilst ensuring freedom of expression.

This confusion in defining harmful content has the effect of projecting a broad category, yet one which in practise is reducible to children accessing adult material. Other possible forms of 'harmful' content are conveniently dropped early in the discussion, somehow devalued through the Commission's consigning of them to the domain of culturally relativist, subjective values somehow beyond the European Union's remit.

'Illegal content' is a similarly problematic category in European Union policy. This is so because of the diversity in the legal regimes of the member states. As the communication outlines:

The exact definition of offences varies from country to country. Within the EU, even child pornography, for example, where a high degree of consensus exists, is covered by specific legislation in some Member States and by more general rules relating to obscenity in others.

In view of this situation, the Commission stresses 'the fundamental importance of co-operation between the Member States in the field of Justice and Home Affairs, and that 'common definitions of what ought to be treated as unlawful are needed' (Commission, 1996b). Since Justice and Home Affairs is subject to the intergovernmental regime of the Third Pillar, where unanimity is the order of the day, and given the sensitivities involved, such common definitions are likely to focus such areas of high degree consensus as child pornography. Illegal Content in any European regime is likely to be defined by the lowest common denominator.

If we turn to another area of controversial content where there is less consensus - racism related content - we see it fall between the two stools of 'illegal' and 'harmful' content. This is despite serious concerns about racism on the Internet, as exemplified by Michael Whine in his survey (1997) of its use by far right-wing extremists. He expresses concern that such extremists are using the new medium to avoid legal sanctions against racist propaganda in many countries, offering them 'undreamed-of possibilities'(1997: 209). Holocaust denial material now has its own newsgroups, he notes, and racist video games are being promoted (such as 'concentration camp manager'), some of which have fallen into the hands of children. (1997: 214, 220). Whine desires a more proactive approach by concerned authorities, citing the International Covenant on Civil and Political Rights and the Convention on the

Elimination of all Forms of Discrimination as relevant instruments (1997:227). While the Communication's definition of harmful content seems to include such content, it is soon eclipsed by the reduction of the harmful category I have outlined above. As a potential area of illegal content, racism related content displays huge diversity in terms of the legal regimes of the member states. For example publication of *Mein Kampf* or 'revisionism' (ie holocaust denial) are forbidden in some member states, e.g. Germany, but not in others (Commission, 1996a: note 7). The Parliament, recalling in the Council's Resolution designating 1997 European Year Against Racism, lists racism, incitement to racial hatred or violence, and holocaust denial - among other categories - as problems which the European Union 'cannot stand aside from' (European Parliament, 1997: par J) and advocates the adoption of common legislation explicitly banning such content (European Parliament, 1997: par K). A long series of strong statements by the Parliament on racism related issues is invoked. The prospects for such common legislation are complicated not only by the exigencies of the Justice and Home Affairs apparatus, but also by the demand for homogenous regimes amongst diverse media.

The policy-making process

Policy on controversial Internet content takes place in the regulatory cluster of policy making in the Union, as opposed to constituent, distributive and redistributive clusters. The typical style of policy making in this regulatory cluster is characterised by 'disaggregated decisions, legal or quasi-legal processes and specialised interests' (Wallace and Wallace, 1996: 446). According to Wallace and Wallace (1996: 449) the structure of community policy making was 'designed from the outset to disaggregate issues wherever possible, to disguise broader political issues, [and] to push issues down from ministerial confrontation to official *engrenage* within the hierarchy of committees which formulated proposals for ministers to approve and the parallel hierarchy of committees which co-operated in their implementation' (Wallace and Wallace, 1996: citing

Wessels 1990, 1992). According to the argument, the rhetoric of technocracy and rational administration has reinforced this tendency to depoliticize issues. Members of Council of Ministers, preoccupied with their national dossiers, cannot focus on the technicalities of policy. Moreover, the Union's framework reinforces a tendency towards sectoral policy communities. Wallace and Wallace conclude that the massive growth of European Union regulation in recent years, placing it at the core of the Union's policy making, 'partly reflects a recurrent coalition between the Commission as policy entrepreneur and industrial interests preferring to move regulation to the European Union level'. This conclusion is one which mirrors the analysis drawn from Streeck and Schmitter in the preceding chapter, authors who emphasise that 'by fostering a transnational system of organised interest formation, the Community and its Commission in particular would thus contribute to its own growth as a policy arena and executive body' (Streeck and Schmitter, 1991: 134-5).

These elements in the policy process can be seen at play where Internet content is concerned. Moreover, it can be argued that these elements are reinforced by the nature of issues in this policy area. The technical complexity involved enhances Commission technocracy, and entails the use of its pattern of co-opting external, commercial, expertise. Preoccupied Ministers may be presented with a *fait accompli*. Moreover, the crucial role of intermediaries (Internet Service Providers) provides further rationale for their involvement in policy development. This pattern is borne out by the decision of the Council of Telecommunications Ministers of 27 September 1996 to expand the Working Party on illegal and harmful content (from a collection of national delegations) to include representation of the relevant industry interests, including content providers, telecom/cable operators, access/service providers, a hardware manufacturer and representatives of users (Commission, 1996d). Many of the resulting report's recommendations are reproduced word for word in the Council of Ministers Resolution. A Commission official has confirmed to me that non elected civil servants have played in the policy's development. Notwithstanding the crucial situation of

service providers in the Internet's infrastructure, one recalls the makeup of the Working Party when the Report asserts that 'co-operation from the industry and a fully functioning system of self-regulation are essential to limiting the flow of illegal content on the Internet.' Besides the momentum toward European level interest organisations represented by the Working Party itself, any system of self regulation in the Commission's vision would involve European level organisations of service providers and self regulation bodies (Commission, 1996c).

Another relevant element in the policy-making process is the potential obstacle represented by the difference in outlooks among the member states. We have already seen a degree of diversity in the relevant constitutional and legal provisions of the member states, albeit with a certain amount of common ground. A representative of Ireland on the Working Party has outlined to me how disagreement between members on substantive common legal instruments has led to an increasing emphasis on a policy which has received unanimous assent, namely the promotion of the Platform for Internet Content Selection (PICS). This is a technical standard which aims to restrict the access of minors to adult content. The promotion of this standard represents a new form of governance in the context of content regulation, I will argue below, and presents unique problems as regards implementation. But it is worth pointing out at this juncture how much this policy option is supported by the nature of the policy-making process I have been describing. It eclipses nationally based discord. It involves close co-operation between the commercial industry and Commission technocrats on a protocol which is presented as a package and is thus unlikely to be questioned in its details by the Council or the Parliament. Moreover, in its presentation as a technically complex mechanism ethical nuances are obscured. Significantly, PICS has been developed by an institution charged with developing web standards which has been sponsored by the European Commission.

