INTERNET CONTENT REGULATION

UK GOVERNMENT AND THE CONTROL OF INTERNET CONTENT

Yaman Akdeniz

Internet content regulation with an emphasis on the existence of sexually explicit content remains one of the greatest concern for governments, supranational bodies and international organizations. The 1990s witnessed the proliferation of the Internet and the current concerns by the regulators mainly concentrate on the existence of illegal content such as child pornography over the Internet, and the access of (mainly) sexually explicit content over the Internet by children. This article will analyze the recent developments in relation to Internet content regulation and will argue that there is too much unwarranted anxiety about what is and what is not available over the Internet. Furthermore, the specific technical solutions offered within different foras for the availability of illegal and harmful content may not be the right solutions to pursue as there remains serious concerns for cyber-speech.

INTRODUCTION

There have been many initiatives to deal specifically with the existence of illegal and harmful content over the Internet and these include an emphasis on self-regulation by the Internet industry with the creation of Internet hotlines for reporting illegal Internet content to assist law enforcement agencies and the development of filtering and rating systems to deal with children's access to content which may be deemed as harmful. These two issues are different in nature and should be addressed separately as what may not be appropriate for children may certainly be legal and therefore accessible by willing adults.

These initiatives are mainly led by the Internet industry[1]and are favoured and supported by the European Commission's Action Plan for the safer use of the Internet within the European Union.[2] The UK Government's policy in relation to these matters remains consistent with the European Commission's Action Plan through the Department for Trade and Industry (DTI)[3] and through the quasi-regulatory body, the Internet Watch Foundation (IWF) which works closely with the DTI.[4]

IDENTIFYING THE PROBLEMS

Content-related problems have been largely identified and categorized as illegal and harmful content by the European Commission ever since October 1996.[5] The European Commission in its October 1996 communication on *Illegal and Harmful Content on the Internet* stated that:

> "These different categories of content 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."[6]

Although the Commission's Action Plan for the European Union for a safer use of the Internet[7] (which follows from the above Communication paper) suggests that "harmful content needs to be treated differently from illegal content",[8] these categories have never been clearly defined by the Commission in its Action Plan or by regulators elsewhere. The Action Plan states that illegal content is related to a wide variety of issues such as instructions on bomb-making (national security),[9] pornography (protection of minors),[10] incitement to racial hatred (protection of human dignity) and libel (protection of reputation). But none of these categories provided by the European Commission are necessarily 'illegal content' and not even considered as 'harmful content' (probably undefinable in a global context) by many European countries.

The following headings will try to identify the above concerns by the regulators and the possible problems related to the availability of illegal and harmful content over the Internet from a UK perspective before looking into the approaches that are offered to deal with such content.

ILLEGAL CONTENT

It would be wrong to consider the Internet as a 'lawless place'[11] and therefore law of the land would also apply to the Internet in theory. This is also true for the availability of illegal content over the Internet. Content-related criminal laws would also apply to the Internet if the perpetrators are within the UK jurisdiction.

The most common and the most referred example of illegal content is the availability of child pornography over the Internet. This has been a concern for the UK law enforcement agencies and the regulators ever since Operation Starburst took place in the summer of 1995.[12] The whole issue of illegal content and how to deal with this sort of Internet content has since revolved around child pornography even though child pornography and paedophilia are not Internet-specific problems.

ISSN 0267 3649/01/$20.00

Apart from child pornography, the law enforcement bodies within the UK are also concerned about the existence of commercial websites featuring sexually explicit content created and maintained by UK citizens which may be deemed as obscene under the Obscene Publications Act.

Another concern for content-related criminal activity by the UK law enforcement agencies is the possibility of using the Internet for harassment and threats and the availability of hate speech material over the Internet. According to the NCIS *Project Trawler Report*,[13] the Internet users "may find themselves repeatedly receiving unwanted and distressing communications, such as threatening, obscene or hateful E-mail".[14]

Furthermore and more seriously, the availability of documents which contravene the Official Secrets Act 1989[15] over the Internet have been a concern for the UK Government and security agencies (rather than the law enforcement bodies).[16] Under section 1(1) of the 1989 Act, a person who is or has been a member of the security and intelligence services, would be "guilty of an offence if without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services or in the course of his work while the notification is or was in force."The 1989 legislation would apply to the dissemination of such information over the Internet as in the above examples.

It should also be noted that the law enforcement bodies within the UK remain concerned about the incidental use of the Internet for existing crimes such as fraud,[17] and the emergence of specific cybercrimes[18] such as unauthorized access (hacking) to computer networks,[19] distribution of computer viruses such as the "ILOVEYOU"[20] or the Melissa viruses,[21] and the denial-of-service attacks to computer networks.[22] However, these issues are not so much content-related and therefore will not be further discussed in this article.

HARMFUL CONTENT

The difference between illegal and harmful content is that the former is criminalized by national laws, while the latter is considered as offensive or disgusting by some people but certainly not criminalized by national laws. So, within this category of Internet content, we are dealing with legal content that may offend some Internet users or content that may be thought to harm others, e.g. children accessing sexually explicit content.

This form of Internet content may include sexually explicit content, political opinions, religious beliefs, views on racial matters, and sexuality. However, it should be noted that the European Court of Human Rights has confirmed in the *Handyside*[23] case that freedom of expression extends not only to ideas and information generally regarded as inoffensive but even to those that might offend, shock, or disturb,[24]and this sort of information legally exists over the Internet as well as in other medium.

But, legal regulation of this sort of Internet content may differ from one country to another and this is certainly the case within the European Union with different approaches to sexually explicit content or to hate speech by the member states of the European Union.[25]

For example, even though publishing or distribution of obscene publications may be illegal within the UK under the above mentioned Obscene Publications Act, possession or within the nature of the Internet, browsing or surfing through sexually explicit (as well as obscene) content is not an illegal activity for consenting adults. Furthermore, there are no laws making it illegal for a child to view such content through a magazine or through the Internet.The laws normally deal with the provision of such content to children.[26]

Therefore, harm remains as a criterion which depends upon cultural differences and this is accepted within the jurisprudence of the European Court of Human Rights.[27] However, the availability of harmful Internet content remains as a politically sensitive area and the UK Government and the European regulators remain concerned about the existence of such content over the Internet. The September 1999 *e-commerce@its.best.uk*, the Cabinet Office report[28] stated that "there are worries about the content of the Internet",[29] and according to the report this remains as one of the major issues that "lead to lack of confidence for the development of E-commerce within the UK". However, the main reason for the failure of establishing trust for E-commerce has been the failure of the UK Government to develop a regulatory framework for the use of strong encryption technologies,[30] not the presence of harmful, or offensive Internet content.

UK GOVERNMENT APPROACH TO ILLEGAL AND HARMFUL CONTENT

This part of the article will analyse the UK Government's approach to the availability of illegal and harmful content over the Internet and will explain the UK policy and to some extent the European Union's position and the industry self-regulatory schemes in relation to Internet content.

Within the UK, lead responsibility for content issues lies with the Department for Trade and Industry (DTI) with support from the Department for Education and Employment (DfEE) and Home Office. However, there is no simple one way approach for the problems identified in the above sections and therefore relying on the legal system or the provision of new laws and regulations is not the best way of dealing potential problems that may be encountered with Internet content. Therefore, a multi-layered approach with the involvement of both public and private regulatory bodies at both national and international level is inevitable[31] to deal effectively with the current problems. The UK Government favours a co-regulatory approach in which there is a role to be played by industry self-regulation. However, whether the current proposals and the policy can address the problems effectively remains to be seen. Therefore, the following sections will also include a critique of the current proposals and the current policy of the UK Government.

ENFORCEMENT OF NATIONAL LAWS

This article identified child pornography as the most common and the most referred example of illegal content. So far, law enforcement agencies within the UK have been dealing successfully with child pornography-related offences (cre-

ation, possession and distribution offences)[32] ever since the Protection of Children Act 1978 and the Obscene Publications Act 1959 were amended by the Criminal Justice and Public Order Act 1994 to take into account the new technologies (such as computers, computer data and also computer generated images).[33]

There have been many police operations in relation to the availability of child pornography on the Internet[34] following the relevant laws being amended by the Parliament[35] and these operations resulted in many successful prosecutions involving possession and distribution of child pornography[36]

However, the application of the Obscene Publications Act 1959 and the availability and distribution of obscene content (not child pornography) have been more problematic from a UK perspective. There are not many cases brought under the 1959 legislation in relation to the Internet. One notable example is the **R v Graham Waddon**[37] case under the Obscene Publications Act.[38] Waddon was charged with publishing obscene articles contrary to s.2(1) Obscene Publications Act 1959 as he had maintained a commercial website featuring sexually explicit images in the USA. As publishing an article under s.1(3)(b) of the 1959 Act included data stored electronically and transmitted, Waddon was successfully prosecuted. He was given an 18-month prison sentence suspended for two years in September 1999.[39] Such cases are rare and this one certainly does not set up a precedent as the defendant pleaded guilty to 11 sample counts of publishing obscene articles on the Internet. However, the case stands as a good (or bad) example of the application of the obscenity legislation to the Internet.

In relation to the cyber-stalking and harassment issues, the NCIS Trawler report claimed that "E-mail harassment will increase as Internet usage grows."[40] However, such claims remain unfounded as the UK courts only witnessed a single Internet-related case under the Protection of Harassment Act since that legislation was enacted in 1997. The unique prosecution for Internet harassment or cyber-stalking involves the case of **Nigel Harris**[41] and Harris received a two year conditional discharge in March 1999 from the Horseferry Road Magistrates Court followed by a three year jail sentence in October 1999 for breaching a court order (not Internet-related).[42] At the time of writing, there were no cases involving hate speech and the Internet within the UK.[43]

The above examples clearly show that the legal system and the law enforcement agencies are capable of dealing with Internet-related illegalities if the perpetrators are within the jurisdiction.

This article also identified the publication of official secrets over the Internet to be a major concern for law enforcement and security agencies within the UK. Although it is not clear who published a list containing the names of more than 100 MI6 spies over the Internet, an ex MI6 officer, Richard Tomlison who lives abroad was accused by the UK Government of circulating the names over the Internet.[44] In this specific example, the Official Secrecy Act 1989 was not applicable as the perpetrators were outside the jurisdiction (or unknown). Therefore, there will be instances in which national laws will not be applicable or enforceable because of the global nature of the Internet.

