

Controlling the Net: European approaches to content and access regulation

Louise Cooke

Department of Information Science, Loughborough University, Loughborough, UK

Correspondence to: Dr. Louise Cooke, Department of Information Science, Loughborough University, Loughborough, Leics. LE11 3TU. Email: l.cooke@lboro.ac.uk

Abstract.

Organisations, national governments and supranational bodies have all been active in formulating measures to regulate access to Internet content. This paper reports the findings of a documentary analysis of such measures adopted over a ten year period by the European Union. The investigation took place from a perspective of concern for the potential impact on freedom of expression and freedom of enquiry of such initiatives. On a theoretical level, the study adopted Lessig's models of direct and indirect regulation as an analytical framework. The Habermasian concept of the erosion of the public sphere was used as an analogy for the issues posed by the regulation of speech on the Internet. It is argued that the findings of the study suggest that the democratising potential of the Internet is indeed being constrained by measures imposed in an attempt to control the perceived dangers posed by the medium.

Keywords: Content regulation; European Union; policy studies; freedom of expression; Habermas; public sphere.

1. Introduction

Although much has been written about restrictive measures being adopted by more overtly authoritarian regimes such as China, with the intention of regulating and controlling 'dubious' content on the Internet, and its potential

for misuse (see, for example, [1,2,3,4,5] among many others), less attention has been paid to the approaches of Western democratic governments and institutions. This paper aims to redress this balance by reporting the findings of research into policy measures intended to control and regulate access to illegal, 'harmful', 'undesirable' or 'inappropriate' Internet content that were adopted and implemented by the European Union over a ten-year period (1996 to 2005 inclusive). A central aim of the research was to determine what effects, if any, such measures were having on freedom of expression and freedom of access to information on the Internet, using the Habermasian concept of the erosion of the Public Sphere as an analogy to any identified detrimental impact. From a methodological and theoretical viewpoint, the study aimed to evaluate the usefulness of the regulatory models proposed by Lessig [6] as a heuristic device to explore complex areas of information policy formulation.

2. A note on scope and methodology

The policy monitoring was conducted through documentary analysis of both hard copy and electronic primary and secondary sources. This included retrospective analysis from 1996 onwards through to the end of 2005, thus providing a longitudinal insight into shifts in policy emphases over this period. Although there was much pertinent legislative activity taking place in this arena in the US during the same period, analysis of this activity warrants study in its own right and here only brief reference is made to such developments as have impacted on European contexts. Similarly, although there are many other aspects of information policy that impact on the freedom of an individual to access information on the Internet (such as data protection, copyright and privacy) as well as other potential barriers to use such as lack of network infrastructure or access to computer facilities, the monitoring concentrated on policy that specifically aimed to regulate access to illegal, offensive or harmful Internet content.

The analysis relied on data derived from primary and secondary documentary sources. Although it is recognised that a greater insight into the processes and debates behind decision-making and the competing perspectives of different stakeholders in the arena would have resulted from using a broader range of methods such as interviews, and observation, the scope of this study precluded the use of such methods. It is suggested that the significance of the issue to information professionals, and to the wider society, would render this an appropriate area for such research to be carried out in the future.

From a methodological point of view, Rowlands [7] asserts the need for more 'value-critical' and 'paradigm-critical' approaches towards information policy research, and, together with Turner [8] identified the potential for research into the interaction and impact of different theoretical models in an information policy context. In response to this appeal, analysis of the study's findings used Lessig's regulatory models [6] as an interpretative framework to inform the analysis, thus extending our understanding of their potential application to the information policy arena.

Controlling the Net: European approaches to content and access regulation

3. Rationale – a virtual Public Sphere?

...we must not think to make a staple commodity of all the knowledge in the land, to mark and license it like our broad-cloth and our woolpacks. [9]

The Internet is now exerting a significant impact on global patterns of access to information, education, commerce and entertainment. It has been categorised alternately as a neo-utopian liberating force facilitating the expression of alternative and dissenting speech; or as a dystopian space that is responsible for an increased atomisation and fragmentation of modern societies. It is suggested here that it offers a forum with the potential to repair, at least in part, the erosion of the public sphere (Öffentlichkeit) identified in an earlier epoch by Habermas [10]. According to Habermas, this erosion has led to a reduction in the rational discussion of public affairs that once enabled democratic decision-making to take place. This decline and distortion can be attributed to factors such as an increasing manipulation of information by the media, political ‘spin doctors’, technocratic ‘experts’ and commercial advertising. The extension of the role of the State, and the trend towards an increasing legal regulation of private life (Verrechtlichung) has also brought about restrictions on the freedom of the individual [11]. These trends towards increased information manipulation and intervention by the State into areas of personal behaviour and well-being (see [12], chapter 5 on bio-politics for further discussion) can be seen to be continuing – and even gathering pace – in the twenty-first Century. The potential remedy to this situation, according to Habermas, lay in the development and promotion of ‘ideal speech’ situations in which there is genuine equality of participation in the analysis of social problems and public policy decision-making leading to the attainment of the most favourable policy outcomes for society.

With regard to the Internet, the moral panic [13] that has characterised its portrayal by the media, the resulting high levels of public anxiety and the very real dangers posed by its use to perpetrate a range of criminal activities, have all led to a range of measures on the part of international organisations, governments and institutions. It was hypothesised that these measures are, at least in part, preventing the full democratic and informational potential of the Internet from being realised, and are limiting its effectiveness as a forum for rational debate and the free expression of ‘viewpoint diversity’ [14].

Many writers have recognised that the introduction of new technologies tends to be accompanied by a desire on the part of public authorities to control and regulate their use and access to them (for example, see [15,16,17,18,19,20]). The invention of the moveable type printing press is a good illustration of this tendency. As the Internet permeated beyond its military and research-led origins and came to be used as a primary communications medium and information source, as well as a means of recreation, in universities, libraries, schools, the workplace and private homes, the same desire for regulation could be witnessed. However, the control of Internet content and access presents very particular difficulties, as content transcends national boundaries and legislative jurisdictions. Attempts to define illegal or offensive content inevitably encounter problems due to differing cultural values and norms, as well as different legislative regimes. Technical solutions,

originally hailed as offering the solution to the ‘problem’ of Internet control, have evidenced serious – and seemingly insurmountable – limitations and shortcomings. Despite these difficulties, concern on the part of governments, corporations, the media and individuals regarding the availability and dissemination of offensive, harmful, potentially libellous and illegal content on the Internet has led to the adoption of a number of policy measures at institutional, national and international levels, with the expressed intention of monitoring and controlling access to, and dissemination of, such content.

3.1. *The Internet and freedom of expression*

Although the most rapid growth in Internet use in recent years has been in the area of business use (for example, the value of Internet sales grew by 81% from £39.3 billion to £71.1 billion in the year from 2003 to 2004 [21]), and the medium’s popularity for communication and recreation has extended worldwide, its education and research driven origins continue to exert a strong influence on its use and content. Moreover, the unplanned – some would even say anarchistic – origins of the Internet led to its early characterisation as a forum for individualism and the free expression of alternative or controversial content, ranging from unorthodox political expression through to pornographic and obscene matter. New Web-enabled communications and collaboration media such as blogs and wikis offer the potential for individuals to promote their own message on a global scale. Today, despite the ‘unrelenting commercialisation’ of the Web, and the concomitant influence that this exerts on Internet content, Ebersole [22, p.537] comments that the Web ‘remains the least regulated of all mass media’. Jordan [23, p.3] has noted the egalitarian potential of the Internet, commenting that ‘in cyberspace no one can be silenced because their voice is the quietest, and no one can be heard with more effect simply because they are more aggressive’. As long ago as 1965, Arthur C. Clarke was giving poetic expression to a utopian vision of the liberating potential of new communications technologies:

The advent of communications satellites will mean the end of the present barriers to the free flow of information; no dictatorship can build a wall high enough to stop its citizens listening to the voices from the stars. [24]

Castells [25,26] gave early recognition to the potential of the Internet as a tool for democracy. He noted [25, pp.350-351] that

...online information access and computer-mediated communication facilitate the diffusion and retrieval of information, and offer possibilities for interaction and debate in an autonomous, electronic forum, bypassing the control of the media...More importantly, citizens could form, and are forming, their own political and ideological constellations, circumventing established political structures, thus creating a flexible, adaptable political field.