Emergent Substantive Policy

The emphasis in this section will be on the emerging policy on illegal content as expressed in various documents of the Commission, the Council of Ministers and the Parliament. In Chapter 5, I will examine policy on 'harmful content' as represented by PICS, the most concrete single policy measure on which there is large policy consensus. The European Commission's policies are enunciated in the Communication (1996a), the Green Paper (1996b) and the Report of the Working Party' (1996c). The Communication is aimed at presenting proposals for immediate action to deal with both illegal and harmful content. On illegal content it calls for reinforced co-operation between member states in the Justice and Home Affairs context, an assessment of the need for a 'common European framework to clarify the administrative rules and regulations which apply to access providers and host service providers' (liability) and the encouragement of self-regulation. The Green Paper is framed with a longer term outlook and is a consultative document. The policy options considered more or less mirror those in the Communication, however, including: 'systematic exchange of information, joint analysis of national legislative provisions, establishment of a common framework for self-regulation, recommendations for co-operation in the field of justice and home affairs, [and] common orientations for international co-operation'. However the Green Paper focuses on raising questions as much as on narrowing down the options. Questions such as liability and the appropriate fora for international co-operation are left open.

The Working Party Report comes out strongly in favour of self regulation, perhaps reflecting the Working Party's makeup, as we have seen above. Representative bodies for industry and users are envisaged as a key element in any self regulatory system. Such a system would include:

- A Code of Conduct for Internet service providers (access providers, host service providers and anonymous remailers),

- A hot-line for complaints from the public, with appropriate safeguards against misuse, (and)
- An independent self-regulatory body, including representatives of industry and users, to advise on whether or not a breach of the Code of Conduct has occurred (without prejudice to the due process of law) (Commission, 1996c).

The self regulation system, it is asserted, would need to be in compliance with and supported by the legal system. Failure to comply with the system rules can result in legal sanctions. Moreover, the code of conduct could be made more binding by member states through a requirement that it be formally approved, or integrated into contracts between network operators and service providers. The Report advocates European co-ordination of representative and self regulation bodies and asserts that the Commission should collaborate in establishing this and should contribute towards the initial cost. Co-ordination should include common standards for national codes of conduct and the establishment of a European network of hot-lines.

The areas of consensus in the above documents are reflected in the Council of Ministers Resolution politically agreed at the Telecommunications Council of the 28 November 1996 and formally adopted at the Council of 17 February 1997. The resolution welcomes the Working Party Report, and repeats many of its recommendations. It requests the Commission to 'ensure the follow-up and coherence of work on the measures suggested in the report, taking into account other relevant work in this field (the Communication and Green Paper) and to reconvene the Working Party as necessary to monitor progress and take further initiatives if appropriate'. Furthermore, it requests the Commission to 'foster co-ordination at Community level of self-regulatory and representative bodies and to promote and facilitate the exchange of information on best practice in this area.' Finally, it requests the Commission to foster research into technical issues, in particular filtering, rating, tracing and privacy-enhancing technologies, taking into account Europe's cultural and

linguistic diversity and to consider further the question of legal liability for Internet content'. (Filtering and rating will be dealt with below in Chapter 5.) Liability remains an outstanding unresolved issue. The mention of privacy-enhancing and tracing technologies (originating in a recommendation in the working party report) may reflect an oblique acknowledgement of the thorny issue of encryption. Interestingly encryption provides not only for the evasion of regulation but also for secure business transactions, which impinge greatly on the European Union's project of developing the Internet as an engine of economic growth. The aspiration towards tracing technologies is thus aimed at reconciling material interests as well as those of combating crime, all in a pre-given context of Convention protected privacy rights for those who have legitimate needs for anonymity (e.g. sexual abuse survivors, those recovering from addictions, etc.) However, given the nature of packet switching and the availability of strong encryption, it is likely that tracing technologies will remain merely an aspiration. The Resolution also invites the Member States to take the following actions:

- To encourage and facilitate self-regulatory systems including representative bodies for Internet service providers and users, effective codes of conduct and possibly hot line reporting mechanisms available to the public.
- Encourage the provision to users of filtering mechanisms and the setting up of rating systems (for instance the PICS standard launched by the international World-Wide-Web consortium with Commission support should be promoted).
- To participate actively in the International Ministerial Conference to be hosted by Germany and encourage attendance by representatives of the actors concerned. (The Bonn Conference). (Council of Ministers, 1997)

The Resolution further recommends that the Commission and the member states take all necessary steps to enhance the effectiveness of the above measures 'through international co-operation building on the results of the International Ministerial Conference and in discussions in other international fora'.

In response to the above policy statements, a Resolution of the European Parliament has been passed on the subject of illegal and harmful content. In addition to the parts addressed to the issue of racism, as outlined above, the resolution echoes the emphasis of the Commission and the Council on self regulation and filtering. A 'purely punitive approach', it is argued, would 'substantially undermine' the positive contribution of the new technology. The Commission is called upon to 'draw up a European quality rating system for providers of Internet services and to support international co-ordination of such ratings'. The Parliament's concern with the public interest is apparent when it states that Justice and Home Affairs co-operation under the TEU, being purely intergovernmental in character 'fails to provide for the democratic control and impetus which it is up to Parliament to provide in this area'. (European Parliament, 1997: par m.) As noted above, the Parliament calls for common European legislation banning racist content (1997: par K).

Self Regulation, Liability and Intermediaries

The emphasis on self regulation in the emerging policy reflects, in my view a realistic appraisal of the limits of a traditional government role in this area and an acknowledgement of the key place of 'intermediaries' in the governance of Internet content, given the unique infrastructure of the Internet as a communicative medium. Self regulation has other positive dimensions, as argued for instance by Clive Walker:

Self-regulation in this field has a number of advantages. Rules devised by the media are more likely to be internalised and accepted. In addition, it may avoid heavy-handed legal intervention which carries with it the spectre of government censorship (1996: 537-38).

As the Commission states, 'the issue of self-regulation and liability are... closely connected and need to be examined together' (1996c). As we have seen above, however, liability remains an unresolved issue which the Commission has been asked by the Council to consider further.

Territory and Encryption

At times, the Working Party report seems unrealistic, for instance in seeking to apply a code of conduct to anonymous remailers. The whole point of anonymous remailers is that they are usually located outside of the relevant jurisdiction, thus allowing the user to benefit from Froomkin's 'regulatory arbitrage'. Thus I believe that European self regulation is likely to be bypassed in this respect, in the couple of seconds it takes to type a web address on a keyboard. Maybe it is thought that anonymous remailers operating within European jurisdictions may be restricted from facilitating the actions of their overseas clients. Such clients have the whole globe at their disposal, however. This is before we take into account the implications of the availability of encryption technologies which receive little attention in the documents under consideration here (Froomkin, 1997). Astonishingly, the word encryption is not actually mentioned in any of the key policy statements on controversial content. This may reflect the disadvantages of the highly sectoralised nature of policy-making in the union. Other policy sectors have been highly active in promoting the legal recognition of strong encryption as a means of guaranteeing European pre-eminence in the sphere of electronic commerce (Campbell, 1997c; Commission, 1997).

The Working Party report also seems to be unrealistic elsewhere, again treating the Internet as a sub-global infrastructure:

Where the (illegal) content emanates from abroad, they should pass information to the host country's self-regulator. They should also if requested transmit appropriate information to the police to allow them to fulfil their tasks, or to exchange information with another police force.

This is fine in a European context, and even in this context self regulation and police regulation is embryonic. What of illegal content originating in, say, Thailand? The obvious question of global structures for governance in this area is raised, one to which I will turn later.