Although within the ambit of the legal system, illegal content therefore, may not be perfectly dealt with by the legal system. In many instances, it may not be possible to identify the perpetrators or the criminal activity may take place in another jurisdiction where the matter may not be an act of illegality.

The global nature of the Internet and the pressures to deal with the availability of illegal Internet content inevitably resulted in new approaches to deal with such problems and, therefore, a new partnership approach between the Internet Service Providers and the law enforcement agencies has been seen as the best way to address criminal content and criminal activity over the Internet together with the improvement of law enforcement techniques in relation to Internet-related crimes.

The recently published *e-commerce@its.best.uk* report by the Cabinet Office[45] therefore recommended the improvement of the "technical capability of law-enforcement and regulators," and the establishment of an Internet Crime Unit[46] possibly within the Home Office. This idea was initially recommended by the NCIS report and endorsed by the Cabinet Office in its *e-commerce@its.best.uk report* "as a practical way of coordinating expertise and ensuring clear lines of responsibility".[47] The report claims that:

> A strengthened law-enforcement ability will send a clear signal to potential Internet criminals that Internet crime does not pay. It will help to boost the confidence of both E-commerce buyers and sellers. Similarly, stronger detection and presentation effort will deter hackers, spammers and those, such as paedophiles and racists, who place illegal material on the Internet.[48]

These recommendations have been accepted by the Association of Chief Police Officers (ACPO) crime committee and discussed by the ACPO Council, the NCIS, the National Crime Squad and HM Customs and Excise and they have drafted a National Hi-Tech Crime Strategy and Funding Bid.[49] The matter has also been considered by the Home Office[50] and in January 2000, a proposal for £377 000 to set up a High Tech Crime Planning Unit at NCIS was agreed by the Home Office as part of the overall NCIS levy settlement.[51] This resulted in the establishment of the National Hi-Tech Crime Unit in April 2001[52] which will have primary responsibility for investigating the most serious and organized hi-tech crime offences, ranging from attacks on national infrastructure and networks to the more traditional crimes involving new technologies such as the Internet.[53] According to Home Office Minister Charles Clarke "tackling paedophiles, terror groups, and commercial warfare on the World Wide Web is at the heart of the Government's drive to tackle the menace of Internet crime." Mr Clarke stressed that "new methods of cooperation are needed in order to investigate crime on the Internet,"[54] and that "it is vital that Internet Service Providers and telecommunication companies are alive to the need for cooperation with the law of enforcement".

Such a cooperation between the law enforcement bodies and the UK Internet Service Providers has been ongoing since late 1997. In November 1997, the Association of Chief Police Officers Computer Crime Unit together with the Internet Service Providers established the ACPO/ISPs Government Forum with the objective of developing good practice guidelines between Law Enforcement Agencies and the Internet Service Providers Industry, describing what information can lawfully and reasonably be provided to Law Enforcement Agencies, and the procedures to be followed.[55] Given the

concern over cybercrimes and cyber-criminals it is entirely understandable that the police and the ISPs should wish to develop mutual understanding and support, and to establish working relationships.[56] However, such a collaboration process should be transparent and accountable with clearly defined rules that take into account the rights of individual Internet users. Furthermore, those directly affected by such a collaboration, e.g. the users should also be represented in such a collaboration and therefore the partnership approach should include public interest groups and users' representatives.[57] Cooperation and reliance on the ISP industry is further emphasized under the Regulation of Investigatory Powers Act 2000 as far as the duty of maintenance of interception capability by the ISPs is concerned.[58] Apart from the cooperation of the Internet industry and the law enforcement agencies at the national level, the UK Government is also building international cooperation at policy level through a G8 sub-group on High Tech Crime and also taking an active role in the formation of the Council of Europe Cyber-crime Convention[59] as well as contributing to the European Union policy work on cybercrimes.[60]

The Draft Council of Europe Convention on Cyber-crime was discussed by the House of Commons Select Committee on European Scrutiny[61] and as "this type of crime poses a growing threat,"[62] effective action requires international collaboration according to the UK position. The work for the Council of Europe Convention started in September 1997 and the Convention will be finalized by September 2001.The Convention would require "state parties to ensure that their criminal law includes offences against the integrity, confidentiality and availability of computer data; copyright and related offences; and content-related offences such as the possession and distribution via the Internet of child pornography"[63] among other things.[64]

Therefore, illegal content issues are dealt both at a national and international level by the UK regulators and law enforcement bodies and governing this sort of content over the Internet requires a multi-layered and international effort. However, as far as the UK laws are concerned, some forms of illegal content does exist over the Internet and to the extent that the perpetrators are within the UK, the law enforcement agencies and the courts are dealing with such crimes as this section tries to explain. Moreover, the National Criminal Intelligence Service in its Project Trawler report "does not assess the risks or scale of criminal activity on the Internet to be as extensive as sometimes portrayed". Content-related criminal activity remains very low for the moment as far as such crimes are initiated from the UK.[65]

INTERNET SERVICE PROVIDERS LIABILITY

Furthermore, as a result of concerns over the Internet content and related criminal activity,[66] the Internet Service Providers (ISPs) were pressured into self-regulating themselves as they were seen by the law enforcement agencies to be responsible for the content that they carry[67] in their servers even though they have no control over third party Internet content. Similar pressures on the ISPs resulted with the successful prosecution of CompuServe in Germany in May 1998 mainly for the distribution of child pornography.[68]

Although pressured to self-regulate themselves, ISPs have not been prosecuted within the UK even though they may well be liable for the content they carry as in the German case of **Somm** under Section 3 of the 1978 Protection of Children Act.[69] However, Landgericht Munchen (Regional Court of Munich I, 20th Criminal Division) quashed the **Somm** decision in November 1999 and acquitted Somm following an appeal by both CompuServe and the prosecution in May 1998.[70]

Although all the above mentioned efforts both at a national and international level are welcome to deal with illegal Internet content, the prosecution of Internet Service Providers (ISPs) within the UK remains completely undesirable and cases such as **Somm** should be avoided at all costs.

The ISP liability issue may be resolved at a European level but the recently finalized European Parliament and Council Directive on certain legal aspects of electronic commerce in the Internal Market[71] offer only limited protection to ISPs with the introduction of an 'actual knowledge' test for removal of third party content from ISP servers.[72] Therefore, the practice known as 'notice and takedown' will be common practice for the removal of Internet content through the ISP servers. Such notices can be given either by hotlines like the Internet Watch Foundation (*see below*) for the removal of allegedly illegal content or by private companies or individuals for the removal of other forms of content including content deemed to be defamatory[73] or content that infringe copyright and trademark laws.The 'notice and takedown' provisions of the 1996 Defamation Act (Section 1) were criticized by Cyber-Rights & Cyber-Liberties (UK):

> It is totally unacceptable that an offended party should simply notify an Internet Service Provider claiming the information to be legally defamatory. The current state of the UK laws forces the ISPs to be the defendant, judge, and the jury at the same time. Notice should not be enough in such cases.[74]

Furthermore, the law enforcement agencies should act against the real perpetrators — those who create and circulate (or publish) the content over the Internet.[75] Putting pressure on the ISPs to resolve the content-related matters should not be the way forward[76] and will only hamper the development of the Internet and electronic commerce within UK.

A SELF-REGULATORY APPROACH?

Although the above sections set the scene and provide some criticism about the current national regulatory approach for Internet content, it is important to analyze some of the new approaches that are advocated for Internet content regulation.

Apart from the enforcement of national laws in relation to illegal Internet content, the UK Government favours self-regulatory solutions[77] for Internet content regulation rather than the introduction of any specific legislation (unlike the US Government).[78] The UK Government policy is also consistent with the European Union policy and with the European Commission's Action Plan on Safer Use of the Internet.[79]

The EU Action Plan, encourages the creation of a European network of hotlines to report illegal content such as child pornography by online users, the development of self regulatory and content-monitoring schemes by access and content providers, the development of internationally compatible and interoperable rating and filtering schemes to protect users, and measures to increase awareness of the possibilities available among parents, teachers, children and other consumers to help these groups to use the networks

whilst choosing the appropriate content and exercising a reasonable amount of parental control.

DEVELOPMENT OF HOTLINES FOR ILLEGAL CONTENT

Hotlines for reporting illegal Internet content has been promoted by the European Union's Action Plan and the UK's Internet Watch Foundation (IWF) represents one of the earliest examples of such an hotline. The IWF acts as a hotline for reporting illegal content, and this involves mainly child pornography. The IWF, as an industry based self-regulatory body, was announced in September 1996 (supported by the UK Government). The organization is a private body financed by the Internet Service Providers and it is not an accountable public body.

Its activities concentrate on the Usenet discussion groups and the organization acts upon Internet users reports sent via E-mail, fax, or telephone in relation to illegal Internet content. Once the IWF locate the "undesirable content" (according to its own judgment) through reports made by Internet users,[80] IWF informs all British ISPs for the removal of the content located. Furthermore, the hotline also contacts the law enforcement agencies (for example NCIS) in relation to these reports in addition to the ISPs.[81]

According to the first IWF annual report (which covers the period between December 1996 and November 1997),[82] there have been 781 reports to the Foundation from online users and in 248 of them action was taken. These reports resulted in the review of 4324 items, and the Foundation has taken action in 2215 of them (2183 referred to the Police and 2000 to ISPs). 1394 of these originated from the US while only 125 of the items originated from the UK.[83] According to IWF's second report (January - December 1998 statistics), the number of reports reached 2407 and in 447 action was taken (430 of the actions reports contained child pornography).[84] These involved 14 580 items in which the IWF took action on 10 548. 9176 of these were referred to NCIS, 541 to the UK police, and 9498 to the UK ISPs. 11.79% of this illegal content originated from the UK, while 49.05% originated from the USA. Furthermore, according to the third year statistics of the hotline (covering the period January - December 1999), there were 4809 reports involving 19 710 items. However, only 4% of the 11487 items on which the IWF took an action originated from the UK which is an improvement in respect to the 1998 statistics and shows that the problem of child pornography is not a growing problem in the UK and remains an international problem.