Controlling the Net: European approaches to content and access regulation

A highly significant factor in determining the future development and culture of the Internet was the decision by Berners-Lee not to patent the Web; his vision of the Web was 'a global space where people could share information, ideas and goods, unfettered by any central body' [27]. In the early days of the Web, Laudon [28, p.36] commented that:

Among Internet aficionados there is a strong libertarian ethic that argues that individuals should be able to 'do what they want, when they want' and that the collective social welfare is advanced by the pursuit of a kind of minimally organized anarchy.

However, he also conceded that, when carried to an extreme, such an approach risks turning into 'an amoral free-for-all with no connection to the collective social welfare' [28, p.36]. Such fears, combined with intensive media reporting in which the Internet was portrayed as almost synonymous with pornography, soon led to strenuous calls for regulation of Internet content. In addition, from the early optimistic notions of the Internet as a virtual marketplace of ideas and opinions, 'marketplace' being used in the classical sense of an open public forum (agora), it has become a literal marketplace, where business corporations rely on a secure, 'decent' and non-controversial environment. Such pressures have led to demands for legislation and the development of a variety of non-legislative control techniques to regulate the Internet.

Wall [29] has referred to these competing perspectives that favour either a hands-off approach or stronger controls as being those of the 'cyber-liberators' versus those of the 'cyber-regulators'. Likewise Castells [26] maintains that the Internet has evolved into what he describes as a 'contested terrain' between the contrasting paradigms of freedom and regulation.

3.2. Measures to regulate Internet access and content

A variety of methods of restraint and control have developed in response to concerns about the potential impact of access to 'unacceptable' Internet content, and fears on the part of public access providers, Internet Service Providers (ISPs) and network administrators with regard to their potential legal liability. Such measures include the development and implementation of filtering, monitoring and ratings technologies; metadata schemes for describing and organising Internet resources; Acceptable Use Policies (AUPs) and Codes of Conduct governing network use within institutions and organisations; user education to promote appropriate use of facilities; and requirements for users to sign disclaimers limiting the legal liabilities of access providers.

3.2.1 A technological fix?

From the time of the initial moral panic concerning the Internet, it has often been suggested that the control of Internet content and problems of access to 'inappropriate' content would be resolved through the implementation of technical solutions, in particular the use of filtering software [see, for example, 30, 31, 32]. In the US a number of legislative initiatives have been put forward in attempts to mandate the implementation of filtering software, in

particular with regard to public access to the Internet in schools and libraries. Many private corporations and public sector organisations have also adopted Internet filtering and monitoring software with enthusiasm as a means of avoiding time-wasting by employees and reducing the risk of legal liability for their communications [33].

However, such software has demonstrated considerable technical limitations and its potential impact on freedom of expression and freedom of enquiry has been questioned. Although it has been argued that the installation of filtering software affords greater control to the end user over access to content and balances the right to freedom of expression with some hypothetical right not to have to encounter offensive material [30, 32, 34], this perspective has been subject to much debate and challenge, not least on account of the lack of context sensitivity of many of the products, their potential for bias and the lack of transparency of the process that determines blocking decisions by software providers.

Thus, Lasica [35] for example, puts forward arguments against the use of filtering software, quoting David Sobel of the Electronic Privacy Information Center (EPIC), who defines the use of such software as ‘a move towards the privatising of censorship’. He expresses concern that filters are too subjective and constitute a threat to freedom of speech, screening out ‘much more than smut’ such as information on alternative lifestyles, family planning, atheism, feminism and women’s organisations, animal rights groups, political organisations, safe sex and drug use. An example of evidence of bias in the selection of sites blocked by CyberPatrol, a popular filtering software package, was demonstrated by a student who reverse-engineered the software to enable him to access the list of sites blocked by the software. He found that the list included sites critical of CyberPatrol and its parent company, as well as a website for the left-wing magazine *Mother Jones* [36]. Meanwhile, an EPIC report of 2001 [37] concluded that filtering and rating systems, far from being mere software features or tools, can be considered to constitute ‘fundamental architectural changes that facilitate the suppression of speech far more effectively than national laws alone ever could’ (see [38] for further debate on this point).

The potential issues arising from the technical imperfections and limitations of filtering technologies, and the difficulties encountered in arriving at a universal definition of ‘acceptable’ content that is nevertheless sensitive to the norms of local community standards, are significant. Apart from the potential impact on individual freedoms of over-blocking that the implementation of filtering software may incur, concerns have also been expressed with regard to the false complacency that may result from its use. Parents, librarians and teachers may be led to adopt a misplaced sense of security, putting too much reliance on filters rather than personal supervision to prevent children from accessing content that they consider harmful.

However, not all forms of filtering work on the basis of excluding resources; recommender systems use evaluation of resources to ‘select in’ those that meet certain specified criteria [39]. Both selection and exclusion filtering rely on metadata to facilitate the rating and labelling of content in order to aid the end user in making a decision about the suitability of a particular resource. Labelling is a means of identifying the contents of an

Controlling the Net: European approaches to content and access regulation

electronic data file without having to open it, the label providing the user with enough information to decide whether to open it, whereas rating involves assigning a value to the data file, based on defined assumptions or criteria. Filtering can be carried out on the basis of selecting or excluding files as a result of the rating assigned to them.

Despite the theoretical ability of rating and labelling schemes to transfer greater control to end users over their own access to electronic resources, the American Civil Liberties Union (ACLU) is one of many bodies that have strongly criticised the long-term implications of Internet rating schemes. The ACLU, in particular, suggests that the wide-scale deployment of such schemes will lead to the Internet becoming 'bland and homogenized' [40]. More worryingly, they maintain that they are 'open to abuse by governments eager to censor and control information'. This argument is also put forward by Lessig [6] who suggests that labelling schemes offer a potential for invisible 'upstream' filtering and a lack of transparency in restrictions to information access. This is a crucial point, as it raises the issue of the point in the flow of information at which censorship takes place, and with whom the responsibility for regulatory decisions should rest: is this ultimately the role of government, of content providers, of ISPs, or of the end user? This also invokes the issue of transparency of decision-making and the imposition of restrictions, as will be discussed in section 3.3 below with reference to Lessig's regulatory models. Again, this is a crucial issue as a lack of transparency in decisions to censor invalidates the end user's ability to challenge such decisions.