The conclusion to the Commission's Green Paper contends that:

.. faced with the limits to purely national solutions and the difficulty and of devising and applying world-wide solutions, the European Union has a fundamental role to play. But the potential for transnational development of the decentralised services is such that common or at least compatible solutions are worth seeking in the European Union. (1996b)

This encapsulates an important issue to be faced. First and foremost, the obvious question that arises is whether actions at a European level do not suffer from the same limits as those on a national level. How can the Union's role be fundamental? Obviously, where offending material originates in a member state common European Union rules can facilitate action. Where material originates from outside the community it may be argued that any European action will have greater influence at international level than isolated national action, an argument made to me by the secretary of the Working Group. However any actions suffer the same limitations imposed by the decentralised nature of the Internet. The CompuServe case in Germany, among others, illustrates the process of regulatory arbitrage which would affect European enforcement as much as that in any member state. In the CompuServe

case the public prosecutors considered that certain items available on newsgroups were illegal, and requested CompuServe to block access to these newsgroups. Since CompuServe's software did not initially make it possible to differentiate between German subscribers and others for access to newsgroups, CompuServe suspended access to a number of newsgroups to all of its subscribers world-wide. This action spawned wide-spread protests that German standards of morality were being exported. Subsequently, CompuServe restored access to most of these newsgroups except to its German subscribers. No action was apparently taken against other access providers based in Germany, so their subscribers could continue to consult this content, if the access provider chose to carry the newsgroup in question. At the latest count, the material is mirrored on 43 web sites and 2 newsgroups and is available from an e-mail listserver (Commission, 1996a). This process of mirroring illustrates the way in which the Internet interprets censorship as damage and routes around it. In another case, a court injunction ordered the removal of a leaked county council report from web sites in England. The result was to 'produce a rash of mirror sites on the Internet, outside the jurisdiction of British courts'. The Council dropped its legal action against the offending site, appearing to concede that it had been counterproductive (Campbell, 1997a). The conclusion that must be drawn is that safe havens, regulatory arbitrage and exit from rule-sets can only be prevented in a situation of globally harmonised regulation.

5 Protecting Minors from Adult Content

The issue which has stimulated the most concrete proposals from the Commission is that of access of children to adult material which may be harmful to their development. The type of content here primarily involves sexual material and violence. All of the key policy statements support the use of filtering and rating, and in particular the PICS system. The Communication, for instance, envisages a Council recommendation 'setting out a clear political message encouraging the use of filtering software such as PICS, and for one or more European rating systems' (Commission, 1996a). Likewise, the Council's Resolution on the issue calls on member states to 'encourage the provision to users of filtering mechanisms and the setting up of rating systems for instance the PICS (Platform for Internet Content Selection) standard' (Council of Ministers, 1997). The other key documents all mirror this stance. Filtering software has been the main technological response to the problem of children accessing 'adult content'. The emphasis the Union has placed on this area reflects, in my view, the sense among policy makers that this is one of the more viable policy instruments on offer. It also reflects disquiet at the amount of pornography available on a medium which represents such an economic and cultural resource.

The Extent of Pornography Online

Yaman Akdeniz, in his study of Internet pornography regulation (1997) outlines the different forms of availability. These range from the pictures, short animated movies, sound files and stories found on the World Wide Web ('WWW') to sex related discussions on the Internet Relay Chat ('IRC') channels where users in small groups or in private channels exchange messages and files (Akdeniz, 1997). There are also Usenet discussion groups devoted to sex, and Wayne Myers (1996) outlines how the Internet can make it possible to see live sex acts and arrange sexual activities from computer screens. While the proportion of web pages containing explicit content

may be very low, in Joel Weinberg's estimation 'an astonishingly small fraction' constituting 'less than a tenth of one per cent' (1997: 1), these pages tend to be well flagged in search engines. The point is, a child only has to search under the first taboo word that comes to mind, in order to access a plethora of adult content. I have noticed in my own researches that fairly innocuous search terms yield copious hits pointing to explicit material (e.g. 'toys', 'love' and ironically, 'PICS'). And while Akdeniz (1997: 3) claims that 'most of the WWW sites with pornographic content require proof of age and payment by credit card to access their materials' my own researches quickly revealed a huge range of free samples and many completely free sites, easily accessible by any minor, and graphically representing every mainstream and 'paraphiliac' category I had known to exist, and some more besides (though thankfully no child pornography).

Filtering Software

The technological response of creating filter software for installation on the computers of end users has been an inevitable attempt to recreate 'gatekeeping' mechanisms that have existed in more traditional media. The global nature of the Internet makes any 'watershed' viewing time impossible. Similarly, there is no gatekeeper analogous to a retailer obliged by law to refuse to sell 'top shelf' materials to minors. Internet filtering software has received wide acclaim as a means of blocking the access of children to content that may be harmful to their development. Plaintiffs in *ACLU v. Reno* (US District Court for the Eastern District of Pennsylvania, 1996) relied heavily on the existence and capabilities of blocking software in arguing that the CDA was unconstitutional, while President Clinton has pledged to 'vigorously support' the development and widespread availability of filtering software, mirroring the European Union position. Free speech activists see such software as providing the answer to the dilemma of indecency regulation,

making it possible 'to reconcile free expression of ideas and appropriate protection for kids' (Daniel Weitzner quoted in Weinberg, 1997: 1).

The European Commission's 'Communication' (1996a) usefully distinguishes three main models of filtering software. These are the 'blacklisting' model, where access to listed sites is blocked; 'white listing', where access is only possible to listed sites; and 'neutral labelling', where sites are labelled or rated, but it is up to the user to decide how to use the label or rating.

The Limits of Blacklisting

The first generation of filter packages generally follow the blacklisting model, and I will argue, suffer from serious shortcomings as a result. Programs such as Cybersitter, Surfwatch and Netnanny rely on blocking access to sites on the blacklist and sites containing certain blacklisted 'strings', that is, keywords. The blacklist in some cases is downloaded and updated online, and is difficult to access. In others the list is accessible in the software's configuration settings. These packages are stand alone systems, which may be purchased and downloaded online. Besides the effort and expense involved for parents, the fact that these programs are not integrated into the web browser means that they can be easily deleted by the precocious minor - unless protected by another program designed to deny access to selected files.

The author has installed one of these packages (Net Nanny) on an experimental basis, and has seen some of these drawbacks exemplified. I accessed just one of Net Nanny's banned sites and discovered it to be a completely innocuous page about skiing. Apparently, some programs block entire directories of web pages because they contain a single 'adult' file (Berlin and Kantor, 1996). This means that large numbers of innocuous Web pages are blocked merely because they are located near some other page with adult content, which probably account for the unfortunate fate of

the skiing page. Some programs block entire domains, including all of the sites hosted by particular Internet service providers (Meeks & McCullagh, 1996).