These figures tell us little as the actual amount of child pornography on the Internet is unknown.[85] It is, therefore, difficult to judge how successful the UK hotline has been so far despite its own claims and the UK Government claims to its success. While around 10 189 items were removed from the servers of UK ISPs (up until December 1999), it is not known how many new images are posted to various newsgroups (replacing those removed images) within the time framework of the above activities, nor it is known how much child pornography is out there in the Wild West Web while the activities of the hotline is concentrated on the Usenet discussion groups.

Another downside is that the efforts of the organization are concentrated on the newsgroups carried by the UK ISPs although more hotlines are developed in other countries and cooperation between these hotlines is expected in the near future.[86] This means that while illegal material is removed from the UK ISPs servers, the same material will continue to be available on the Internet carried by the foreign ISPs in their own servers.

Therefore, the expensive monitoring of the Internet at a national level is of limited value as the few problems created by the Internet remain global ones and thus require global solutions. While the UK Government should be involved in finding solutions to global problems with its international partners, the global problems do not justify expensive monitoring of the Internet at a national level by industry-based organizations. This is not an attempt to dismiss the roles that can be played by hotlines but there remains serious concerns for the policing role that can be played by such organizations. Privatized policing organizations are not acceptable to judge the suitability or illegality of Internet content and there is a serious risk for hotline operators to act as 'self-appointed judges' with an 'encouragement for vigilantism'.[87] According to Nadine Strossen, "These hotlines violate due process concepts that are also enshrined in international, regional, and national guarantees around the world."[88]

The IWF mainly deals with child pornography as mentioned above, but there are plans to expand its hotline duties and while child pornography may be an example of clear cut illegality (even though there are variations in national laws), the same cannot be true for other forms of Internet content such as hate speech.[89] The IWF hotline model is supported by the European Union's Action Plan and also by the Internet industry[90] that favours the creation of such organizations for assisting ISPs and law enforcement agencies in various countries. However, illegality remains a matter to be decided by courts of law and not by private organizations or by quasi-regulatory bodies and the industry proposals which advocate that the "task of evaluating the legality or illegality of specific data is difficult for Internet providers and should, therefore, be integrated into the work of hotlines"[91] is wrong in principle and would be unacceptable in democratic societies.

Undoubtedly, the availability and distribution of child pornography should be regulated as well as other illegal activities, whether on the Internet or elsewhere. The main concern of law enforcement and regulatory bodies should, however, remain the prevention of child abuse — the involvement of children in the making of pornography, or its use to groom them to become involved in abusive acts rather than the cleansing of the Internet from such images.[92] At least the former, more serious issue of prevention of child abuse, should be given a priority in national policies and organizations that deal with Internet policy should align their policies to take into account the prevention of child abuse.

DEVELOPMENT OF RATING AND FILTERING SYSTEMS

"Internet users are concerned about protecting children and vulnerable people from illegal or immoral material. A May 1999 survey of US parents showed that 78% have concerns about the content of Internet material to which their children have access. In the UK the IWF handled 2407 reported cases of illegal content in 1998, compared with 898 in 1997.

Control of content for consumers is thus a serious, and growing issue and a problem that must be solved."[93]

What the Cabinet Office report refers to as immoral content is often referred to as harmful content by the policy makers and in any case the sort of content that is referred to remains as legal content (in most cases) rather than illegal content as explained above. The area of harmful content has been problematic for the regulators so far and the main self-regulatory initiatives try to address this sort of Internet content.

The Cabinet Office report referred to a US study having not conducted its own survey in relation to Internet content-related concerns within the UK. The reference to illegal content and the role that has been played so far by the Internet Watch Foundation (its hotline function as explained above) has less implications for the issues of harmful content and the two policy issues should be kept separate and not confused by the policy makers. The confusing debates and arguments provided by the government and industry policy makers are the real reason behind the media hype about the availability of sexually explicit content and the availability of illegal content over the Internet.[94] As a consequence of such concerns, in February 1998, the Internet Watch Foundation (IWF), announced its consultation paper for the development of rating systems at a national level as a solution to dealing with harmful Internet content.[95]

The Department of Trade and Industry and the Home Office played key roles in the establishment of the IWF. According to Mrs Roche of the DTI, "As part of its remit to help ensure that the Internet can be a safe place to work, learn and play, the IWF has convened an advisory board comprising representatives of content providers, children's charities, regulators from other media, ISPs and civil liberties groups, to propose a UK-focused system for rating Internet content."[96] In reality, no civil liberties organizations were involved or consulted as was pointed by the Cyber-Rights & Cyber-Liberties (UK) November 1997 report, leaving the IWF a predominantly industry-based private organization with important public duties.[97] The two *Who Watches the Watchmen* reports by the non-profit organization Cyber-Rights & Cyber-Liberties (UK) questioned the accountability of the IWF to the public and openness and transparency of its procedures and decision making process as a quasi-regulatory body in November 1997 and in September 1998. However, to date there has not been any improvement in relation to the structure of the IWF and a review of this self-regulatory body by the DTI did not address these issues.[98]

Rating systems such as the Platform for Internet Content Selections (PICS)[99] works by embedding electronic labels in the Web documents to vet their content before the computer displays them.[100] The vetting system could include political, religious, advertising or commercial topics. These can be added by the publisher of the material, or by a third party (e.g. by an ISP, or by an independent vetting body). In addition to rating systems, it is important mention the availability and use of filtering software which is intended to respond to the references of parents making decisions for their own children. There are currently around 15 filtering products, (mainly US-based)[101] and these do not necessarily reflect the cultural differences in a global environment such as the Internet.

According to an IWF press release, rating systems would "meet parents' concerns about Internet content that is unsuitable for children". The IWF proposals are also supported by the UK Government which also supports "The deployment of the Platform for Internet Content Selection (PICS), and the development of ratings systems."[102] Furthermore, in many instances the Government and the members of the Parliament showed their support for the development and use of filtering and rating systems for the protection of children from 'immoral and harmful' Internet content or from potentially objectionable material as referred to by the DTI's *Net Benefit* document.[103] The Net Benefit document states that:

> Some classes of material are legal, and desired by some users, but expressly not desired by others. There is a risk that some users are put off using the Internet and engaging in electronic commerce because they fear unwanted exposure to offensive content.[104]

The Net benefit document follows on from the DTI's Secure Electronic Commerce Statement[105] that was mainly concerned about the regulation of the use of encryption technology and the development of electronic commerce and was issued in April 1998.[106] However, that statement also referred to Internet content matters and in Paragraph iv, (entitled "Internet content") stated that:

> As the Internet becomes a mass medium it is only right to ensure that the most vulnerable users are protected. This has meant supporting, and encouraging, such initiatives as the Internet Watch Foundation to ensure that the law is applied online in the same way as it is offline.

The policy developments in relation to Internet content therefore continued with the Net Benefit document (which was published in October 1998) which relies on self empowerment by concerned users as a priority for the UK. To achieve this, the DTI recommended "The use of rating systems which describe the content of a website objectively in accordance with a generally recognized scheme, and filtering software which enables the user to block access to websites according to their rating or if they are unrated."[107] According to John Battle, Minister for Science, Energy and Industry, "Such ratings and filtering tools can be extremely useful in helping parents and other adults who care for children to decide on the types of legal material they wish their children to access."[108]

The *e-commerce@its.best.uk* report which was published a year after the Net Benefit document encouraged software companies to supply free content-filtering software[109], but complained about the limited use of such software and tools by the Internet users.[110] However, there are initiatives under the National Grid for Learning programme to develop 'parents' websites' with the facility to download filtering software.[111]

Self-rating and filtering systems are also promoted by a recently published Memorandum on Internet Self-Regulation by the Bertelsmann Foundation[112] as empowering user choice. The Memorandum argued that "Used wisely, this technology can help shift control of and responsibility for harmful content from governments, regulatory agencies, and supervisory bodies to individuals." The Memorandum advocated for an "independent organization to provide a basic vocabulary for rating and to oversee updates to the system at periodic intervals". However, the

organizations that deal with the rating proposals including the UK's Internet Watch Foundation pursue an undemocratic and unaccountable process for developing such systems and it is not independent.

Furthermore, according to the *e-commerce@its.best.uk* report, the development of rating and filtering systems and the wide availability of such systems "will make it clear that the Government takes parents' concerns seriously and is prepared to take active measures to meet those concerns".[113]But the Government continues to assume that parents are concerned about Internet content. However, the so-called consultation document by the IWF did not discuss whether these systems are suitable for Britain or whether they are needed at all. In fact, a decision has been taken by the UK organization to develop these systems, and the consultation paper addressed how to develop these systems and had a set of recommendations which suggested that the decision in principle was already taken — rating systems are good and should be developed for use in Britain.

Despite the establishment consensus, it would have been more appropriate to establish a Working Group, with both representatives from the public and private sector to assess the real problem of illegal and harmful content at a UK level rather than trying to find temporary or ineffective solutions to activities which do not necessarily take place within the British jurisdiction.[114]

A substantial study together with a public consultation in this field was needed in the UK (and still needed) before moving forward with the current proposals. It therefore remains as the duty of the UK Government to set up such an 'independent' working group (or conduct a Select Committee inquiry) which would assess the real amount of problems and seek the best solutions in an open, transparent, and accountable way without infringing the rights of UK citizens. However, the creation of such an independent body or wide public consultation is not expected in the near future.[115] At the same time, the IWF continues with its policy making process and the development of rating and filtering systems within the UK, the European Union,[116] and elsewhere[117] despite the potential problems associated with such systems as will be explained in the next section.[118]

A CRITIQUE OF RATING AND FILTERING SYSTEMS

As far as the rating and filtering systems are concerned, it is important to provide the whole picture which includes the limitations and criticisms of the use and development of rating and filtering systems for the availability of harmful content over the Internet which are usually not considered by government representatives, the European Commission, and by the industry bodies.[119]

> Originally promoted as technological alternatives that would prevent the enactment of national laws regulating Internet speech, filtering and rating systems have been shown to pose their own significant threats to free expression. When closely scrutinized, these systems should be viewed more realistically as fundamental architectural changes that may, in fact, facilitate the suppression of speech far more effectively than national laws alone ever could.[120]

First of all, although the use and development of rating systems are welcome by various governments including the UK Government, the capacity of these tools is limited to certain parts of the Internet and therefore these tools do not address the availability of harmful content issue fully. But at no point do the official UK Government statements address or warn about the limitations of these technologies.