Lessig (among several others: see [41], for example) also makes a strong case against 'perfect filtering', even if the technology allows this to take place. If rating and labelling schemes do permit us accurately to screen out undesirable content, society may be the poorer because we never have to 'confront the unfiltered', for example issues of poverty and inequality elsewhere in the world [6, p.180]. Stoker, who applies such an argument to the use of filters in an academic environment, comments that it is not part of the role of a University to deliberately shield its students from 'some of the more unpleasant features of life' [42, p.4]. Shapiro [43] notes that filtering allows us to avoid information that leads to 'cognitive dissonance' by confronting us with challenging or uncomfortable facts ("freedom from speech"). This in turn means that, instead of re-evaluating our own beliefs and behaviours in the light of new evidence, we 'would likely become self-satisfied and unchallenged, lacking motivation or curiosity' [43, p.111]. Even the World Wide Web Consortium (W3C) have noted the dangers of any one labelling standard becoming too powerful: 'If a lot of people use a particular organisation's labels for filtering, that organisation will indeed wield a lot of power. Such an organisation could, for example, arbitrarily assign negative labels to materials from its commercial or political competitors' [cited in 19, p.227].

3.3. Direct and indirect regulation: the models of Lawrence Lessig

Lessig proposes the notion that cyberspace is unquestionably a closely regulated sphere, subject to four specific modalities of regulation: those of architecture, law, the market and social norms [6,44]. These modalities do not act in isolation of each other, but instead interact and compete with each other. The “net regulation” to which cyberspace is subject, is equivalent to the impact of the regulatory effects of all four modalities taken as a whole. These are visualised in his model of direct regulation to illustrate the way in which this combination of forces acts to constrain and regulate information flows on the Internet, as shown in Figure 1.

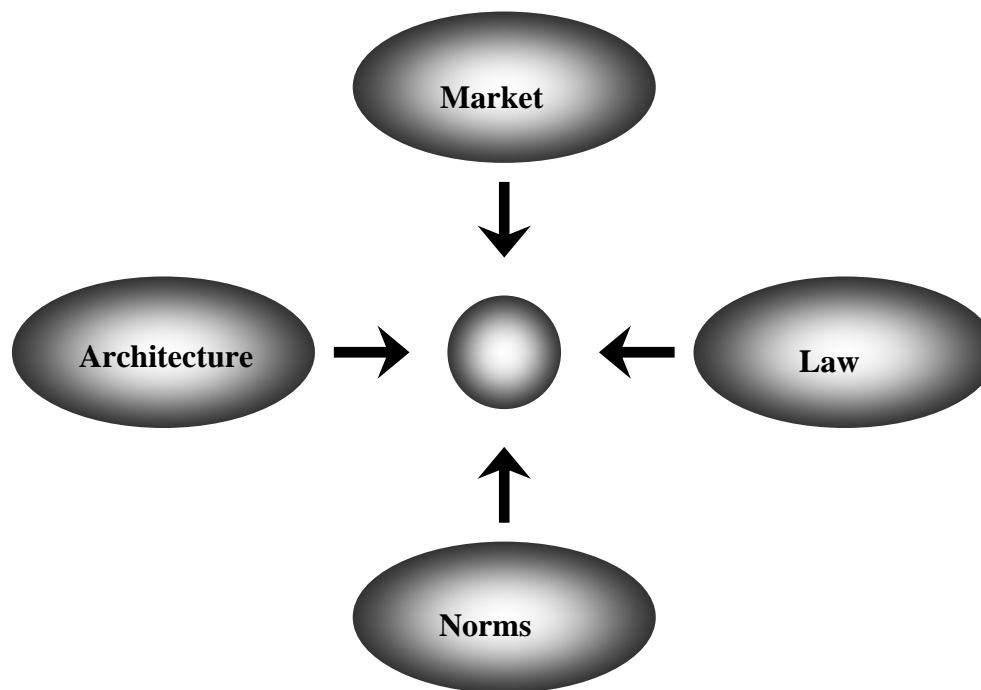


Fig.1 Lessig's model of direct regulation [6, p.88]

In this model, regulation is exerted on the central 'dot' by the different forces of law, the market, social norms and architecture. In the case of Internet regulation, therefore, censorship or constraints on access may be exercised through legislation (e.g. in the UK by the *Obscene Publications Acts* of 1959 and 1964); through the market (by charging for access to infrastructure or to content); through social norms (e.g. by educating users such

Controlling the Net: European approaches to content and access regulation

that they self-regulate their own access); or through architecture (e.g. by the installation of filtering software). The regulation is direct and mostly transparent to those whom it affects.

However, regulation is not always direct, and this is particularly true of the many self-regulatory initiatives that have been implemented with regard to the control of Internet use and content. Lessig therefore developed his model further to illustrate the ways in which indirect regulation can operate, particularly through the implementation of legislation that exerts an influence on the other modalities of regulation. This model of indirect regulation is shown in Figure 2.

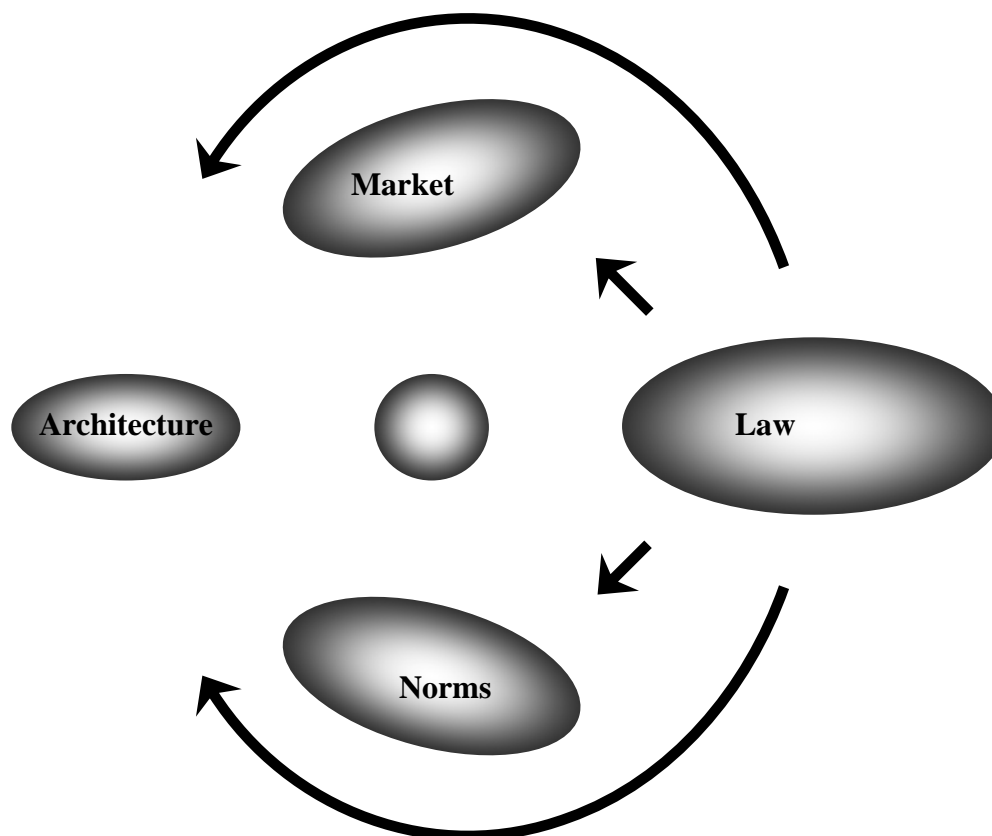


Fig.2 Lessig's model of indirect regulation [6, p.93]

In this model direct regulation, whereby the law instructs citizens on how they should behave and punishes deviation from that behaviour, is replaced by legislative and regulatory initiatives that are used to modify the other modes of constraint (the market, social norms or technical architecture) in order to produce the desired control. For example, market conditions (such as the cost of petrol) may be manipulated by government (for

example, by higher taxation) in order to regulate behaviour (in this case, perhaps, to reduce traffic congestion). With regard to the regulation of Internet content, the withholding of grants to libraries that do not implement filtering software (as, for example, is the case with the Children's Internet Protection Act in the US) is a good illustration of a government exercising indirect control. As Lessig points out, this model of regulation risks producing a regulatory environment that lacks transparency and undermines political accountability [6]. Whereas a law restricting the use of private cars can be seen to be a clear statement of the government's position on transport regulation, higher petrol prices as a result of increased taxation may be confused by consumers as being the responsibility of 'greedy' oil companies and petrol station owners.