Another snag arose after my first installation, when I found it impossible to access EU documents of relevance to this thesis. It transpired that 'pornography' itself was a banned word. The only other banned word was 'anarchism'. Apparently vigilant parents must also take into account the private political agendas of software manufacturers when choosing a filter. While with Net Nanny the blacklist of banned words and banned sites is easily accessed, manufacturers of other programs keep theirs highly secret. What arises as a result often amounts to censorship, with no accountability. Cyber Patrol blocked animal-rights web pages because of images of animal abuse, including syphilis-infected monkeys, classing these as 'gross depiction' (Weinberg, 1997: 8; Meeks and McCullagh, 1996). The problem was aggravated by the fact that Cyber Patrol, following the entire-directory approach described above, blocked all of the hundred or so animal welfare, animal rights and vegetarian pages hosted at the Animal Rights Resource Site. Anything remotely connected with homosexuality is liable to be blacklisted by Cyber Patrol, Cyber Sitter and Net Nanny (Weinberg, 1997: 9). Banned directories include ones with 'vital information from the Centers for Disease Control and Prevention, the AIDS Book Review Journal, and AIDS Treatment News' (Meeks and McCullagh, 1996). Weinberg outlines the often 'surprising and alarming' nature of blacklisting. He instances Cyber Patrol's blocking of Usenet newsgroups including alt.feminism, soc.feminism, clari.news.women, soc.support.pregnancy.loss, and alt.support.fat-acceptance. The same program blocks the Web site of the League for Programming Freedom (a group opposing software patents), and the Electronic Frontier Foundation's censorship archive. Cyber Sitter blocks the National Organization of Women web site, and sites which contain the words 'Sinn Fein' (Ó Marcaigh, 1997). Disturbingly, it blocks the site of Peacefire, cyber-rights group run by teenagers, purely on the basis that it contains criticism of CYBER Sitter. The makers of Cybersitter have even threatened

to block every site hosted by the service provider which hosts the Peacefire site (Weinberg, 1997; Ó Marcaigh, 1997). In the words of Meeks and McCullagh (1996), who procured leaked blacklists, '[t]he smut-censors say they're going after porn, but they quietly restrict political speech.'

Other problems arise from the sometimes ridiculous antics of string-recognition software. America Online's software, for example, in seeking to screen four-letter words embedded in text, refused to let users register from the British town of 'Scunthorpe' (Ó Marcaigh, 1997; Weinberg, 1997). The same company, enforcing a rule forbidding certain words in personal member profiles, barred subscribers from identifying themselves as 'breast' cancer survivors (Weinberg, 1997: 15).

The shortcomings in these first generation filtering programs are summed up well by Yaman Akdeniz (1997: 23):

..sometimes this kind of software goes too far away and limits access to or censors inconvenient web sites, or filters potentially educational materials regarding AIDS and drug abuse prevention. Furthermore, the companies creating this software provide no appeal system to the banned content providers, thereby subverting the self-regulating exchange of information that has been a hallmark of the Internet community.

PICS: Neutral Labelling

Contrasting with first generation filtering software, PICS is aimed at providing a standard infrastructure for 'neutral labelling' and filtering Internet content. It separates the two functions of rating of sites and filtering of sites (and, significantly, of individual pages). Praised for allowing a high degree of flexibility and security, PICS is acclaimed by the European Commission as 'undoubtedly the most

comprehensive and innovative solution yet to tackle Internet contents issues.’(Commission, 1996a). PICS tags Internet sites with, in the words of the Commission, ‘value neutral’ labels. The Commission gives an excellent, albeit idealised, account of PICS in operation:

These labels can support different types of information: ratings (for instance, evaluating language, nudity, sexual content, violence), or pointers (identifying contents according to their relevance or interest for various constituencies of users). To be viewed, the site must (1) carry a PICS label, (2) be within the parameters set by parents on the home computer. Ratings can be established by content providers themselves (such as entertainment companies operating family-oriented web sites) or by third parties (such as religious groups or parents’ associations). Each family decides which ratings systems it wishes to use and then, using the parameters, what is acceptable and what is not. (Commission, 1996a).

While PICS can theoretically support different rating systems, any PICS compliant rating system must be rule based. The rating system most frequently associated with PICS, almost to the point of being synonymous is the Recreational Software Advisory Council’s RSACi (i for Internet) system (Akdeniz, 1997:23). Table 5.1 summarises the RSACi system, and it is easy to deduce from it that the correspondence of ‘levels’ with numerical values is the technical key to the PICS. RSACi parameters were originally devised for rating computer games. The PICS protocol, according to the European Parliament ‘would appear to be the most comprehensive and ground-breaking means of dealing with the problems of content on the Internet’. Is PICS capable of living up to the high expectations of its European Union supporters? Below, I will look at some of its inherent limitations, and the obstacles which must be overcome if it is to become a global standard.

Level	Violence	Nudity	Sex	Language
0	No aggressive violence; No natural or accidental violence.	No nudity.	Romance, no sexual activity portrayed.	Inoffensive slang; no profanity
1	Creatures injured or killed; damage to realistic objects	Revealing attire	Passionate kissing	Mild expletives or mild terms for body functions.
2	Humans or creatures injured or killed. Rewards injuring non-threatening creatures	Partial nudity	Clothed sexual touching	Expletives; non-sexual anatomical references
3	Humans injured or killed	Frontal nudity	Non-explicit sexual touching	Strong, vulgar language; obscene gestures; use of epithets.
4	Wanton and gratuitous violence.	Provocative display of frontal nudity	Explicit sexual activity.	Extreme hate speech or crude language. Explicit sexual references

Table 5.1² The Levels and Categories of the RSACi rating system.

Rules and Standards

Jonathan Weinberg has provided the most important scholarly assessment of filtering and rating systems to date (Weinberg, 1997). While viewing such systems as a ‘huge step forward’ he contends that:

² Abstracted by the author from ‘PICS-Version 1.0’ in the <rsaci.rat> file which is installed automatically into the Windows operating system with recent versions of Netscape Navigator and Internet Explorer which incorporate the PICS protocol.

..it is worth trying to locate the technology's limitations and drawbacks. Blocking software is a huge step forward in solving the dilemma of sexually explicit speech on the Net, but it does come at a cost. People whose image of the Net is mediated through blocking software will miss out on worthwhile speech ~ through deliberate exclusion, through inaccuracies in labelling inherent to the filtering process, and through the restriction of unrated sites. (Weinberg, 1997:1)

Weinberg surveys the different types of blocking systems, outlining the distinction between approaches based on 'rules' and those based on 'standards'. PICS may incorporate only rule-based systems such as RSACi. Designers of a PICS compliant system must devise simple, hard-edged rules, with the results 'turning mechanically on a limited number of facts' (Weinberg, 1997:5). According to Weinberg:

Legal thought teaches that rules and standards each have disadvantages. A problem with standards is that they are less constraining; relatively speaking, a standards-based system will lack consistency and predictability... Rules become increasingly necessary as the universe of law-appliers becomes larger, less able to rely on shared culture and values as a guide to applying standards in a relatively consistent and coherent way. (1997:12).

Thus, the W3C and the European Union, in seeking to promote a global standard among heterogeneous cultures is seeking to overcome this diversity through the rule-based PICS. Weinberg affirms this rationale, arguing that with the 'large universe of evaluators' necessary to map the Internet, a ratings system relying too heavily on the standards approach would be prone to great dangers of arbitrariness and inconsistency (Weinberg, 1997:6).