Rating systems are designed for the World Wide Web sites while leaving out other Internet-related communication systems such as the chat environments,[121] file transfer protocol servers (ftp),[122] Usenet discussion groups, real-audio and real-video systems which can include live sound and image transmissions, and finally the ubiquitous E-mail communications. These systems cannot be rated with the currently available rating systems and therefore the assumption that rating systems would make the Internet a 'safer environment' for children is wrong as the WWW content represents only a fraction of the whole of the Internet content. Although it may be argued that the World Wide Web represents the more fanciful and the most rapidly growing side of the Internet, the problems that are thought to exist by the regulators over the Internet are not World Wide Web-specific.

Secondly, even when the rating technology is applicable (to World Wide Web pages), it is not clear what the regulators have in mind when it comes to what sort of content should be rated. Examples from official statements in which the category is referred to as 'harmful', 'immoral' or as 'objectionable' content have been provided above. However, there is no consensus as to what is actually being referred to by the regulators (perhaps apart from the availability of sexually explicit content over the Internet). In all cases, the targeted category of Internet content remains within the limits of legality rather than illegality.

According to the UK Internet Watch Foundation, there is "A whole category of dangerous subjects" that require ratings and these are information related to drugs, sex, violence, information about dangerous sports like bungee-jumping, and hate speech material.[123] This kind of content would certainly include such publications as *The Anarchist Cookbook*[124] which can be downloaded from not only WWW sites[125] but also can be obtained through ftp servers or through the use of automatic E-mail services apart from its availability through well-known bookshops such as Waterstones, Dillons, and Amazon.co.uk within the UK.Therefore, rating systems would not in any way be a complete solution to content deemed harmful to minors.

Thirdly, if the duty of rating is handed to third parties, this would pose free speech problems and with few third-party rating products currently available, the potential for arbitrary censorship increases (note that no UK-based third party rating body exists currently).This would mean that there will be no space for free speech arguments and dissent because the ratings will be done by private bodies and the governments will not be involved 'directly'.When censorship is implemented by government threat in the background, but run by private parties, legal action is nearly impossible, accountability difficult, and the system is not open or democratic. In fact, none of the criticisms in relation to these issues were taken into account by the IWF.[126]

Fourthly, another downside of relying on such technologies is that these systems are defective[127] and in most cases they are used for the exclusion of socially useful websites and information. The general excuse remains the protection of children from harmful content and also the duty of the industry to give more choices to the consumers. Filtering software and rating systems will be used to exclude minority views and socially useful sites rather than protecting children from anything.[128]

Fifthly, while the children's access is the most cited excuse for the regulation of the Internet, this global medium is not only accessed and used by children. In fact, it is not possible for children to have their own Internet accounts without the involvement of a parent or adult as it is not possible to get an Internet account through an Internet Service Provider before the age of 18 in almost all countries including the UK. Therefore, children's access to the Internet is already limited as it is not possible to obtain an account without the involvement of a parent. Therefore, there is always a role to play for the adults and parents in relation to the children's access to the Internet and adults should act responsibly towards children's Internet usage rather than relying on technical solutions that do not fully address Internet content-related problems. Librarians and teachers should also have a role to play as far as access to the Internet is provided from public libraries and schools for children.

Moreover, it has been reported many times that, filtering systems and software are over-inclusive and limit access and censor inconvenient websites, or filter potentially educational materials regarding AIDS and drug abuse prevention. Therefore, 'censorware' enters homes under the guise of 'parental control' and as a purported alternative to government censorship but in fact such systems impose the standards of the software developers rather than leaving the freedom of choice and browsing to the consumers who buy and rely on such products. The companies creating this kind of software provide no appeal system to content providers who are 'banned or blocked', thereby "subverting the self-regulating exchange of information that has been a hallmark of the Internet community".[129]

Lastly, and more importantly, rating and filtering systems with blocking capabilities would allow repressive regimes to block Internet content, or mandate the use of such tools. "By requiring compliance with an existing rating system, a state could avoid the burdensome task of creating a new content classification system while defending the rating protocol as voluntarily created and approved by private industry."[130]

Such a concern on the part of civil libertarians remains legitimate in the light of the recently introduced Australian Broadcasting Services Amendment (Online Services) Act which mandates blocking of Internet content based upon existing national film and video classification guidelines.[131] So there is governmental support for mandatory rating systems and this is an option that may be considered by not only repressive regimes but by other democratic societies like the UK.

Furthermore, any regulatory action intended to protect a certain group of people, such as children, should not take the form of an unconditional and universal prohibition on using the Internet to distribute content that is freely available to adults in other media. The US Supreme Court stated in **Reno v ACLU**,[132] that "the Internet is not as 'invasive' as radio or television" and confirmed the finding of the US Court of Appeal that "communications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden". However, the US Government tried to regulate the Internet once again with the Child Online Protection Act (COPA) which was enacted by the US Congress as part of an omnibus appropriations bill. COPA intended to punish 'commercial' online distributors of material deemed 'harmful to minors' with up to six months in jail and a $50 000 fine. However, COPA was immediately challenged by civil liberties organizations including the ACLU, EPIC in court in October 1998. Furthermore, COPA was criticized by the members of the Global Internet Liberty Campaign (GILC) which stated that:

> COPA will not be effective in keeping from minors material that might be inappropriate for them. No criminal provision will be more effective than efforts to educate parents and minors about Internet safety and how to properly use online resources. Moreover, we note again that the Internet is a global medium. Despite all the enforcement efforts that might be made, a national censorship law cannot protect children from online content they will always be able to access from sources outside of the United States.[133]

On 19 November 1998, Judge Lowell A. Reed, Jr. stated that the plaintiffs have shown "a likelihood of success on the merits of at least some of their claims" that the COPA violates the First Amendment rights of adults. Significantly, the judge emphasized that the temporary restraining order, applies to all Internet users, and not just the plaintiffs in the case.[134] In June 2000, in a unanimous decision, a three-judge panel of the Third Circuit Court of Appeals in **ACLU v Reno II**,[135] struck down COPA by stating that the 1998 law "imposes a burden on speech that is protected for adults".

It should therefore be noted that current solutions offered at various regulatory for as such as the development of rating and filtering systems, may not be the real answers and solutions for the existing problems and the development of such systems may result in censorship of Internet content which is not illegal at all. Furthermore, as the Economic and Social Committee of the European Commission on its report[136] on the European Commission's "Action Plan on promoting safe use of the Internet" pointed out, it is highly unlikely that the proposed measures will in the long term result in a safe Internet with the rating and classification of all information on the Internet being 'impracticable'.[137] The Committee, therefore, concluded that there is "little future in the active promotion of filtering systems based on rating".[138] But so far, the promotion of such tools continue by the Internet industry and by the regulators within the UK and elsewhere.

CONCLUSION

This article tries to provide an overview of the Internet regulation within the UK with special reference to illegal and harmful content. For both categories of Internet content, there is no unique solution for effective regulation; the emergence of 'Internet governance' entails a more diverse and fragmented

regulatory network with no presumption that these are anchored primarily in the nation-states.

Governance theorists are beginning to recognize that "objects of governance are only known through attempts to govern them"[139] and "governance is not a choice between centralization and decentralization. It is about regulating relationships in complex systems,"[140] and the Internet does provide a great challenge for governance.

Therefore, a multi-layered approach[141] is inevitable as pointed out earlier in this article in which a mixture of public and private bodies will be involved for Internet governance including the individual Internet users for self-control as far as harmful Internet content is concerned. A multi-layered approach will also include layers at a supranational and international level of Internet governance apart from the national level. Furthermore, "If such mechanisms of international governance and re-regulation are to be initiated, then the role of nation states is pivotal."[142] Hence, it would be wrong to dismiss the role that may be played by the governments especially for the creation of laws and for maintaining the policing of the state.

However, at a national level, it is now widely accepted that "government cannot simply regulate to achieve its aims in this new global electronic environment,"[143] and therefore a "light regulatory touch" is preferred for the development of E-commerce. Although there has been much emphasis for a partnership between the government and the industry "to get the right balance" to build confidence and to protect consumers in the information age, that balance should reflect and respect the rights of the individual Internet users, an issue often not considered by the regulators and by the industry. To achieve such a balance which takes into account individual rights and not only the interests of the business community, there is an urgent need for openness, accountability, and transparency in relation to regulatory initiatives[144] aimed at Internet content at the national level, rather than knee jerk reaction to such media hyped coverage of cases such as the **Gary Glitter** case.[145]

At a supranational (for example within the European Union, or within the Council of Europe) or international level (for example within the OECD, or within the United Nations),[146] we will witness more cooperation between various police forces including the Interpol (which holds regular meetings for law enforcement agencies dealing with cybercrimes for stimulating further collaboration) for Internet-related criminal activity but alignment of national criminal laws 'in general' seems not to be a feasible option due to the moral, cultural, economic, and political differences between the states. It is possible that some sort of consensus may be established as far as some specific crimes such as child pornography are concerned following the development of the Council of Europe's Cybercrime Convention.[147]

This is one reason why the European Commission preferred a self-regulatory approach for the European Union with its Action Plan which promotes the industry-based proposals for a "safer use of the Internet".[148] Furthermore, according to a recent House of Commons Select Committee on Culture Report - The Multi-Media Revolution,[149] international initiatives will have an important impact on national Internet regulation but at the same time "the question is whether such attempts at regulation can be anything more than optimistically indicative rather than genuinely effective".[150]

So, there is no unique effective solution at an international level. That is why some argue for the development of rating and filtering systems to deal with harmful Internet content. However, the current technology does not seem to respect these legitimate differences between nation-states.