The analysis of EU measures intended to regulate Internet content and access used these models as a framework in order to illuminate the balance between the different modalities of control, and the extent to which regulation was imposed in a direct and transparent manner.

4. Approaches to content regulation – the European Union

4.1. The debate begins

Initially, the EU focussed much of its ICT policy on the competitiveness of European information technology products and the creation of a 'European Information Society'. The concept of a 'European Information Society', as portrayed in the Bangemann Report of 1994 [45], with its emphasis on the market, economic growth and the liberalisation of the telecommunications sector, firmly established the context of subsequent initiatives with regard to the Internet. Although the report gave some initial acknowledgement to the potential role of the Information Society in fostering social cohesion and well-being, the overall message was heavily focussed on competition, and the role of the market. As a result, much of the emphasis of early EU policy towards the Internet remained firmly biased towards funding Research and Development activity to enhance competitiveness, and to reduce unemployment [46,47].

It is therefore not surprising, perhaps, that the EU was initially much slower to address issues of Internet content than was the US [48]. This may be explained in part by the cultural and linguistic diversity of Member States. The slower initial penetration of the Internet in Europe was no doubt another factor that delayed the EU from addressing issues of content regulation [49]. However, the Commission argued in its defence that it was avoiding rushing into any unwise decisions: a Commission communication of 1996 stated that 'Over-hasty legislation should be avoided until it is clear where and what type of intervention is required' [50]. Whether this should be seen as a common-sense cautionary approach, or as an excuse for bureaucratic procrastination in making decisions in a difficult and controversial arena is open to question.

Controlling the Net: European approaches to content and access regulation

In addition to this initial tardiness on the part of the Commission, individual Member States have also tended to delay implementing legislation in accordance with EU policy relating to Internet regulation. According to Charlesworth [48] this can be attributed to:

- Resistance from entrenched commercial interest groups to perceived threats to their existing rights;
- The fear of national governments of losing their autonomy to control online activities;
- A lack of understanding of the technical workings of the Internet and its implications for societal norms on the part of legislators;
- The rapid pace of technological development, of which national governments and legislators have been unable to keep abreast.

The principle of subsidiarity, which stipulates that for areas of joint competence the EU should only take action where the scale or effects of a particular policy area makes action at the EU level more effective than individual action by Member States, has traditionally favoured leaving the regulation of broadcasting and other mass media largely in the hands of national authorities [51]. However, the advent of new technologies, increased technical and economic convergence, the increasingly ‘trans-frontier’ reach of media such as the Internet and cable and satellite broadcasting, together with the widening scope of the EU beyond the simple creation of a ‘common market’ – for instance, the ambition to ‘promote cultural policies, and to stimulate the creation of consensus between European cultures’ [51, p.75] – have led to a greater level of EU intervention in the media arena. In particular, Pillar Three of the Maastricht Treaty [52], allowing for co-operation in the field of justice and home affairs, provides a basis for the Commission’s involvement in co-ordinating the efforts of national law enforcement agencies with regard to illegal content on the Internet [49, p.145; 53, pp.345-6].

And so, by the mid 1990s, the EU started to express interest in the control of ‘harmful’ and illegal Internet content, particularly with a view to protecting the interests of minors. The debate was initiated by the Commission in 1996, with the Commission’s *Communication Paper on Illegal and Harmful Content on the Internet* [54], which proposed that the solution to controlling access to illegal and harmful content lay in

...a combination of self-control of the service providers, new technical solutions such as rating systems and filtering software, awareness actions for parents and teachers, information on risks and possibilities to limit these risks.

This favouring of a combination of regulation through manipulation of social norms and of architecture set the scene for the subsequent *Action Plan* [55]. The initial debate identified several key themes that have continued to characterise the approach of the EU to the issue, namely the centrality of industry self-regulation as a mechanism for content control; that, given the diversity of the Member States, categorising ‘illegal content’ is easier than categorising ‘harmful content’; that, to be effective, content regulation requires a global solution; and finally that responsibility for content lies with producers and distributors, rather than with intermediaries such as ISPs [48,

pp.59-60). It does have to be noted, however, that the latter principle has not been without subsequent challenge in some Member States, as for example in the 1998 Compuserve case in Germany¹ [56], and the UK case between Demon Internet Ltd and Godfrey² [57, p.127].

As a result of the initial *Communication* the Parliament called on the Commission to propose a common framework for self-regulation at EU level. The framework was to include

- Objectives in terms of the protection of minors and human dignity;
- Principles governing the representation of the industries concerned and the decision-making procedures;
- Measures to encourage private enterprise to develop message protection and filtering software;
- Measures for ensuring that all instances of child pornography uncovered on computer networks would be reported to the police and shared with Europol and Interpol.

It also called on the Commission and the Member States to encourage the development of a common international rating system, compatible with the PICS (Platform for Internet Content Selection) protocol³, that would be sufficiently flexible to accommodate cultural differences, and asked the Commission to submit proposals for a common regulation of liability for Internet content.

4.1.1 Green Paper on the Protection of Minors and Human Dignity

At much the same time as the Commission Communication was being debated, a *Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services* [58] was adopted by the Commission. The *Green Paper* was intended above all to stimulate public debate in order to identify the main problems posed by the new information services, and to identify what should be done to address these [59]. This debate culminated in a *Proposal for a Council Recommendation* [60], which saw the role of the EU mainly in a co-

¹ Felix Somm, Managing Director of the Internet Service Provider Compuserve Germany at the time of the case, was convicted and received a two-year suspended sentence for complicity in distributing illegal pornography by not blocking CompuServe customer access to the relevant sites. The judgement was later overturned on the grounds that there was no technology available at the time that would have allowed CompuServe to block the material in question.

² Internet Service Provider Demon Internet Ltd was sued by Godfrey for a defamatory statement posted on a newsgroup hosted on its server. Demon argued that, as it merely played a passive role by providing the infrastructure for the poster of messages, they could not be liable for content published. The court rejected this defence on the grounds that Demon chose to receive and store the newsgroup, and had the power to delete messages from it, and was therefore a publisher, subject to the provisions of the Defamation Act 1996.

³ PICS is a rating system for Internet content, widely supported by various governments and industry-based organisations. It works by embedding electronic labels in text or image documents, allowing users to vet their content before the computer displays them or passes them on to another computer.

Controlling the Net: European approaches to content and access regulation

ordinating light: it was to ensure a minimum level of coherence between national self-regulatory frameworks and to encourage co-operation at European level [49, p.151]. The Council adopted the *Recommendation* in May 1998. With specific regard to Internet content, the *Recommendation* requested ISPs to develop codes of conduct and also offered guidelines for the development of national self-regulation regarding the protection of minors and human dignity, based on three key elements:

- The involvement of *all* interested parties (Government, industry, service and access providers, and user associations) in the production of codes of conduct;
- The implementation of codes of conduct by the industry;
- The evaluation of measures taken.

Once again, there was an emphasis on social norms as a regulatory mode, and importance given to the involvement of the private sector in the regulatory process. Broad recognition was given to the commitment of the EU towards ensuring that measures taken are consistent with observance of Articles 8 and 10 of the European Convention on Human Rights [61], relating to the rights of privacy and of freedom of expression. Particular emphasis was placed on measures that support parental control and the promotion of access to high quality content, including the further development of technology-supported measures such as content rating and filtering systems.