Shortcomings of PICS

Rules-based systems suffer their own shortcomings. In a rule-based system it is impossible to include determinations as to whether nudity is 'artistic', 'erotic', or 'pornographic'. If we consider the categories relating to sexuality in Table 5.1, we see that there is no attempt to distinguish educational materials from other depictions, so that users can allow the former but not the latter (Akdeniz, 1997; Weinberg, 1997). Such classification requires more a more standards based judgement on the part of the evaluator. According to Weinberg rules based systems 'direct law-appliers to treat complex and multifaceted reality according to an oversimplified schematic' (1997:6). In order to simplify a complex inquiry, factors which a sensitive decision maker would otherwise take into account are 'screened off'. At best, a rule-based filtering system can miss nuances; at worst, it can generate absurd results, as in the cases of banned strings described above. As Weinberg explains:

There is no way, consistent with rulishness, that it can seek to distinguish the serious or artistic from the titillating. It achieves rule-boundedness, and ease of administration, at the expense of nuance; it achieves consistent labelling, but in categories that do not correspond to the ones many people want. (1997:7)

The challenge facing ratings system designers is to devise rules-based systems which encompass the complexity of content as well as possible, minimising these difficulties. According to Weinberg the product of any such effort will necessarily be flawed. Other researchers are stronger in their criticism. Jonathan Wallace asks how he is to rate 'An Auschwitz Alphabet', a deeply chilling work of reportage on the Holocaust. The work contains descriptions of violence done to sexual organs of concentration camp inmates. According to Wallace, a self-rating system would force him to choose between the unsatisfactory alternatives of labelling the work as suitable for all ages, on the one hand, or lumping it together 'with the Hot Nude

Women page' on the other. Legal researcher, Yaman Akdeniz raises a similar query concerning his 'Cyber-Rights & Cyber-Liberties' web site, which deals with the regulation of child pornography on the Internet.

How will this site be labelled under the PICS/RSACi initiatives? Hopefully, it is an informative and educational site but sometimes there may be strong language such as in the court cases reported in the newspapers. Some rating authorities may judge the site as an offensive even though it has a public purpose. This is the same for various newsgroups or web sites dealing with serious issues such as sexual abuse and AIDS. (Akdeniz, 1997)

One also thinks of sites depicting human rights abuses. According to Akdeniz, there is no room for dissent in the system because ratings will be done by private bodies rather than by government, leaving an accountability deficit. Such concerns force Akdeniz to conclude that 'further research into this problem may be needed before implementing it as a standard for labelling the Internet content.' (Akdeniz, 1997: 24)

Problems are also encountered in choosing which categories with which to label content. According to Electronic Frontiers Australia (1997), 'the definitions used in determining the four [RSACi] categories were 'clearly chosen with computer games in mind and lack the flexibility required for a wider range of materials. It is ludicrous that such a system should be applied to novels, online libraries, art galleries, and other such resources.' Practicalities demand a limited amount of categories. To keep things manageable, RSACi ignores much content that some other ratings systems class as potentially unsuitable, including speech relating to 'drug use, alcohol, tobacco, gambling, scatology, computer hacking and software piracy, devil worship, religious cults, militant or extremist groups, (and) weapon making...' (Weinberg, 1997). In Weinberg's view, if the Internet is to be rated in a comprehensive manner, fairness and consistency can only be achieved if the ratings system uses simple, hard-

edged categories relying on a few, easily ascertainable characteristics of each site. Any such categories will be inherently value laden, despite the claim of neutral labelling.

Implementation

Compared to the regulation and governance of illegal content, PICS poses very different issues of implementation. No questions concerning liability or intermediaries arise; indeed few legal issues arise. The crux of PICS is the need for universality of rating. As Weinberg explains:

Blocking software can work perfectly only if all sites are rated. Otherwise, the software must either exclude all unrated sites, barring innocuous speech, or allow unrated sites, letting in speech that the user would prefer to exclude. (1997:20).

The most obvious obstacle to be overcome is the sheer scale of content. One solution is to encourage self-rating where evaluators follow a rule bound questionnaire following the categories of the rating system, be it RSACi or whatever. There is the inevitable problem of misrepresentation of sites, which could possibly be dealt with by a citizen hotline reporting mechanism, similar to current hotlines for illegal content. But a far greater problem is that of providing an incentive to rate. According to Weinberg the incentives are highly uneven:

Mass-market commercial providers seeking to maximize their audience reach will participate in any significant self-rating system, so as not to be shut out of homes in which parents have configured their browsers to reject all unrated sites. Many noncommercial site owners, though, may not participate. They may be indifferent to their under-18 visitors... For the owner of large archives containing many documents, supplying a rating for each page may be a time-consuming pain in the neck.

Then there are those I have instanced above who may be philosophically opposed to the rating system. Rating may also involve financial costs (Weinberg, 1997:22). It seems likely that any incentive would be likely to increase as the amount of rated pages reaches a certain critical mass, the point at which parents are happy to leave their browser set at a default setting which excludes unrated pages. But reaching such a point would necessitate mass compliance in the first place. Industry backing has meant that the market leading web browsers now come with PICS/RSACi included. At present, even though most newly installed browsers, my own included, contain the rating system, very few sites are actually rated. The result is that if unrated sites are excluded there is little material to view, even for minors. Allowing access to unrated sites leaves one faced with most of the offending content the system is designed to deal with.

6 Conclusion: Governance in a Global Information Infrastructure

The Network Governance Paradigm

At this point it is worth assessing these policies in the light of the questions raised about governance in the Introduction and in the literature review. To what extent can European Union policy on Internet content be said to bear out the paradigm of 'network governance' described by Reidenberg and others? That paradigm may be summarised as follows. The role of the state is circumscribed in terms of its traditional exclusive sovereignty and regulatory powers in a distinct territory. However the state retains crucial degree of manoeuvring room. In Walker's words 'the fragmentary state can respond to challenges by more imaginative forms of governance'. The state can maintain 'crucial functions in terms of managing the political linkages in governance'. The role of the state is not exclusive; it 'may need further sustenance by the activation of more varied levels of power at second hand'. In Reidenberg's view the state becomes just one element in a 'complex mix of rule-makers'(1997:96):

On the GII governance can no longer be viewed as an exercise in state edict. The relationships among the different participants ...become interactive. States have direct interests ...The Private Sector has a crucial role ...Technologists have a pivotal position ...and the GII empowers citizens to establish rules of their own. (1997: 926)

In this view of governance, policy-making among the different interests referred to is intertwined. It cannot ignore technological concerns and technologically-driven decision making. How are these views borne out in the policies and the policy-making mechanisms we have reviewed? In general terms we have seen that the policy making process in the European Union has been specifically structured with a view to including the commercial and consumer groups involved, through the constitution of the Working Party on illegal and harmful content. In the context of substantive policy on illegal content, the advocacy of a self regulation system involves the key industry players in a central way, through determining codes of conduct. This may be backed up by legislation making intermediaries liable, to different degrees, for the content they carry. However, as I have pointed out above, liability is an issue on which the Union has yet to reach closure. This bears out Reidenberg's suggestion of a 'movement toward a system of state provided incentives through encouragement, as well as allocation of liability, that will induce networks themselves to adopt desirable public policies' (1996, 930). According to this view the allocation of liability might evolve as a policy instrument to promote network self regulation. Beyond the involvement of intermediaries, the advocacy of hotlines and the general promotion of user awareness (the Commission has set up its own awareness site) involves the wider citizenry in enforcement of norms.