It is the submission of this article that the preferred solutions for the availability of harmful Internet content have not been carefully assessed or examined by the UK Government. Therefore, some of these initiatives favoured by the government (and by the European Commission)[151] but enforced or developed by quasi-governmental bodies would almost amount to censorship of legal Internet content.[152]

The European Convention on Human Rights and other international human rights instruments such as the Universal Declaration of Human Rights, and the International Covenant on Civil and Political Rights, enshrines the rights to freedom of expression and access to information. These core documents explicitly protect freedom of expression without regard to borders, a phrase especially pertinent to the global Internet.[153] The proposed rating and filtering systems would violate these freedom of expression guarantees.[154] Alternatives to current available solutions (such as filtering and rating systems) should be considered before trying to build the likes of fortress UK on a global medium with too much emphasis on the protection of children from harmful content. Instead, there should be more emphasis on promoting the Internet as a positive and beneficial medium and there is urgent need for awareness of Internet usage. If a 'light regulatory touch' with an emphasis on self-regulatory or co-regulatory initiatives represent the government's vision, then 'self' should mean individuals rather than self-regulation by the Internet industry without the involvement of individuals and Internet users.

Yaman Akdeniz, Report Correspondent, Director of Cyber-Rights & Cyber-Liberties (UK).

FOOTNOTES

[1]By various bodies such as the Internet Watch Foundation within the UK (http://www.iwf.org.uk); Internet Content Rating for Europe (http://www.incore.org), and the Internet Content Rating Association (see: http://www.icra.org).

[2]Decision No /98/EC of the European Parliament and of the Council of adopting a Multiannual Community Action Plan on promoting safer use of the Internet by combatting illegal and harmful content on global networks, December 1998, at<http://www2.echo.lu/legal/en/internet/actplan.html>. For a critique of the EU proposals see Walker, C. and Akdeniz, Y., "The governance of the Internet in Europe with special reference to illegal and harmful content," [1998] *Criminal Law Review*, December Special Edition: Crime,

Criminal Justice and the Internet, pp. 5-19.

[3]See Department of Trade and Industry, *Net Benefit: The Electronic Commerce Agenda for the UK*, DTI/Pub 3619, October 1998, at <http://www.dti.gov.uk/CII/netbenefit.html> and the Cabinet Office Performance and Innovation Unit Report, *e-commerce@its.best.uk: The Government's Strategy*, September 1999, at <http://www.cabinet-office.gov.uk/innovation/1999/ecommerce/index.htm>.

[4]For the formation of the IWF see Safety-Net proposal, "Rating, Reporting, Responsibility, For Child Pornography & Illegal Material on the Internet" adopted and recommended by the Executive Committee of ISPA - Internet Services Providers Association, LINX - London Internet Exchange and the Internet Watch Foundation at <http://dtiinfo1.dti.gov.uk/safety-net/r3.htm>. See further the Review of the Internet Watch Foundation: A report for the DTI and Home Office by KPMG and Denton Hall, February 1999, at http://www.dti.gov.uk/public/frame2.html. For a critique of the IWF and its activities, see Cyber-Rights & Cyber-Liberties (UK) Report: "Who Watches the Watchmen: Part II - Accountability & Effective Self-Regulation in the Information Age," September 1998 at <http://www.cyber-rights.org/watchmen-ii.htm>.

[5]See European Commission Communication, Illegal and Harmful Content on the Internet, Com (96) 487, Brussels, 16 October 1996; and European Commission Green Paper on the Protection of Minors and Human Dignity in Audovisual and Information Services, Brussels, 16 October 1996.

[6]*Ibid.* at page 10.

[7]Decision No /98/EC of the European Parliament and of the Council of adopting a Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, December 1998. See further Akdeniz, Y., "The European Union and illegal and harmful content on the Internet," (1998) *Journal of Civil Liberties* 3(1), March, 31-36; Walker, C., & Akdeniz, Y., "The governance of the Internet in Europe with special reference to illegal and harmful content," [1998] *Criminal Law Review*, December Special Edition: Crime, Criminal Justice and the Internet, pp. 5-19.

[8]*Ibid*.

[9]Next stop is bookshops as a book named Anarchist's Cookbook is available through well known bookshops such as Waterstones and Dillons within the UK.

[10]See generally Akdeniz, Y., *Sex on the Net? The Dilemma of Policing Cyberspace*, Reading: South Street Press, 1999.

[11]See Reidenberg, J.R., "Governing Networks and Cyberspace Rule-Making" (1996) *Emory Law Journal* 45. See generally Akdeniz, Y., & Walker, C., &, Wall, D., (eds), *The Internet, Law and Society*, Addison Wesley Longman, 2000.

[12]See generally Akdeniz, Y., "Child Pornography," in Akdeniz, Y., & Walker, C., &, Wall, D., (eds), *The Internet, Law and Society*, Addison Wesley Longman, 2000. See further Akdeniz, Y., 'The Regulation of Pornography and Child Pornography on the Internet,' 1997 (1) The Journal of Information, Law and Technology (JILT), at <http://elj.warwick.ac.uk/jilt/internet/97_1akdz/default.htm>.

[13]In October 1996, the National Criminal Intelligence Service (NCIS) launched Project Trawler to study the extent of criminal misuse of information technology, and the methods law enforcement officials should use. See Uhlig, R., Hyder, K., "E-mail open to police scrutiny," *The Daily Telegraph*, 9 June, 1997.

[14]See NCIS, *Project Trawler: Crime On The Information Highways*, 22 June 1999.

[15]Under section 1(1) of the Official Secrets Act 1989, "A person who is or has been - (a) a member of the security and intelligence services, or (b) a person notified that he is subject to the provisions of this subsection, is guilty of an offence if without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services or in the course of his work while the notification is or was in force.

[16]For example the NCIS Project Trawler report did not refer to the issues that may be related to the Official Secrecy Act. See NCIS, *Project Trawler: Crime On The Information Highways*, 22 June 1999.

[17]See Davis, D., "Criminal Law and the Internet: The Investigator's Perspective," [1998] *Criminal Law Review*, December Special Edition, pp. 48-61.

[18]See Wall, D., "Policing and the Regulation of the Internet," [1998] *Criminal Law Review*, December Special Edition, pp. 79-90; Sieber, U., "Legal Aspects of Computer-Related Crime in the Information Society," Legal Advisory Board, European Commission, January 1998, at <http://www2.echo.lu/legal/en/comcrime/sieber.html>.

[19]See Akdeniz, Y., "Section 3 of the Computer Misuse Act 1990: an Antidote for Computer Viruses!" [1996] 3 *Web Journal of Current Legal Issues*.

[20]See "From hackers with love: the computer bug that brought world business to its knees," *The Independent*, 5 May, 2000.

[21]The Melissa virus first appeared on the Internet in March of 1999. It spread rapidly throughout computer systems in the United States and Europe. It is estimated that the virus caused $80 million in damages to computers worldwide. David Smith pleaded guilty on 9 December 1999 to state and federal charges associated with his creation of the Melissa virus. See **United States of America v David Smith**, Criminal No. 99-18 U.S.C.§ 1030(a)(5)(A) information, United States District Court District of New Jersey.

[22]BBC News, "Canada charges hacker suspect," 20 April 2000; Royal Canadian Mounted Police Press Release, "Charges laid in the case of attacks against American electronic commerce sites," (Montreal), 18 April 2000.

[23]See **Handyside v UK**, App. no. no. 5493/72, Ser A vol.24, (1976) 1 EHRR 737.

[24]See further **Castells v Spain**, App. no.11798/85, Ser.A vol.236, (1992) 14 EHRR 445.

[25]See generally Sieber, U., "Legal Aspects of Computer-Related Crime in the Information Society," Legal Advisory Board, European Commission, January 1998.

[26]See for example the Children and Young Persons (Harmful Publications) Act 1955 which is enacted to prevent the dissemination of certain pictorial publications harmful to children and young persons. Under section 2(1) of the 1955 legislation, a person who prints, publishes, sells or lets on hire a work to which this Act applies, or has any such work in his possession for the purpose of selling it or letting it on hire, shall be guilty of an offence and liable, on summary conviction, to imprisonment for a term not exceeding four months or to a fine not exceeding [level 3 on the standard scale] or to both.

[27]Under Article 10(2) of the European Convention on Human Rights states that "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, … for the protection of health or morals ..." See for example **Handyside v UK**, App. no. no. 5493/72, Ser A vol.24, (1976) 1 EHRR 737.

[28]Cabinet Office Performance and Innovation Unit Report, *e-commerce@its.best.uk: The Government's Strategy*, September 1999, at <http://www.cabinet-office.gov.uk/innovation/1999/ecommerce/index.htm>.

[29]*Ibid* at para 10.6.

[30]See The House of Commons Select Committee on Trade and Industry, "Report on Building Confidence in Electronic Commerce: The Government's Proposals," HC 187, seventh report of session 1998-99, 19 May 1999. See further Akdeniz, Y.; Taylor, N.; Walker, C., Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights, [2001] *Criminal Law Review*, (February), pp. 73-90; and Bowden, C., & Akdeniz, Y., "Cryptography and Democracy: Dilemmas of Freedom," in Liberty eds., Liberating Cyberspace: Civil Liberties, Human Rights, and the Internet, London: Pluto Press, 1999, 81-125. An online version is at <http://www.cyber-rights.org/reports/yacb.pdf>.

[31]As argued by the author in an earlier piece, see Akdeniz, Y., "Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach," in eds Edwards, L., and Waelde, C., *Law and the Internet: Regulating Cyberspace*, Oxford: Hart Publishing, 1997, pp. 223-241.

[32]See a recent controversial decision of the Court of Appeal in the case of **R v Jonathan Bowden** (1999), CA (Otton LJ, Smith J, Collins J) 10/11/99 involving making of child pornography by downloading images from the Internet. See further Akdeniz, Y., "Child Pornography," in Akdeniz, Y., & Walker, C., &, Wall, D., (eds), *The Internet, Law and Society*, Addison Wesley Longman, 2000.

[33]See further Akdeniz, Y., "Computer Pornography: A Comparative Study of the US and UK Obscenity Laws and Child Pornography Laws in Relation to the Internet," [1996] *International Review of Law, Computers and Technology* 10 (2), pp. 235-261.

[34]Operation Starburst and Operation Cathedral are among many other police investigations into the use of the Internet by paedophiles. See <http://www.cyber-rights.org/reports/child.htm> for further information.