A particularly interesting response to the debate was put forward by the European Commission Legal Advisory Board [62]. This endorsed a number of important principles set out in the documents, and raised some additional points for consideration. Among those that it emphasised were:

- Existing rules such as laws intended to protect minors and human dignity should apply equally to all media – the Internet is not a “sphere apart” subject only to voluntary self-regulation and exempt from national law;
- The Internet is ‘a positive instrument, empowering citizens and educators, lowering the barriers to the creation and distribution of content and offering universal access to ever richer sources of digital information’ – thus any action taken to deal with ‘atypical’ use should not have a disproportionate impact on Internet users and on the industry as a whole;
- The potential empowerment of users through increased transparency of government and availability of public sector information should be at the forefront of the debate;
- ISPs are responsible for their own content that they make available for use, but they are not responsible for third party content to which they merely provide access for use, unless they can ‘reasonably be said to have had knowledge about its possibly illegal or harmful content and blocking its use is both technically possible and can be reasonably expected’;

- Information on the Internet should be allowed the same free circulation as paper-based information. The requirements of Article 10 of the European Convention on Human Rights should guide decisions on the proportionality of any measures restricting freedom of expression and any regulatory approach to control harmful content should abide by the terms of the Article;
- Where content rating is used, the criteria and procedures for rating content should remain transparent. With regard to filtering services, information access providers should make their use of such devices transparent to their clients; they should not oblige their users to use a particular filtering service, and they should respect the right to privacy;
- ISPs and Internet access providers should make software available that allows parental control, and should make information about the software available to parents and teachers. [62]

The Board's paper concludes with a further two guiding principles that it believed should underpin the debate. Firstly, that the focus of EU efforts should be on facilitating practical co-operation rather than on attempts to find a new specific legislative solution for the Internet. Secondly that, although consensus in the broader international context is desirable, 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' [62].

In April 2004, the Commission proposed an updated *Recommendation* [63] intended to take account of new technological developments. In particular, this concentrated on the right to reply across all media; media literacy; the harmonisation of ratings descriptors; and measures against discrimination and incitement to hatred on the grounds of race, sex or nationality in online media. The *Recommendation* met with general approval from the EESC, the Parliament and the Council, with only minor amendments being agreed under the co-decision process.

4.1.2 Action Plan on Promoting Safe Use of the Internet

Meantime, a parallel initiative originating from DG XIII and leading on from the 1996 *Communication* was also being developed by the Commission. The four-year *Action plan on Promoting Safe Use of the Internet* [55] was originally intended to cover the period 1998-2001 inclusive, and was adopted in November 1997 with a budget of 25 million Euro. The *Action Plan* was based on a self-regulatory approach and shaped by the same underlying principles as the *Recommendation*. However, whereas the *Recommendation* was a legal instrument providing guidelines for national legislation, the *Action Plan* was intended as a mechanism for targeting financial support towards implementing actions. Following the themes identified in the *Communication* it proposed four main action lines to 'create a safer environment' by combating illegal and harmful Internet content:

- Industry self-regulation – for example, through the creation of a European network of hotlines to allow users to report content that they consider to be illegal, and through the development of industry codes of conduct;

Controlling the Net: European approaches to content and access regulation

- Technical measures, such as the development of filtering and rating systems;
- Raising user awareness, for example by developing material for use in the education sector;
- Support actions, such as those aimed at identifying the legal implications of actions taken under the *Action Plan*. [55]

The *Action Plan* recognised the need for co-ordination and co-operation across Member States. Illegal use that it considered should be controlled included ‘actions or speech that may be prejudicial to national security; content that threatens the protection of minors (in particular child pornography) and the protection of human dignity (in particular race-hate speech); actions prejudicial to economic security (e.g. fraud) and information security; and actions liable to damage the protection of privacy, reputation or intellectual property’ [55]. It advocated that illegal content be dealt with at source by law enforcement agencies, aided by industry self-regulation (for example, by the use of hotlines to alert ISPs to potentially illegal content). Content deemed harmful (that is, content that is potentially offensive but not illegal) should be controlled via access restriction (such as filtering and ratings technologies) and by raising parental and user awareness, but should not be removed on the grounds of allowing freedom of expression. It noted that ‘a definition of ‘harmful’ content will always be subject to the cultural differences inherent in the Member States’ [55]. This continued the earlier reliance on a combination of modes of regulation, in this case specifically those of architecture, social norms and law.

The *Action Plan*, with its emphasis on industry self-regulation and its support for user hotlines, gave added impetus to the work of the Internet Watch Foundation (IWF) in the UK. Set up in September 1996 as an independent organisation (originally called the Safety-Net Foundation), largely in response to demands from the Metropolitan Police, the Foundation was to implement proposals for controlling Internet content that were jointly agreed in the UK by the government, the police and the Internet Service Providers associations (ISPA and LINX). In addition to drafting a Code of Practice for the Industry, the initial focus of the Foundation’s work was on the regulation of child pornography, with ISPs agreeing to exclude clients who hosted illegal pornographic or paedophile images or messages, wherever this was brought to their attention. A hotline was set up to enable Internet users to alert the ISF to sites that they suspect contain illegal materials and, if found to be so, IWF alerts any ISP hosting the site. Only if the ISP does not co-operate in removing the content at this stage would it be liable for prosecution.

During debate in the European Parliament, it was noted that, while the *Action Plan* was ‘a step in the right direction’, the fact that EU legislation does not cover criminal law makes the promotion of safe Internet use a difficult task. Indeed

It was the unanimous view of the House that illegal and harmful content on the Internet could be damaging to the mental health, safety and economic interests of consumers and thus affect the creation of an environment conducive to sound ethical standards. But combating Internet content liable to prosecution was a matter for the member states. In practice, this was made considerably more difficult

by the fact that there were not even identical or at least comparable legal standards governing important issues in this area throughout the EU. [64]

This apparent reluctance to take responsibility at European level for potentially illegal Internet content seems to contradict Pillar Three of the Maastricht Treaty, which, as noted earlier, allows for a measure of co-ordination between national governments in this area. However, on its second reading at the Parliament several amendments to the *Action Plan* were tabled: potentially the most far-reaching proposal of all, was that civil and criminal law within the EU should be harmonised with the aim of ensuring safer use of the Internet [65].

Following an intermediate evaluation of the results of implementing the *Action Plan*, the Commission published a *Communication Paper* on its follow-up, proposing to extend it for a further two years until 31st December 2004 [66]. The intention of the new proposal was to ‘adapt [the scope and implementation of the *Action Plan*] to take account of lessons learned and new technologies, and to ensure co-ordination with parallel work in the field of network and information security’ [66]. In reality, the proposed ‘adaptation’ of scope comprised a significant extension of application, both in terms of the technologies to which the coverage would apply and the nature of the content to be controlled. Thus, in future, proposed actions would apply to mobile and broadband content, online games, peer-to-peer file transfer, and all forms of synchronous online communications such as chat rooms and instant messages. Relevant content would now encompass racism and violence.