Technical Standardisation as Policy Instrument

In the area of harmful content, that is, restricting the access of minors to adult content, the new, wider, concept of governance is even more applicable. Traditional gate keeping mechanisms are rendered inoperable by the technological infrastructure of the new medium, yet it is to technology that the Union has turned in its search for policy instruments. This has involved close alliances with the industry in promoting the PICS protocol as a global standard. The salience of this point is reinforced by the close historical relationship which the European Commission has built with the World

Wide Web Consortium (W3C). This is an international non-profit making association of academics, public interest groups and computer companies which promotes standards and interoperability on the World Wide Web, and also looks at the social consequences of technology (World Wide Web Consortium, 1997). Its key personnel were instrumental in the original development of the Hypertext Transfer Protocol on which the web is based. The Consortium is backed by 39 global computer and communications companies (Akdeniz 1996,1997). Significantly, the European Commission played a role in the establishment of the W3C (Communication) which in turn has been represented on the Commission's Working Party on illegal and harmful content (parts). The Commission is also involved with the W3C in other areas of information policy, as instanced in the WEBCORE project, 'an action undertaken to secure global interoperability and European competitiveness in the Global Information Society' (Commission, 1996?). This confirms Reidenberg's view:

Executive and legislative fora lose a degree of relevance to technical standards organisations. Standards decisions affect fundamental public concerns and are no longer technical rules of purely commercial interest (Reidenberg, 1996: 927).

Reidenberg instances other examples which reflect 'the critical new instrumentality of standards-setting', including encryption standards, as outlined above. PICS is technical standardisation as policy instrument par excellence. The broadness of the range of the alliances involved is underlined by the fact that arch rivals Netscape and Microsoft, who together account for over 95% of the web browser market have both adopted the new protocol. CompuServe, a service and content provider which more than any other has contested heavy handed regulation has announced its support for PICS and now rates its own content using RSACi. However many obstacles must be overcome before the W3C attains its goal of having PICS as a global standard. According to Akdeniz (1997), the consortium expected 80 per cent of information on the Internet to be rated

by the end of 1997. The reality, as we have seen, is that rating is a minority enterprise at present. Other problems may also arise. While PICS is often taken to mean the RSACi system, it is in reality a platform that can support any rule based rating system. To this extent PICS is value-free. The idea of using a distinct 'European' rating has been mooted by the Commission (1996a), but RSACi seems to have a head start in the race to become the default system. IT is RSACi which has been incorporated into browsers. One may apply a market rationale to the way in which one technical standard comes to dominate exclusively (Gates, 1996). This has been the case for instance with VHS versus Betamax video systems, numerous audio standards, and the 'QWERTY' keyboard I am using to write this. Thus, in advocating PICS, the European Union may be pushing a particular (non value free) rating system by default. It is also worth noting RSACi is a proprietary system. While the RSAC is a non profit making organisation charges for those who wish to rate with its system are envisaged to be in place soon. I have already related in chapter 4 how the details of rating are likely to be presented to the council of Ministers as *fait accompli*. This all raises issues of accountability, for technical standardisation obscures the moral issues at stake. As Reidenberg notes: '...citizen interests are either weakly or indirectly represented in setting standards. In the European context, the involvement is indirect, but real, in the shape of the Commission's involvement with the W3C.

The Commission also shows itself to be keenly aware of the potential of technical standardisation as a policy instrument in the context of illegal content:

Attention should be paid to the process by which technical standards for digital communication are adopted since the design of such standards may affect the possibilities of law-enforcement bodies to track criminal activities. (Commission, 1996c)

Another potential, though not explored by the Commission, is inherent in the PICS protocol. While PICS allows filtering of content by the end user, it also enables filtering at the nexus of the service provider. This may become a relevant possibility if rated content becomes predominant on the World Wide Web. This would allow PICS to go beyond the goal of restricting the access of minors to adult content, and block public access in general to certain sites.

Co-operation beyond Europe

It is hoped that the foregoing chapters illustrate the limits of sub-global approaches to dealing with controversial Internet content. However any project of instituting instruments of governance on a global scale poses serious challenges. The need for international co-operation is asserted in many of the European Union's policy statements, yet there is a lack of consensus as to which international forum or fora would be appropriate to such an enterprise. The Green Paper (Commission, 1996b) asks the question for us:

What should the priorities be at European level and at international level? In particular, should one give priority to developing solutions at European Union level and then promoting them at international level or should this be done in parallel? What are the most appropriate international fora for international co-operation (G7, OECD, ITU [International Telecommunications union], WTO, UN or bilateral relations) ? How should this international co-operation be formalised?

Both the Commission's Communication and the Parliaments Resolution offer a similar list of international organisations in the search for new international legal instruments. The list of organisations in the question above is interesting if we remember the role of economic interests in this policy process. The first two, the G7

and the OECD are organisations of the dominant powers of global capitalism, primarily concerned with furthering economic growth. The World Trade Organisation (WTO) is also specifically concerned with economic issues, namely the regulation of free trade. The International Telecommunications Union (ITU) is concerned with technical standards, which, in the information age, are an issue of key economic interest. Only the UN has a brief which extends to human, civil and political rights, and moreover, has a make up that is in some sense global, and possesses institutions, albeit limited, which can provide a discourse convivial to the provision of accountability to the world's citizens. The Commission's Legal Advisory Board sounds a note of caution in the face of approaches which economic and technical issues and calls for a choice of forum more clearly focused on the rights of citizens:

The progress already achieved in Europe in building a consensus must be built upon in the broader international context. A note of caution, however, seems to be warranted. Similarly to the debate on privacy protection, international discussions should bear in mind that an issue is being discussed which although having obvious economic implications is mainly an issue of the effectiveness of human rights, cultural values and balances between state authority and citizens' rights and interactions among the rights of citizens. Not all international fora lend themselves equally well to adequately discussing such issues. (Legal Advisory Board, 1997, 9)

However, if we consider the question of implementation and enforcement, there is perhaps some case to be made for organisations with an economic purview. Since it has been argued above that economic interests are crucial in determining the policies of governments, the sanctions imposed by, say, the WTO may prove an incentive for

nations to comply with any international accord. Conor O' Cleary (1996) postulates a link between China's regulation of the Internet - in this case towards liberalisation - with such economic imperatives.

The action [deregulation of the Internet] coincides with new thinking in Beijing on making the economy more open to strengthen China's case for joining the World Trade Organisation. At the weekend, the official media published details of new trade initiatives as part of its drive for WTO entry.

The question as to which forum is an appropriate one in which to seek international accord remains open in all of the European Union's key policy statements. The Parliaments Report (Report, point 31) urges avoidance of duplication of efforts. A lack of closure on the issue will surely have a diffusive effect.

Any international agreement faces the challenge of the tendency towards a lowest common denominator, a process already noted in the European context. The recent US Supreme Court decision ruling the CDA unconstitutional points to an important limiting factor. The Freedom of speech provisions of the American constitution's First Amendment are less qualified than those of the European Convention on Human Rights as set out in Chapter 3 above. With the US being such a strong political power and still the location of the 'core' of the Internet, this is likely to have a large impact on the unfolding search for international accord.