[35]Note also the recent amendments made to the 1978 Act by the Criminal Justice and Court Services Act 2000 in relation to penalties under section 1 offences.

[36]See generally Akdeniz, Y., "Child Pornography," in Akdeniz, Y., & Walker, C., &, Wall, D., (eds), *The Internet, Law and Society*, Addison Wesley Longman, 2000. See further **R v Fellows and Arnold** [1997] 1 Cr.App.R. 244; Davis, D., *The Internet Detective - An Investigator's Guide*, Appendix D, Police Research Group, Home Office, 1998; Davis, D., "Criminal Law and the Internet: The Investigator's Perspective," [1998] *Criminal Law Review*, December Special Edition, pp 48-61; See Akdeniz, Y., "Regulation of Child Pornography on the Internet: Cases and Materials," at <http://www.cyber-rights.org/reports/child.htm>. Last updated May 2001.

[37]**R v Graham Waddon** (1999), Southwark Crown Court (Judge Hardy) 30 June, 1999, Court of Appeal (Criminal Division), 6 April 2000.

[38]Another notable case involves the prosecution of a French citizen living in the UK, Stephane Perrin, in November 2000 who was imprisoned for 30 months under the Obscene Publication Act 1959 for the provision of commercial obscene materials through a US based Internet site. Guardian Unlimited, Net pornographers face harsher sentences, November 6, 2000, at <http://www.guardian.co.uk/Archive/Article/0,4273,4087129,00.html>. See further Stephane Perrin's Case and related information at <http://www.cyber-rights.org/documents/stephane_perrin.htm>.

[39]Wilson, J., "Net porn baron escapes jail," *The Guardian*, 7 September 1999.

[40]See NCIS, *Project Trawler: Crime On The Information Highways*, 22 June 1999.

[41]See Seenan, G., "Computer programmer sentenced over banned visit to ex-lover," *The Guardian*, 16 October, 1999; Born, M., "Country's first E-mail stalker is convicted," *The Daily Telegraph*, 24 March, 1999. See further Ellison, L., & Akdeniz, Y., "Cyber-stalking: the Regulation of Harassment on the Internet," [1998] *Criminal Law Review*, December Special Edition: Crime, Criminal Justice and the Internet, pp. 29-48.

[42]Note also a similar prosecution in Scotland, "E-mail 'stalker' jailed for nine months," *The Times*, 25 February 2000.

[43]Note a debate on this issue within the House of Lords: The Internet: Race Hatred Material, House of Lords, Hansard, 11 December 2000.

[44]See Wired News, "Britain Shuts Down Spy Sites," 12 May 1999; The Mirror, "TRAITOR: Ex-spy puts names of MI6 agents on Internet in revenge for getting the sack," 13 May 1999, Evans, M., "Government fears that rogue website might put lives at risk," *The Times*, 13 May 1999.

[45]Cabinet Office Performance and Innovation Unit Report, *e-commerce@its.best.uk: The Government's Strategy*, September 1999, at <http://www.cabinet-office.gov.uk/innovation/1999/ecommerce/index.htm>.

[46]*Ibid*, recommendation 10.5.

[47]*Ibid*, para 10.46. "The proposed national unit would have three broad roles: to investigate the most serious 'IT crimes'; to act as a centre of excellence for 'cybercrime' issues; and to support local forces which encounter offenders using sophisticated IT skills." (From the NCIS Project Trawler Report: Key Judgements section, June 1999).

[48]*Ibid*, para 10.47.

[49]This was presented to the Home Office on 29 November 1999. The key elements of the strategy are the development of a multi-agency National Hi-Tech Crime Unit supporting enhanced and nationally coordinated local activity against hi-tech crime.

[50]*Ibid*, para 10.48.

[51]The funding bid for the additional costs of the strategy (£51 million over three years) are being considered in the Spending Review 2000.

[52]NCIS Press Release, Launch of the United Kingdom's first National Hi-Tech Crime Unit, 18/01, 18 April 2001, at <http://www.cyber-rights.org/documents/ncis_1801.htm>. See further House of Commons Hansard Written Answers for 21 Nov 2000 (pt 14), Cyber Crime.

[53]See further the Home Office press notice, New hi-tech crime investigators in £25 million boost to combat cybercrime, 359/2000, 13 November 2000, at <http://www.cyber-rights.org/documents/hi-tech.htm>.

[54]Home Office Press Release, "Making the Internet Safe," (306/99), 4 October 1999.

[55]The first meeting entitled as "The Police Service and the Internet - Issues for Debate" was held at the DTI on 7 November 1997.

[56]See further Akdeniz, Y, & Bohm, N, "Internet Privacy: New Concerns about Cyber-Crime and the Rule of Law," (1999) *Information Technology & Communications Law Journal* (5) pp. 20-24.

[57]Akdeniz, Y., "New Privacy Concerns: ISPs, Crime prevention, and Consumers' Rights," [2000] *International Review of Law, Computers and Technology*, 14 (1), 55-61; Akdeniz, Y., "Policing the Internet: Regulation and censorship," chapter in Gibson, R, & Ward, S., (eds), *Reinvigorating Democracy? British Politics and the Internet*, Ashgate, 2000, pp. 169-188.

[58]Note sections 12-14 of the RIP Act 2000. See further Akdeniz, Y.;

Taylor, N.; Walker, C., Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights, [2001] *Criminal Law Review*, (February), pp. 73-90.

[59]European Committee on Crime Problems (CDPC), Committee of Experts on Crime in Cyberspace (PC-CY), Draft Convention on Cyber-crime Declassified – Public version, PC-CY (2000) Draft No. 19, Prepared by the Secretariat Directorate General I (Legal Affairs), Strasbourg, 25 April 2000. The text of the draft Convention can be found at: <http://conventions.coe.int/treaty/en/projects/cybercrime.htm>. As of April 2001, the 25th version of the draft Convention is published and the draft Convention has been approved by the Parliamentary Assembly of the Council of Europe in its 2001 Ordinary Assembly Session during 23-27 April 2001.

[60]See the European Scrutiny Committee Reports, First Report, 7 December 1998, HC 34-I, Session 1998-99, (High Tech Crime).

[61]Select Committee on European Scrutiny Twenty-First Report, HC 34-xxi, 21 June 1999.

[62]*Ibid*.

[63]*Ibid.*

[64]The draft Convention is also supported outside the member states of the Council of Europe. Given the importance of the subject, non-member States, such as Canada, Japan, South-Africa and the United States, also actively participate in the negotiations and the G8 countries do support the draft Convention.

[65]See the IWF statistics at <http://www.iwf.org.uk/about/stats/stats.html> (last updated on 16/02/99).

[66]Mainly because of the availability of child pornography on the Internet (mainly through the Usenet discussion groups) and its provision by the ISPs.

[67]See generally the Letter from the Metropolitan Police to the UK ISPs, August 1996, at <http://www.cyber-rights.org/documents/themet.htm>.

[68]See the Criminal case of Somm, Felix Bruno, File No: 8340 Ds 465 JS 173158/95, Local Court (Amtsgericht) Munich. An English version of the case is available at <http://www.cyber-rights.org/isps/somm-dec.htm>. See further Sieber, U., "Control possibilities for the prevention of criminal content in computer networks," Part I in [1999] 15 *CLSR* 1, 34-39; Part II in [1999] 15 *CLSR* 2, 90-100, Part III in [1999] 15 *CLSR* 3, 168-181 for an examination of the German Information and Communications Act (IuKDG); and Sieber, U., "Responsibility of Internet Providers - A comparative legal study with recommendations for future legal policy," [1999] 15 *CLSR* 5, 291-310. See further Julia-Barcelo, J., "Liability for On-line Intermediaries: A European Perspective," [1998] *EIPR* 12, 453-463; Bodard, K., De Hert, P., De Schutter, B., "Crime on Internet: A Challenge to Criminal Law in Europe," (1998) *MJ* 5, 222-261.

[69]Section 3 of the 1978 Act states that "Where a body corporate is guilty of an offence under this Act and it is proved that the offence occurred with the consent or connivance of, or was attributable to any neglect on the part of, any director, manager, … he, as well as the body corporate, shall be deemed to be guilty of that offence and shall be liable to be proceeded against and punished accordingly. See for an interpretation Leong. G., "Computer Child Pornography - The Liability of Distributors?" [1998] *Criminal Law Review* Special Edition: Crime, Criminal Justice, and the Internet, (December), pp. 19-29.

[70]"Germany clears Net chief of child porn charges," The Independent, 18 November 1999. Note also the French case of League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, v Yahoo! Inc. (USA), Yahoo France, Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order, 20 November 2000.

[71]European Commission, "Proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market," COM(1998) 586 final, 98/0325 (COD), Brussels, 18.11.1998; European Commission, Amended proposal for a European Parliament and Council Directive on certain legal aspects of electronic commerce in the Internal Market (presented by the Commission pursuant to Article 250 (2) of the EC-Treaty), COM(1999)427 final, 98/0325 (COD). (Official Journal of the European Communities) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce") vol 43, OJ L 178 17 July 2000 p.1.

[72]See articles 13 and 14 of the Directive.

[73]This is already possible under section 1 of the Defamation Act, and "notice and takedown" is common practice for the removal of content alleged to be defamatory. See for example Akdeniz, Y., Case Analysis: **Laurence Godfrey v Demon Internet Limited**, *Journal of Civil Liberties*, July 1999; Cyber-Rights & Cyber-Liberties (UK), *Hulbert's Case, the Lord Chancellor and Censorship of the Internet*, 11 November, 1999; and Akdeniz, Y., & Rogers, W.R.H., "Defamation on the Internet," in Akdeniz, Y., & Walker, C., &, Wall, D., (eds), *The Internet, Law and Society*, Addison Wesley Longman, 2000.

[74]Cyber-Rights & Cyber-Liberties (UK) Press Release, "UK ISP found liable for defamation," 26 March, 1999, at <http://www.cyber-rights.org/press>. See also; Uhlig, R., "Libel setback for Demon," *The Daily Telegraph*, Connected Section, 1 April 1999; and Akdeniz, Y., "The case for free speech," *The Guardian*, (Online Section), 27 April 2000.