The Commission still claimed the underlying rationale of the *Action Plan* as being that of user empowerment, with the Commission acting as facilitator for, and contributor to, European and global co-operation in this arena. EU actions were promoted by the Commission as complementary to national initiatives, with the aim of achieving a considerable degree of decentralisation through a network of national co-ordinators. Four areas still requiring action were identified in the proposed extended *Action Plan*:

- Support for hotlines to enable users to report illegal content;
- Continuing promotion of industry self-regulation;
- User empowerment through filtering software;
- Increasing awareness about safer use of the Internet. [66]

Although not radically different from earlier priorities, it was emphasised that the focus of the new programme should be on self-regulatory and non-regulatory aspects of safe Internet use, and in particular on those actions intended to raise awareness of safe use, especially in countries that currently lack appropriate experience and infrastructure. It was also suggested that part of the new initiative should include support for the creation of high quality European content intended specifically for children. Enhanced networking was to be encouraged among all those involved in the field through the establishment of a Safer Internet Forum, and more active involvement of the media and content industries was promoted as desirable. This reflects a shift away from an earlier belief in

Controlling the Net: European approaches to content and access regulation

the potential of technical solutions (as represented by ‘architecture’ in the Lessig models) to a more emphatic focus on the manipulation of social norms to address the issue.

In response to the *Communication* from the Commission, the European Economic and Social Committee (EESC) argued the case for a more restrictive approach based on legislation. The Committee recommended adopting a legal framework that ensured co-regulation⁴ rather than the voluntary self-regulation proposed by the Commission. It also advocated stronger government and industry support for ratings and warning schemes, particularly with regard to chat rooms, and the adoption of a stronger line against racism on the Internet, which ‘should not be condoned on the grounds of protecting freedom of expression’ [67].

On 16th June 2003 the Parliament and Council agreed to the original communication proposal by adopting the new *Action Plan* [68]. In addition to the changes already described, the title of the Plan was amended to ‘*The Multiannual Community Action Plan on Promoting Safer Use of the Internet and New Online Technologies by Combating Illegal and Harmful Content Primarily in the Area of the Protection of Children and Minors*’ in order to reflect new emphases. An additional sum of 13.3 million Euro was made available for implementing the extended actions.

In August 2003 the European Commission announced that, in addition to the extension of the Action Plan to 2004, it was making preparations for a follow-up programme, the Safer Internet Plus programme [69], to cover the period 2005-2008. The overall objective of this programme remained the promotion of safer use of the Internet and other new technologies, particularly by children, and to continue the fight against illegal content and ‘content unwanted by the end user’ (notably, spam) [69]. The stated intention this time was to focus on the end-user, in particular parents, educators and children. The programme was also opened up to other new media, and to new issues such as the expansion of network infrastructure to accession countries.

⁴ The Interinstitutional Agreement on better law-making [70, cited in 71, pp.11-12], defines co-regulation as ‘...the mechanism whereby a Community legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognised in the field (such as economic operators, the social partners, non-governmental organisations, or associations)’. Self-regulation is defined as ‘...the possibility for economic operators, the social partners, non-governmental organisations or associations to adopt amongst themselves and for themselves common guidelines at European level (particularly codes of practice or sectoral agreements)’. Thus, although both forms of regulation could be said to involve some form of interaction between the European Institutions’ processes and private actors, there is a clear distinction between the voluntary or legislative basis for action. For further discussion on these forms of regulation see [71].

5. Discussion and conclusions

The level of European Union activity in developing and debating new initiatives on content regulation from 1996 onwards suggests that this issue has climbed higher on the policy agenda, particularly with regard to preventing access by minors to material with a sexual content. However, the sheer volume of different initiatives, usually emanating from different Directorates General and each with a different policy emphasis, has led to a fragmentation and lack of overall coherence that has arguably diluted the impact and effectiveness of the different measures. Nevertheless, this overview of some of the key EU policy measures in this area demonstrates that, as far as the EU is concerned, the Internet is certainly far from being an unregulated zone. In reality, the analysis suggests that the EU has adopted a multi-faceted approach to the regulation of Internet access and content, resulting in the imposition of a variety of constraints in the form of legal instruments (e.g. the *Recommendation on the Protection of Minors and Human Dignity*); the shaping of technical architecture (e.g. by funding filtering software development projects); attempts to manipulate cultural norms (e.g. through the promotion of educational initiatives); and self-regulatory mechanisms at a range of levels (e.g. through the support of national hotlines). From a methodological perspective, the adoption of Lessig's models of regulation to map these constraints has proved useful as a heuristic tool, highlighting the complexity of the balance between different modalities of control and the inherent dangers to accountability and transparency of an over-reliance on industry self-regulation.

The findings suggest that the EU has chosen to adopt each of Lessig's four modalities of regulation in combination with each other in order to control Internet access and content, albeit with less emphasis on control through the market than through the other modalities. This accords with the complex and multi-faceted approaches that have been identified elsewhere in response to a range of information policy issues such as privacy protection on the Internet [see 44,72,73,74].

In addition to highlighting the manner in which a range of modalities of control have been combined at EU level to exert a regulatory effect on Internet content and access, these models illuminate a shift in emphasis away from an earlier favouring of technical solutions towards approaches based on the manipulation of social norms via education, awareness-raising and self-regulatory initiatives. This is in contrast to the more top-down, legislation-driven approaches adopted across the EU towards e-commerce, data protection and privacy rights. It is likely that this is in part due to the sheer difficulties presented by attempts to legislate at transnational level on an issue that is framed by cultural values and community norms. It may also be influenced by the failure of technical solutions to provide a suitable context sensitive approach to content regulation, acceptable to a wide and diverse clientele. The apparent shift towards a model of content regulation that favours co-regulation (as defined earlier) risks a further 'democratic deficit' as the power for law enforcement is increasingly delegated to private bodies.

Although Lessig [6] highlights the primacy of code as a regulatory force, it must be recognised that code itself inevitably represents the interests of its developers and is therefore inherently socially shaped [75, cited in 76].

Controlling the Net: European approaches to content and access regulation

Thus the two-way nature of this shaping should be acknowledged: technology both shapes and is shaped by society and therefore impacts on regulation, but is also subject to the impact of regulation. Moreover, it should be noted that technology does not always act in a predictable ways and therefore any attempts to build regulation into technology may founder as the technology ‘objects’ to such control [77]. This suggests the limitations of technology (architecture) as a regulatory mode of control. Lessig himself also highlights the fact that regulation by architecture (code) is likely to be less visible than regulation by law, and thus carries the danger of lack of transparency [44]. At the same time the other modalities of regulation also exhibit their own limitations: thus, for example, law and social norms both require a degree of internalisation on the part of individuals if they are to be effective, and relying on manipulation of market forces as a means of regulation may incur other problems such as exacerbating existing inequalities in access to information: the wealthy may be able to overcome attempts to regulate, whereas the less well-off are not able so to do.

The enthusiasm with which the EU has embraced a primarily neo-liberal self-regulatory approach to the issue of Internet content regulation, compared with its more directive co-regulatory approach in areas such as e-commerce, may seem to pose fewer threats to the protection of freedom of expression and freedom of enquiry than is the case in more repressive regimes. Nevertheless, an approach based on industry self-regulation carries its own dangers, as has been highlighted by Lessig’s model of indirect regulation. This is reflected in the following comment:

Because the approach to Internet regulation has been legislation-driven in the United States, and of course because the US has a constitution, the debate can at least happen in an ordered and accountable manner. The danger with the European approach, according to civil liberties groups, is that it tends to be more covert. [78]

The ensuing lack of legal clarity has also been shown to have led to a ‘chilling effect’ on ISPs, who are deterred from hosting controversial material or material that could attract legal action. Collins and Murrone [79, p.172] have criticised a reliance on industry self-regulation on the grounds that ‘Self-regulatory bodies are accountable not to citizens or consumers – even through the imperfect channel of Parliament – but only to the industry which has established them’. This leads ultimately to the risk of a situation where only ‘acceptable’ voices are heard: and because of the lack of transparency and judicial process to review decisions to withhold access to content, citizens are not even aware of the restrictions imposed. There are clear parallels here with the distortions to the conditions that favour ideal speech as discussed by Habermas [10].