The Challenge of the Global - A Speculation about Statehood

As I argued above, the Internet represents one element in the growing phenomenon of globalisation. Increased economic interdependencies, global ecological crisis and the GII are creating the need for new forms of governance which can encompass a large portion of the planet's polities. It has been argued above that responses to regulatory problems posed by the Internet are yielding a new form of governance. It is worth posing the question as to whether in addition to a new definition of governance, a new concept of statehood will also be needed for the future. The traditional equation of statehood with the monopoly of coercive power over a distinct territory (Weber, Elias) reaches its own limits in an era of increasingly complex global governance. For instance, sovereignty in the economic arena, it could be argued, is actually shared with powers beyond the national realm, and more specifically with international monetary institutions. In areas of civil conflict, there has been an increasing role for internationally sponsored organisations, backed up, of course, by the coercive powers of hegemonic nations. However the development of global institutions remains limited in certain important respects and there are no indications of moves toward the type of relatively deep sovereignty sharing such as we have seen in the European Union. And crucially, the concept of global civil rights is just that, a concept. There is no sign of the a development emulating the faltering, yet real, expansion of European citizenship. Conventions are agreed between nations and it is up to nations to comply and enforce them.

The realisation of stronger global institutions would require such changes in political identity as can only happen through major shifts in cultural world views (Dunne, 1997). Ironically, the GII may contribute to just such a shift. We have seen how Kedsie's argument (1996, 1997) that the Internet is contributing to the development of a global civil society. This echoes the insights of Jürgen Habermas who points to the development of a world-wide communicative arena:

State citizenship and world citizenship form a continuum which already shows itself, at least, in outline form. (Habermas, 1992).

The Internet may represent a renovation of Habermas's 'public sphere'(1991) and its expansion beyond traditional boundaries.

Ken Wilber (1995) makes a complex argument in which global federation and a new informational 'base' to society are inherently linked, the latter making the pre-requisite shift in world-views possible. The argument for geo-political evolution towards global federation is supported by the process sociology (Elias, 1982; Mennell, 1992). Norbert Elias' survey (1982) of the development of statehood in a long-term historical context suggests a momentum towards ever larger units of territories controlled by a single coercive institution, and ever larger 'survival units' culminating in some form of global state. While it is, no doubt, early to speculate, it is worth considering whether the developments I have been describing, and other recent developments in geo-politics conform to this pattern.

A wider historical context also leads, in my view, to the interesting issues involved in state development. In the older nation states of Europe a pattern may be discerned of a widening remit for the state, expanding from core areas of sovereignty (defence, coercion) into the spheres of civil, and then political and welfare rights. However, the development of supranational statehood in the European Union does not yet conform to this pattern (Streeck and Schmitter, 1992:152-152). A minimalist liberal state would seem a better description of the European polity. This combination of economic integration and deregulation with a high level of civil rights is worth noting in the context of this study. It is interesting to speculate whether or not the European Union is an indicative pattern for supranational sovereignty sharing and predictive of global developments in issues both of economy and rights.

In the development of modes of governance for the Internet technical, political and economic interests are enmeshed. In cyberspace the traditional congruence of functionality, identity and territory (Laffan, 1996) which has rendered the state so potent meets an awesome challenge. We can only begin to speculate upon the ultimate implications of this meeting.

References

- Adonis, Andrew and Patrick Wintour 1997. 'Britain to get tough on laws on privacy', *The Observer*, Sunday, July 27 1997.
- Akdeniz, Yaman 1997. 'The Regulation of Pornography and Child Pornography on the Internet', *The Journal of Information, Law and Technology* Available at HTTP: http://elj.warwick.ac.uk/jilt/internet/97_1akdz/default.htm [1997, July 6]
- 1996. 'Pornography on the Internet', *La Lettre de L'Internet Juridique (June 1996)* Available at HTTP: <http://www.argia.fr/lij/english/ArticleJuin11.html> [1997, June 22]
- Anderson, Robert et al. 1996. *Universal Access to E-Mail: Feasibility and Societal Implications*. Santa Monica, CA: Rand.
- Berlin, E. and A. Kantor 1996. 'Who Will Watch the Watchmen?' Available at HTTP: <http://www.iw.com/current/feature3.html> [1997, August 2]
- Bird, David 1996. X*E*M*U: *Censorship web-page*. Available at HTTP: xemu.demon.co.uk/eu_green_nccl.htm [1997, August 10]
- Campbell, Duncan 1997a. 'Net ties up Notts', *The Guardian*, Thursday, July 31 1997.
- 1997b. 'Screw the Internet', *The Guardian*, Thursday, September 13 1997.
- 1997c. 'Europe spikes spooks' E-mail eavesdrop bid', *The Guardian*, Thursday, October 16 1997.
- Clinton, William 1996. *Statement by the President, June 12, 1996*. Available at HTTP: http://www.eff.org/pub/Legal/Cases/EFF_ACLU_v_DoJ/960612_clinton_cda_decision.statement [1997, July 1]
- Commission of the European Communities 1997. 'Ensuring Security and Trust in Electronic Communication.'. Available at HTTP: <http://www.ispo.cec.be/eif/policy/97503.html> [1997, June 30]

- 1996a. *Illegal and Harmful Content on the Internet (Communication)* Brussels, 16 October 1996: Com (96) 487. Available at HTTP:
<http://www2.echo.lu/legal/en/internet/content/communic.html> [1997, June 29]
- 1996b. *'Green Paper On The Protection Of Minors And Human Dignity In Audiovisual And Information Services* Brussels, 16 October 1996: Com (96) 483. Available at
 HTTP:<http://www2.echo.lu/legal/en/internet/content/gpen-toc.html> [1997, June 28]
- 1996c. *Working Party Report: 'Illegal and Harmful Content on the Internet'*. Available at HTTP:<http://www2.echo.lu/legal/en/internet/content/wpen.html> [1997, July 2]
- 1996d. *List of Participants*. Available at
 HTTP:<http://www2.echo.lu/legal/en/internet/content/presence.htm> [1997, July 2]
- 1996e. *Communication From The Commission To The Council And The Parliament On 'Standardization And The Global Information Society: The European Approach'* Brussels, 24 July 1996: Com (96) 359.
- Council of Europe 1993. *European Conventions and Agreements, Vol 1: 1949-1961*.
 Strasbourg: Council of Europe.
- Council of Ministers 1997. *Resolution adopted at the Telecommunications Council of 17 February 1997* OJ C70 6.3.97 p 1. Available at
 HTTP:<http://www2.echo.lu/legal/en/internet/content/resol.html> [1997, June 20]
- Cunningham, Michael 1996. 'US judges' block on Internet `indecency' ban likely to have reverberations', *The Irish Times, Thursday, June 13, 1996*.
- den Boer, Monica 1996. 'Justice and Home Affairs: attachment without integration', in *Wallace and Wallace (eds), pp 389-410*.
- Dunne, Daniel 1997. *'Political Identity in the European Union'*. Available at
 HTTP:<http://www.geocities.com/Paris/Metro/5427/polii.html> [1997, October 1]
- Elias, Norbert 1982. *The Civilizing Process (trans. Edmund Jephcott) Vol. 2: State Formation and Civilization*. Oxford: Blackwell.
- Encyclopaedia Britannica 1997. *'The Internet'*.