[75]Note that in Thailand, the Thai police ordered 17 ISPs to block pornographic websites that superimpose images of Thai actresses on naked images. Newsbytes, "Thai police order ISPs to block sites," 26 November, 1999, at <http://www.newsbytes.com/pubNews/99/139926.html>. See further "Porn swoop worries Net advocates," *The Nation* (Bangkok, Thailand), 27 November 1999.

[76]The Internet Watch Foundation was established as an industry response to law enforcement concerns in September 1996. Furthermore, the Association of Chief Police Officers (ACPO), Government and the Internet Service Providers Forum was established in November 1997 to create further partnership between the Internet industry and the law enforcement agencies within the UK to address Internet related criminal activity. See Akdeniz, Y, & Bohm, N, "Internet Privacy: New Concerns about Cyber-Crime and the Rule of Law," (1999) *Information Technology & Communications Law Journal* (5) 20-24; Akdeniz, Y., Bohm, N., & Walker, C., "Internet Privacy: Cyber-Crimes vs Cyber-Rights," (1999) *Computers & Law*, (10) 1, April/May, 34-39; and Akdeniz, Y., "New Privacy Concerns: ISPs, Crime prevention, and Consumers' Rights," [2000] *International Review of Law, Computers and Technology*, 14 (1), 55-61.

[77]See Safety-Net proposal, "Rating, Reporting, Responsibility, For Child Pornography & Illegal Material on the Internet" adopted and recommended by the Executive Committee of ISPA - Internet Services Providers Association, LINX - London Internet Exchange and the Internet Watch Foundation at <http://dtiinfo1.dti.gov.uk/safety-net/r3.htm>.

[78]See Communications Decency Act 1996 (47 USC s.223); ACLU v Reno (117 S. Ct. 2329 (1997); Akdeniz, Y., "Censorship on the Internet" (1997) 147 New Law Journal 1003. See further the US Child Online Protection Act (<http://www.epic.org/free_speech/censorship/copa.html>) and the related case of **American Civil Liberties Union, et al. v Janet Reno**, Civil Action No. 98-5591, United States District Court for the Eastern

District of Pennsylvania, (February 1, 1999), 31 F. Supp. 2d 473; 1999 U.S. Dist. Lexis 735; 27 Media L. Rep. 1449; 14 Comm. Reg. (P & F) 1145, at <http://www.epic.org/free_ speech/copa/pi_decision.html>. In June 2000, in a unanimous decision, a three-judge panel of the Third Circuit Court of Appeals in ***ACLU v. Reno II***, No. 99-1324, struck down COPA. For the full decision see <http://pacer.ca3.uscourts.gov:8080/C:/InetPub/ftproot/Opinions/991324.TXT>.

[79]Decision No /98/EC of the European Parliament and of the Council of adopting a Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, December 1998. See further Akdeniz, Y., "The European Union and illegal and harmful content on the Internet," (1998) *Journal of Civil Liberties* 3(1), March, pp. 31-36.

[80]See <http://www.internetwatch.org.uk/hotline/report.html>.

[81]See for example the House of Commons Written Answers (8 Jun 1998), Prime Minister (Child Pornography) in relation to this issue.

[82]Which was published in March 1998.

[83]See the IWF statistics at <http://www.internetwatch.org.uk /about/stats/stats.html>.

[84]'Action taken' counts those reports which IWF has judged to contain potentially illegal material.

[85]COPINE project dealt with the availability of child pornography through the newsgroups. See the Proceedings of the First Copine Conference, January 20-21, 1998, Dublin, Ireland; and Proceedings of the Second Copine Conference, April 1-2, 1999, Brussels. Please note that these reports are not online.

[86]INHOPE - Internet Hotline Providers in Europe is a project under the EC Daphne Programme to encourage co-operation between European Internet Hotline providers to reduce the level of child pornography on the Internet. For details see <http://www.childnet-int.org/hotlines/index.html>.

[87]Per Professor Nadine Strossen, from an ACLU Press Release, "ACLU Joins International Protest Against Global Internet Censorship Plans," 9 September 1999, at <http://www.aclu.org/news/1999 /n090999a.html>.

[88]*Ibid*.

[89]Internet Watch Foundation press release, "New Brief for IWF," 25 January, 2000 at <http://www.internetwatch.org.uk/press /archives/p250100.html>. The new role for IWF, will include "seeking to apply IWF's self-regulation approach to racism on the Internet." See further Akdeniz, Y., "The case for free speech," *The Guardian*, (Online Section), 27 April 2000.

[90]See the Bertelsmann Foundation's Memorandum on Internet Self-Regulation, September 1999, at <http://www.stiftung.bertelsmann.de/internetcontent/english/download/Memorandum.pdf>.
For a critique of the Bertelsmann proposals seethe Cyber Rights & Cyber-Liberties (UK) Memorandum for the Internet Content Summit 1999, 9 September, 1999, at <http://www.cyber-rights.org/reports/summit99.htm>.

[91]*Ibid*.

[92]See further Akdeniz, Y., "Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach," in Edwards, L and Waelde, C eds, *Law and the Internet: Regulating Cyberspace*, Hart Publishing, 1997, pp. 223-241.

[93]Paragraph 10.13 of the Cabinet Office report *e-commerce@its.best.uk.*

[94]See for example the **Gary Glitter** case coverage by the Sun and the Mirror newspapers on 13 November 1999.

[95]Internet Watch Foundation, A Consultation paper: *Rating and Filtering Internet Content - A United Kingdom Perspective*," March 1998, at <http://www.internetwatch.org.uk/rating/rating_r.html>. For a critique of such initiatives see Cyber-Rights & Cyber-Liberties (UK) Report, "Who Watches the Watchmen: Internet Content Rating Systems, and Privatized Censorship," November 1997, <http://www.cyber-rights.org/watchmen.htm> and Cyber-Rights & Cyber-Liberties (UK) Report: "Who Watches the Watchmen: Part II - Accountability & Effective Self-Regulation in the Information Age," September 1998 at <http://www.cyber-rights.org/watchmen-ii.htm>.

[96]See Mrs Barbara Roche, DTI, Internet, Commons Written Answers, 26 June 1997.

[97]Cyber-Rights & Cyber-Liberties (UK) Report, "Who Watches the Watchmen: Internet Content Rating Systems, and Privatized Censorship," November 1997, <http://www.cyber-rights.org/watchmen.htm>.

[98]See "Review of the Internet Watch Foundation: A report for the DTI and Home Office by KPMG and Denton Hall," February 1999, at <http://www.dti.gov.uk/iwfreview>.

[99]Note also the ICRA (Internet Content Rating Association) system which follows from the RSACi system. See http://www.icra.org/ for further information.

[100]See Computer Professionals for Social Responsibility, "Filtering FAQ" <http://quark.cpsr.org/~harryh/faq.html>. Note that most filtering systems based on third-party rating, such as CyberPatrol, are compliant with the PICS labelling system.

[101]See <http://www.netparents.org/software/>.

[102]Department of Trade and Industry, Net Benefit: The Electronic Commerce Agenda for the UK, DTI/Pub 3619, October 1998, at <http://www.dti.gov.uk/CII/netbenefit.html>, p. 13.

[103]Department of Trade and Industry, Net Benefit: The Electronic Commerce Agenda for the UK, DTI/Pub 3619, October 1998, at <http://www.dti.gov.uk/CII/netbenefit.html>. See also the associated press release, Net Benefit: Barbara Roche Sets Out Britain's Electronic Commerce Agenda, P/98/755 6 October 1998.

[104]*Ibid* at p. 13.

[105]Department of Trade and Industry, Secure Electronic Commerce Statement, April 1998, is available at <http://www.dti.gov.uk/CII/ana27p.html>.

[106]See Akdeniz, Y., & Walker, C., "UK Government Policy on Encryption:Trust is the Key?" (1998) *Journal of Civil Liberties* 3(2), pp. 110-116.

[107]Department of Trade and Industry, Net Benefit: The Electronic Commerce Agenda for the UK, DTI/Pub 3619, October 1998, at <http://www.dti.gov.uk/CII/netbenefit.html>.

[108]Adjournment Debate, HMG Strategy for the Internet: Memorandum by the Hon John Battle MP, Minister for Science, Energy and Industry, House of Commons, 18 March 1998, at <http://www.dti.gov.uk/Minspeech/btlspch3.htm>. See for further support to the rating and filtering systems, Mr. Alun Michael, Home Department (Children (Pornography), Commons Written Answers, 2 March 1998; Mr Michael, Home Department, Internet Pornography, Commons Written Answers, 18 February, 1998, Column: 678; Mr Michael, Home Department (Internet), Commons Written Answers, 25 June 1997, Column: 510 [4902]; Lord Clinton-Davis, The Minister of State, Department of Trade and Industry, Written Answers on Internet: Addiction, House of Lords, 1087, 27 March 1998.

[109]Recommendation 10.10 of the e-commerce@its.best.uk report.

[110]Para 10.59 of the above report.

[111]Para 10.60 of the above report.

[112]See the Bertelsmann Foundation's Memorandum on Internet Self-Regulation, September 1999, at <http://www.stiftung.bertels-

mann.de/internetcontent/english/download/Memorandum.pdf>.

[113]Para 10.60 of the e-commerce@its.best.uk report.

[114]See for example the (Irish) Department of Justice, Equality and Law Reform, *Illegal and Harmful Use of the Internet* (Pn.5231, Dublin, 1998). See further Akdeniz, Y., "Global Internet Liberty Campaign Submission on illegal and harmful content," to the Irish Minister for Justice, July 1997 through <http://www.cyber-rights.org/reports>.

[115]The Department of Trade and Industry recently reviewed the IWF through a study by KPMG/Denton Hall and the government is pleased with this self-regulatory scheme. See the Review of the Internet Watch Foundation: A report for the DTI and Home Office by KPMG and Denton Hall, February 1999, at <http://www.dti.gov.uk/CII/iwfreview/>.

[116]The INCORE (Internet Content Rating for Europe) project was set up by a group of European organizations including the UK's Internet Watch Foundation with common interest in industry self-regulation and rating of Internet content. It is now focused on a project that aims to create a generic rating and filtering system suitable for European users. This is being funded by the European Commission in 1999 under the Commission's Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999.