The research exposed a conflict arising from the competing aims of initiatives and legislation that aim to protect and promote information access and freedom of expression (for example, Article 10 of the European Convention on Human Rights), and those whose primary aims are to control access to obscene or criminally racist content. In this respect, it can be argued that the EU, in common with the UK, is hampered by the lack of an overarching, coherent information policy that could inform the priorities and balances of approaches to information access. It

is vital that our values and priorities inform and are reflected by our regulatory choices. At the present time, it would appear that, in the EU arena, the desire to control and regulate the Internet is taking precedence over measures to promote freedom of expression and freedom of enquiry online. A reliance on industry self-regulation rather than on autonomous self-regulation by the end-user carries real risks of ‘unseen’ (and therefore unaccountable) censorship. As we embark on the next generation of the Web, the democratising potential of the ‘conversational platform’ [80] offered by new communications and collaboration tools, such as blogs and wikis, can be seen clearly, particularly in so far as they facilitate genuine collaboration in sharing knowledge and in shaping content. This accords well with the Habermasian concept of the Public Sphere and its facilitation of a diverse panoply of dissenting voices beholden to no-one (the ‘ideal speech’ situation) leading to rational and genuinely democratic decision-making. However, as has been seen from the findings of this study, these voices risk being constrained by a range of measures that are intended to promote a ‘decent’ and ‘acceptable’ environment on the Web. This impetus to filter and sanitise the Net is in direct conflict with the views of those who promote the importance of exposure to a wide range of content:

People should be exposed to materials they would not have chosen in advance. Unanticipated encounters, involving topics and points of view we have not sought out and perhaps find irritating, are central to democracy and even to freedom itself. [41, p.58]

Should this impetus hold sway, there is a very real risk that the original vision of Berners-Lee of the Web as a collaborative space for sharing ideas will not prevail. Despite its potential to offer a twenty-first century Public Sphere, our enthusiasm to regulate and control the Internet is likely to prevent such utopian hopes of the Internet as a tool of freedom and democracy from ever being realised.

6. References

- [1] C.R. Hughes and G. Wacker (eds), *China and the Internet: Politics of the Digital Leap Forward* (RoutledgeCurzon, London, 2003).
- [2] L. Tsui, The panopticon as the antithesis of a space of freedom: control and regulation of the internet in China, *China Information* 17(2) (2003) 65-82.
- [3] J. Lacharite, Electronic decentralisation in China: a critical analysis of internet filtering policies in the People’s Republic of China, *Australian Journal of Political Science* 37(2) (2002) 333-346.
- [4] N. Hachigian, China’s cyber-strategy, *Foreign Affairs* 80(2) (2001) 118-133.
- [5] G. L. Taubman, State-sanctioned surfing, limited connectivity, and varied access to cyberspace in non-democracies, *Asian Perspective [S. Korea]* 27(2) (2003) 105-40.
- [6] L. Lessig, *Code and other Laws of Cyberspace* (Basic Books, New York, 1999).

Controlling the Net: European approaches to content and access regulation

- [7] I. Rowlands, Understanding information policy: concepts, frameworks and research tools, *Journal of Information Science* 22 (1) (1996) 13-25.
- [8] I. Rowlands and P. Turner, Models and frameworks for information policy work. In: I. Rowlands (ed.), *Understanding Information Policy* (Bowker Saur, London, 1997).
- [9] J. Milton, *Areopagitica: for the Liberty of Unlicensed Printing* (Clarendon, Oxford, 1973). Originally published 1644.
- [10] J. Habermas, *The Structural Transformation of the Public Sphere* (Polity, Cambridge, 1989).
- [11] W. Outhwaite, *Habermas: a Critical Introduction* (Polity, Cambridge, 1994).
- [12] M. Dean, *Governmentality: Power and Rule in Modern Society* (Sage, London, 1999).
- [13] S. Cohen, *Folk Devils and Moral Panic: the Creation of the Mods and Rockers*, 2nd ed. (Martin Robertson, Oxford, 1980).
- [14] A. Newey, Freedom of expression: censorship in private hands. In: Liberty, *Liberating Cyberspace: Civil Liberties, Human Rights and the Internet* (Pluto, London, 1999).
- [15] I. de Sola Pool, *Technologies of Freedom: on Free Speech in an Electronic Age* (Belknap, Cambridge Ma., 1983).
- [16] N. Moore, Introduction. In: I. Rowlands and S. Vogel, *Information Policies: a Sourcebook* (Taylor Graham, London, 1991).
- [17] K.A. Hill and J.E. Hughes, *Cyberpolitics: Citizen Activism in the Age of the Internet* (Rowman & Littlefield, Oxford, 1998).
- [18] S. Green, A plague on the panopticon: surveillance and power in the global information economy, *Information, Communication and Society* 2(1) (1999) 26-44.
- [19] J. Slevin, *The Internet and Society* (Polity, Cambridge, 2000).
- [20] S. Davies, A Year after 9/11: where are we now? *Communications of the ACM* 45(9) (2002) 35-39.
- [21] Office for National Statistics, *2004 e-commerce Survey of Business* (2005). Available at: www.statistics.gov.uk/downloads/theme_economy/ecommerce_report_2004.pdf (accessed 6 January 2006).
- [22] S. E. Ebersole, On their own: students' academic use of the commercialized Web, *Library Trends* 53(4) (2005) 530-538.
- [23] T. Jordan, *Cyberpower: the Culture and Politics of Cyberspace and the Internet* (Routledge, London, 1999).
- [24] A. C. Clarke, *Voices from the Sky* (Harper & Row, New York, 1965).
- [25] M. Castells, *The Power of Identity* (Oxford, Blackwell, 1997).

- [26] M. Castells, *The Internet Galaxy: Reflections on the Internet, Business and Society* (Oxford, Oxford University Press, 2001).
- [27] R. Woolnough, Web driver issues free ticket to ride, *Times Higher Education Supplement* 30/3/2001, 17.
- [28] K. C. Laudon, Ethical concepts and information technology, *Communications of the ACM* 38(12) (1995) 33-39.
- [29] D. Wall, Policing the Internet: maintaining law and order on the cyberbeat. In: Y. Akdeniz, C. Walker and D. Wall (eds), *The Internet, Law and Society* (Pearson, Harlow, 2000).
- [30] D. Burt, In defence of filtering, *American Libraries* 28(7) (1997) 46-47.
- [31] E. Volokh, Freedom of speech, shielding children and transcending balance, *Supreme Court Review* 141 (1997) 141-197.
- [32] H. Auld, Filters work: get over it, *American Libraries* 34(2) (2003) 38-42.
- [33] Datamonitor, *Internet filtering: preventing porn and pushing productivity* (2002). Available at: www.commentwire.com/commwire_story.asp?commentwire_ID=3647 (accessed 5 July 2004).
- [34] J. B. Pierce, Blaise Cronin: defender of CIPA, *American Libraries* 34(2) (2003) 41.
- [35] J. D. Lasica, Censorship devices on the Internet, *American Journalism Review* 19(7) (1997) 56.
- [36] P. Fine, Cyber Patrol halts student, *Times Higher Education Supplement* 23/11/2001, 56.
- [37] EPIC, *Filters and Freedom 2.0: Free Speech Perspectives on Internet Content Controls* (EPIC, Washington, DC, 2001).
- [38] J. Frechette, Cyber-democracy or Cyber-hegemony? Exploring the political and economic structures of the Internet as an alternative source of information, *Library Trends* 53(4) (2005) 555-575.
- [39] P. Resnick and H. R. Varian (eds), Recommender systems, *Communications of the ACM*, 40(3) (1997) Special Section 56-89.
- [40] ACLU, *Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals may Torch Free Speech on the Internet* (1997). Available at: <http://archive.aclu.org/issues/cyber/burning.html> (accessed 5 July 2004).
- [41] C. R. Sunstein, Democracy and filtering, *Communications of the ACM* 47(12) (2004) 57-59.
- [42] D. Stoker, Filtering out minorities (editorial), *Journal of Librarianship and Information Science* 31(1) (1999) 3-6.
- [43] A. L. Shapiro, *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World we Know* (Century Foundation/Public Affairs, New York, 1999).
- [44] L. Lessig, The law of the horse: what cyberlaw might teach, *Harvard Law Journal* 113 (1999) 501-546.