- European Commission Legal Advisory Board 1997. *Response to the Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services*. Available at [HTTP:http://www.echo.lu/legal/en/internet/gplabreply.html](http://www.echo.lu/legal/en/internet/gplabreply.html) [1997, July 10]
- European Parliament 1997. *Resolution on the Commission communication on illegal and harmful content on the Internet (COM(96)0487 - C4-0592/96)*. Available at [HTTP:http://www.europarl.eu.int/dg1/a4/en/a4-97/a4-0098.htm](http://www.europarl.eu.int/dg1/a4/en/a4-97/a4-0098.htm) [1997, August 16]
- Froomkin, A. Michael 1997. 'The Internet As A Source Of Regulatory Arbitrage', in *Kahin and Neeson (Eds) 1997* Available at [HTTP: http://www.law.miami.edu/~froomkin/arbitr.htm](http://www.law.miami.edu/~froomkin/arbitr.htm) [1997, June 19]
- Gates, William 1996. *The Road Ahead (2nd ed.)*. London: Penguin.
- Habermas, Jürgen 1992. 'Citizenship and National Identity: Some Reflections on the Future of Europe', *Praxis International*, vol. 12, no. 1, pp. 1 - 19.
- 1991. *The Structural Transformation of the Public Sphere*. Cambridge, MA: MIT Press.
- Hass, Ernst 1958. *The Uniting of Europe: Political, Social and Economic Forces 1950-1957*. London: Stevens and Son.
- Huntington, Samuel 1991a. *The Third Wave: Democratisation in the Late Twentieth Century*. Norman, OK: University of Oklahoma Press.
- 1991b. 'Democracy's Third Wave', *Journal of Democracy*, 2, no. 2 (Spring):12-34.
- Jessop, Robert 1994. 'Post-Fordism and the State' in Amin (ed), *Post-Fordism*.
- Johnson, David and David Post 1997a. 'The Rise of Law on the Global Network', in *Kahin and Neeson (Eds) 1997*.
- 1997b. 'The New Civic Virtue of the Net: A Complex Systems Model for the Governance of Cyberspace', In *Coordination of the Internet*, Brian Kahin and James Kellers (eds.), MIT Press, 1997 (forthcoming).
- Kahin, Brian and Charles Neeson (Eds) 1997. *Borders in Cyberspace: Information Policy and the Global Information Infrastructure*. New York: M. I. T. Press.
- Kapteyn, P. 1995. *The Stateless Market: The European Dilemma of Integration and Civilization*. London: Routledge.

- Kaspersen, Henrik 1996. 'Liability of providers of the electronic highway'. Available at
[HTTP:http://www.echo.lu/legal/en/converge/960430/kaspers.html](http://www.echo.lu/legal/en/converge/960430/kaspers.html) [1997, July 1]
- Kedzie, Christopher 1997. 'The Third Waves', in *Kahin and Neeson (Eds) 1997*.
- 1996. 'International Implications for Global Democratization' in, *Anderson et al. 1996* Available at HTTP:
<http://www.rand.org/publications/MR/MR650/mr650.ch6/ch6.html> [1997, June 2]
- Laffan, Brigid 1996. The Politics of Identity and Political Order in Europe, *Journal of Common Market Studies. Vol. 34, No.1.*
- Loader, Brian 1997. *The Governance of Cyberspace*. London: Routledge.
- Mayer-Schönberger, Victor and Tere Foster 1997. 'A Regulatory Web: Free Speech and the Global Information Infrastructure', in *Kahin and Neeson (Eds) 1997*.
- Meeks, Brock and Declan McCullagh 1996. 'Jacking In from the 'Keys to the Kingdom' Port', *Cyberwire Dispatch*. Available at HTTP:
http://www.eff.org/pub/Publications/Declan_McCullagh/cwd.keys.to.the.kingdom.0796.article [1997, August 8]
- Mennell, Stephen 1992. *Norbert Elias, An Introduction*. Oxford: Blackwell.
- Myers, Wayne 1996. 'Fun.nl - Live Sex on the Internet', *Wired UK, 1996, 2.10, 50-56*.
- O' Cleary, Conor 1996. 'Blocks on Internet super highway quietly lifted', *The Irish Times, Tuesday, December 17, 1996*.
- Ó Marcaigh, Fiachra 1997. 'Someone who'll watch over me', *The Irish Times, Monday, March 10, 1997*.
- Perritt, Henry 1997. 'Jurisdiction in Cyberspace: The Role of Intermediaries', in *Kahin and Neeson (Eds) 1997* Available at HTTP:
<http://www.law.vill.edu/harvard/article/harv96k.htm> [1997, June 17]
- 1996. *Law and the Information Superhighway*. New York: John Wiley and Sons.
- 1995. 'What is the Internet?' Available at HTTP: <http://ming.law.vill.edu> [1997, June 1]

- Post, David 1995. 'Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace', *Journal of Online Law*. Available at HTTP: <http://www.law.cornell.edu/jol/jol.table.html> [1997, July 21]
- Reidenberg, Joel 1996. 'Governing Networks and Rulemaking in Cyberspace.', *Emory Law Review*, Vol 45. No.3, Summer 1996, pp 912-930.
- Rhodes, Rod 1994. 'The Hollowing Out of the State: The Changing Nature of the Public Service in Britain', *Political Quarterly* 65.
- Saxby, Steven 1996. 'Public Policy and Regulation of the Information Market in the Digital Network Environment' (PhD Thesis), *Complex* 2/96.
- 1990. *The Age of Information*. New York: Macmillan/New York University Press.
- Smyth, Patrick 1996. 'Mitchell Argues for World Wide Register of Paedophiles', *Irish Times* (Dublin), April 26, 1996.
- Streeck, Wolfgang and Philippe Schmitter 1991. 'From National Corporatism to Transnational Pluralism: Organised Interests in the Single European Market', *Politics and Society* 19, no.2 (1991) 133-164.
- Toffler, Alvin 1980. *The Third Wave*. New York: Bantam Books.
- The Treaty on European Union 1992. O.J. (C 224) 1 (Feb. 7 1992).
- US District Court for the Eastern District of Pennsylvania 1996. *ACLU vs Reno*, Civil Action No. 96-963 (E.D. Pa. June 11, 1996). Available at [HTTP:http://www.aclu.org/court/cdadec.html](http://www.aclu.org/court/cdadec.html) [1997, July 4]
- Walker, Clive 1997. Cyber-Contempt: Fair Trials and the Internet, *Yearbook of Media and Entertainment Law 1997* (Forthcoming).
- 1996. 'Fundamental Rights, Fair Trials and the New Audio-Visual Sector', *Modern Law Review* 59, 4, 517-539.
- Wallace, Helen and William Wallace (Eds.) 1996. *Policy-Making in the European Union*. Oxford: Oxford University Press.
- Wallace, Jonathan and Mark Mangan 1997. *Sex, Laws and Cyberspace*. New York: 1997 Henry Holt and Company.

- Weinberg, Jonathan 1997. 'Rating the Net', *Hastings Communication and Entertainment Law Journal* 453 (1997).
- Whine, Michael 1997. 'The Far Right on the Internet', in *Loader, Brian* 1997.
- Wilber, Ken 1995. *Sex, Ecology, Spirituality*. Boston: Shambhala.
- World Wide Web Consortium 1997. *Joint W3 Initiative*. Available at
[HTTP:http://www.w3.org/Consortium/Prospectus/Hosts.html](http://www.w3.org/Consortium/Prospectus/Hosts.html) [1997, September 16]
- Wriston, Walter 1992. *The Twilight of Sovereignty*. New York: Scribner.