[117]The IWF is also involved with the Internet Content Rating Alliance (ICRA) project with the mission "to develop an internationally acceptable rating system which provides internet users world wide with the choice to limit access to content they consider harmful, especially to children." See the IWF press release, "Consultations on International Internet Self-Rating System launched," 7 October 1998.

[118]See generally EPIC eds, *Filters and Freedom - Free Speech Perspectives on Internet Content Controls*, Washington DC: Electronic Privacy Information Center, 1999, and Akdeniz, Y., & Strossen, N., "Sexually Oriented Expression," in eds Akdeniz, Y., & Walker, C., & Wall, D., *The Internet, Law and Society*, Addison Westley Longman, 2000.

[119]See generally Electronic Privacy Information Center, *Filters and Freedom - Free Speech Perspectives on Internet Content Controls*, (Washington DC: EPIC), September 1999. Please note that partly as a result of the writings contained in this collection, the headlong rush toward the development and acceptance of filtering and rating systems has slowed.

[120]See the Global Internet Liberty Campaign Statement submitted to the Internet Content Summit, Munich, Germany, September 1999.

[121]Interactive environments like chat channels cannot be rated as the exchange and transmission of information takes place live and spontaneously.

[122]Estimated amount of ftp servers on the Internet is about a million. Some of these online libraries may have offensive content or legal content that may be considered harmful for children.

[123]Wired News, "Europe Readies Net Content Ratings," 7 July 1997.

[124]William Powell, *The Anarchist Cookbook*, paperback reissue edition, Barricade Books, (September 1989). In fact, there are many similar books from available through various bookshops and libraries including David Harber, *The Anarchist Arsenal : Improvised Incendiary and Explosives Techniques*, paperback - (October 1990); Rex Feral, *Hit Man: A Technical Manual for Independent Contractors*, paperback - (June 1983); and Maxwell Hutchkinson, *The Poisoner's Handbook*, paperback - (May 1988).

[125]See for example Anarchist's CookBook at <http://www.brandywine.net/users/russell/Hacking/Anarch.zip> or http://www.nextdim.com/users/piranha/members/piranha/acb/index.htm> but note that these are not the same as the above Powell book and are written by Jolly Roger.

[126]See generally Cyber-Rights & Cyber-Liberties (UK) Report, "Who Watches the Watchmen: Internet Content Rating Systems, and Privatised Censorship," November 1997, <http://www.cyber-rights.org/watchmen.htm> and Cyber-Rights & Cyber-Liberties (UK) Report: "Who Watches the Watchmen: Part II - Accountability & Effective Self-Regulation in the Information Age," September 1998 at <http://www.cyber-rights.org/watchmen-ii.htm>.

[127]Electronic Privacy Information Center, "Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet," Washington, December 1997, at <http://www2.epic.org/reports/filter-report.html>.

[128]Gay & Lesbian Alliance Against Defamation report, "Access Denied: The Impact of Internet Filtering Software on the Lesbian and Gay Community," New York, December 1997, at <http://www.glaad.org/glaad/access_denied/index.html>.

[129]See CPSR letter dated 18 December 1996 sent to Solid Oak, the makers of CyberSitter at <http://www.cpsr.org/cpsr/nii/cyber-rights/>.

[130]See the Global Internet Liberty Campaign Statement submitted to the Internet Content Summit, Munich, Germany, September 1999.

[131]See generally <http://www.efa.org.au/Issues/Censor/cens1.html>.

[132]**Reno v ACLU**, 117 S. Ct. 2329 (1997).

[133]The GILC statement on the COPA is at <http://www.cyber-rights.org/gilc/gilc-cda.htm>.

[134]*American Civil Liberties Union, et al. v. Janet Reno*, Civil Action No. 98-5591, United States District Court for the Eastern District of Pennsylvania, 31 F. Supp. 2d 473; 1999 U.S. Dist. Lexis 735; 27 Media L. Rep. 1449; 14 Comm. Reg. (P & F) 1145. See <http://www.epic.org/free_speech/copa/> for details.

[135]*ACLU v. Reno II*, No. 99-1324. For the full decision see <http://pacer.ca3.uscourts.gov:8080/C:/InetPub/ftproot/Opinions/991324.TXT>.

[136]Economic and Social Committee of the European Commission, *Opinion on the Proposal for a Council Decision adopting a Multiannual Community Action Plan on promoting safe use of the Internet*, (OJEC, 98/C 214/08, Brussels-Luxembourg, 10 July 1998) pp. 29-32.

[137]*Ibid* para 4.1.

[138]See *ibid*. See further Walker, C., & Akdeniz, Y., "The governance of the Internet in Europe with special reference to illegal and harmful content," [1998] *Criminal Law Review*, December Special Edition, pp 5-19. See further Akdeniz, Y., "The Regulation of Internet Content in Europe: Governmental Control versus Self-Responsibility," (1999) Swiss Political Science Review 5(2), Summer, pp. 123-131.

[139]Hunt, A., & Wickham, G., *Foucault and Law: Towards a Sociology of Law as Governance*, London: Pluto Press, 1994, at p. 78.

[140]Rhodes, R.A.W., 'The Hollowing Out of the State: The Changing Nature of the Public Services in Britain', (1994) *Political Quarterly* 138 - 151, p. 151.

[141]Akdeniz, Y., "Governance of Pornography and Child Pornography on the Global Internet: A Multi-Layered Approach," in Edwards, L., and Waelde, C., eds., *Law and the Internet: Regulating Cyberspace*, Hart Publishing, 1997, pp. 223-241.

[142]Hirst, P., & Thompson, G., 'Globalization and the Future of the Nation State,' *Economy and Society*, (1995) 24 (3), 408 - 442, p. 430.

[143]Per Tony Blair, foreward to the Cabinet Office Report, e-commerce@its.best.uk, September 1999.

[144]See the Cabinet Office Regulatory Impact Unit's (formerly

known as the Better Regulation Unit) Better Regulation Guide, and the Principles of Good Regulation at <http://www.cabinet-office.gov.uk/regulation/taskforce/2000/PrinciplesLeaflet.pdf>.
Note also the Cyber-Rights & Cyber-Liberties (UK) Response to Better Regulation Task Force Review of E-Commerce, 12 October 2000, at <http://www.cyber-rights.org/reports/brtf.htm>, and the Task Force's report, Regulating Cyberspace: better regulation for E-commerce, 14 December 2000, at <http://www.cabinet-office.gov.uk/regulation/taskforce/ecommerce/default.htm>.

[145]See "Fury as Glitter gets only 4 months," *The Sun*, 13 November 1999;"No tears if he dies in prison," *The Mirror*, 13 November 1999; "Voice of the Mirror act to net perverts like Glitter," *The Mirror*, 13 November 1999.

[146]United Nations, Economic and Social Council, Commission on Human Rights, (Fifty-fourth session), *Racism, Racial Discrimination, Xenophobia and Related Intolerance: Report of the expert seminar on the role of the Internet in the light of the provisions of the International Convention on the Elimination of All Forms of Racial Discrimination*, (Geneva, 10-14 November 1997), E/CN.4/1998/77/Add.2, 6 January 1998.

[147]Note also the European Commission communication paper on Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000)890, Brussels, 26 January, 2001, at <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeCommEN.html>.

[148]Decision No /98/EC of the European Parliament and of the Council of adopting a Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks, December 1998, at <http://www2.echo.lu/legal/en/internet/actplan.html>.

[149]House of Commons Select Committee on Culture, "The Multi-Media Revolution - Volume I," London: HMSO, 21 May 1998, Media and Sport Fourth Report, HC 520-I, at <http://www.parliament.the-stationery-office.co.uk/pa/cm199798/cmselect/cmcumeds/520-vol1/52002.htm>.

[150]*Ibid*, para 108.

[151]See Walker, C., & Akdeniz, Y., "The governance of the Internet in Europe with special reference to illegal and harmful content," [1998] *Criminal Law Review*, December Special Edition, pp. 5-19.

[152]See further Akdeniz, Y., "The case for free speech," *The Guardian*, (Online Section), 27 April 2000.

[153]Universal Declaration of Human Rights, Article 19 (1) states that "[E]veryone has the right to freedom of opinion and expression .includ[ing] [the] freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." See further the Global Internet Liberty Campaign Member Statement on "Human Rights and the Internet," January 1998, at <http://www.gilc.org/news/gilc-ep-statement-0198.html>; and the GILC report, Regardless Of Frontiers: Protecting The Human Right to Freedom of Expression on the Global Internet, Washington DC: CDT, September 1998, at <http://www.gilc.org/speech/report/>.

[154]See the Global Internet Liberty Campaign Statement submitted to the Internet Content Summit, Munich, Germany, September 1999, at <http://www.gilc.org/speech/ratings/gilc-munich.html>.

BOOK REVIEW

E-commerce

E-commerce: A Practical Guide to the Law, by Susan Singleton, 2001, hard-cover, Gower, 144 pp., £45.00, ISBN 0 566 08276 4

As the author notes in her preface:"Electronic commerce has revolutionized the way many carry on business. It has grown from anarchic conditions with a laudable background of freedom of expression to being the principal means of communication between many businesses in the UK, their suppliers, customers, internally with colleagues, and externally with advisers. These 'uses' require the application of laws to ensure a coherent framework for businesses."

The aim of this work is to advise businesses on how to minimize risk and maximize opportunities through E-commerce from a legal perspective. It has sections on employment — E-mail and the Internet; trademarks, copyright and databases — the intellectual property rights; issues related to jurisdiction and advertising on the Web; contracting on the Internet; and a section dealing with problems from insurance and security to contract negotiations and alternative dispute resolution. New legislation, including the Electronic Communications Act and the implementation of the EU Electronic Commerce Directive and Distance Selling Regulations are also featured. The work is up-to-date to 1 February 2001.

Available from Gower Publishing, Direct Sales, Book Point Ltd, 130 Milton Park, Oxford, OX14 4SB, UK; Tel: +44 (0)1235 827730; E-mail: orders@bookpoint.co.uk; Internet: <www.gowerpub.com>.