Controlling the Net: European approaches to content and access regulation

- [45] M. Bangemann et al, *Europe and the Global Information Society: Recommendations to the European Council High Level Group on the Information Society* (European Council, Brussels, 1994).
- [46] B. Mahon, European information policy: the role of institutional factors. In: I. Rowlands (ed.), *Understanding information policy* (Bowker-Saur, London, 1997).
- [47] J. Dearnley and J. Feather, *The Wired World: an Introduction to the Theory and Practice of the Information Society* (Library Association, London, 2001).
- [48] A. Charlesworth, The governance of the Internet in Europe. In: Y. Akdeniz, C. Walker and D. Wall (eds) *The Internet, Law and Society* (Pearson, Harlow, 2000).
- [49] P. Campbell and E. Machet, European policy on regulation of content on the Internet. In: Liberty, *Liberating Cyberspace: Civil Liberties, Human Rights and the Internet* (Pluto, London, 1999).
- [50] European Commission, *Communication on the Implications of the Information Society for European Union Policies – Preparing the Next Steps*. COM (96) 395.
- [51] P. Cincera, The European Union content regulation in the converged communication environment. In: K. A. Eliassen and M. Sjovaag (eds.), *European Union Telecommunications Liberalisation* (Routledge, London, 1999).
- [52] European Commission, *Treaty on European Union*, Cm.1394 (Stationery Office, London, 1992). Available at: http://europa.eu.int/abc/treaties_en.htm (accessed 12 January 2006).
- [53] Y. Akdeniz and C. Walker, Whisper who dares: encryption, privacy rights and the new world disorder. In: Y. Akdeniz, C. Walker and D. Wall, *The Internet, Law and Society*. (Pearson, Harlow, 2000).
- [54] European Commission, *Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: Illegal and Harmful Content on the Internet*. COM (96) 487.
- [55] European Parliament, Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, *Official Journal of the European Communities*, L336 (1999) 1.
- [56] C. Kuner, *Judgement of the Munich court in the Compuserve case: translation and commentary* (n.d.). Available at: <http://www.kuner.com/data/reg/somm.html> (accessed 12 January 2006).
- [57] C. Gringras, *The laws of the Internet*, 2nd ed. (Butterworths LexisNexis, London, 2003).
- [58] European Commission, *Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services*. COM (96) 483.
- [59] European Commission, Illegal and harmful content on the Internet: Interim report on initiatives in EU Member States with respect to combating illegal and harmful content on the Internet, *Info 2000*, version 7, 4/6/1997.

- [60] European Commission, *Commission Communication to the European Parliament, the Council and the Economic and Social Committee on the Follow-up to the Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services including a Proposal for a Recommendation*. COM (97) 570 final, 18.11.1997.
- [61] Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*. (Council of Europe, Strasbourg, 1950). Available at: <http://conventions.coe.int/treaty/en/Treaties/Html/005.htm> (accessed 19 January 2006).
- [62] Legal and Advisory Board, *Response to the Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services* (Legal and Advisory Board, Brussels, 1997).
- [63] European Commission, *Proposal for a Recommendation on the Protection of Minors and Human Dignity and the Right of Reply in Relation to the Competitiveness of the European Audiovisual and Information Services Industry*, COM (2004) 341.
- [64] European Parliament, The Internet – tackling pornography and other abuses: consultation procedure [A4-0234/98-Schmid], *Session News: the Week* (1998) Brussels, 1-2 July, 9-10.
- [65] European Parliament, Promoting safe use of the Internet. co-decision procedure – second reading [A4-0377/98-Schmid], *Session News: Strasbourg Briefing* (1998) Strasbourg, 16-20 November, 18.
- [66] European Commission, *Communication from the Commission on the Follow-up to the Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks*, COM (2002) 152.
- [67] European Economic and Social Committee, Protection of children on the Internet, *Press Release* 37/2003 (2003) Brussels.
- [68] European Commission, Decision No 115/2003/EC of the European Parliament and of the Council amending Decision No 276/1999/EC adopting Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks, *Official Journal of the European Union*, L162 (2003) 1.
- [69] European Commission, Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a Multiannual Community Programme on Promoting Safer Use of the Internet and New Online Technologies. Available at: http://europa.eu.int/information_society/activities/sip/programme/index_en.htm (accessed 2 February 2006).
- [70] European Parliament, Council, Commission, Interinstitutional Agreement on better law-making, *Official Journal of the European Union* C321 (2003) 1.

Controlling the Net: European approaches to content and access regulation

- [71] L. Senden, Soft law, self-regulation and co-regulation in European law: where do they meet? *Electronic Journal of Comparative Law* 9(1) (2005). Available at: <http://www.ejcl.org/91/art91-3.PDF> (accessed 24 July 2006).
- [72] J. R. Reidenberg, Governing networks and rule-making in Cyberspace. In: B. Kahin and C. Nesson, *Borders in Cyberspace* (MIT Press, Cambridge Ma., 1997).
- [73] C. J. Bennett and C. D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, 2nd ed. (MIT Press, Cambridge MA, 2006).
- [74] W. H. Dutton and M. Peltu, *The Emerging Internet Governance Mosaic: Connecting the Pieces*. Forum Discussion Paper No. 5 (Oxford Internet Institute, Oxford, 2005).
- [75] D. MacKenzie and J. Wajcman, *The Social Shaping of Technology*, 2nd ed. (Open University Press, Buckingham, 1999).
- [76] I. Hosein, P. Tsiavos and E. Whitley, *Regulating Architecture and Architectures of Regulation: Contributions from Information Systems*. 17th BILETA Annual Conference, Amsterdam, 2002. Available at: <http://www.bileta.ac.uk/02papers/hosein.html> (accessed 26 July 2006).
- [77] B. Latour, When things strike back: a possible contribution of science studies to the social sciences, *British Journal of Sociology* 51(1) (2000) 107-124.
- [78] Internet censorship: US legislates as Britain volunteers, *Library Association Record* 100(9) (1998) 457.
- [79] R. Collins and C. Murroni, *New Media, New Policies: Media and Communications Strategies for the Future* (Polity, Cambridge, 1996).
- [80] J. Klobas, *Wikis: Tools for Information Work and Collaboration* (Chandos, Oxford, 2006).

Acknowledgements

The author would like to thank Prof. Paul Sturges, Prof. Charles Oppenheim and Dr. James Dearnley of Loughborough University and Dr. Ian Rowlands of University College London for their helpful advice, guidance and comments. In addition, grateful thanks are extended towards the anonymous reviewers whose constructive feedback and ideas led to many improvements in the writing of the paper.