Chicago-Kent Law Review

Volume 79
Issue 1 *Symposium: Do Children Have the Same First Amendment Rights as Adults?*

Article 7

April 2004

Shielding Children: The European Way

Michael D. Birnhack

Jacob H. Rowbottom

SHIELDING CHILDREN: THE EUROPEAN WAY

MICHAEL D. BIRNHACK* & JACOB H. ROWBOTTOM**

INTRODUCTION

At the time of writing, the dangers posed by the Internet to children are making regular headlines in the United Kingdom and elsewhere in Europe. In *Operation Ore*, British police have been investigating a reported seven thousand credit card subscribers to a single child pornography web site based in the US. With this come reports that suspects include judges, lawyers, teachers, university lecturers, policemen, and a few celebrities. Some have argued that this is creating a moral panic.[1] The controversy has sparked many difficult questions as to how many such users may be based in the UK, and whether there is anything wrong in looking at pictures (as opposed to actual child abuse).[2] In these cases, the issue concerns material viewed by adult Internet users and whether that material is linked to the actual abuse of children by encouraging such pictures to be made and by fuelling the viewers' fantasies that may turn to action. While the harm caused to children using the Internet has not been overlooked, it has again been concerned with a link to actual child abuse, especially through the use of chat rooms. Stories have been reported of adults arranging to meet children after posing as teenagers in chat rooms.[3]

* Lecturer, Faculty of Law, University of Haifa, Israel; J.S.D., New York University School of Law, 2000; LL.M., New York University School of Law, 1998; LL.B., Tel Aviv University, 1996.

** Fellow, King's College, Cambridge University; UK. Barrister; LL.M., New York University School of Law, 2000; B.A., Oxford University, 1996.

We wish to thank Nick Barber and Guy Harpaz for helpful comments, and Avihay Dorfman for able research assistance.

1. *See Calm the Witch-Hunt: Even Child Porn Suspects Have Rights*, GUARDIAN, Jan. 18, 2003, at 21, *available at* http://www.guardian.co.uk/leaders/story/0,3604,877205,00.html.

2. *See* Philip Jenkins, *Cut Child Porn Link to Abusers*, GUARDIAN, Jan. 23, 2003, *available at* http://www.guardian.co.uk/online/story/0,3605,879877,00.html; Matthew Parris, *Child Abuse, or a Crime in the Eye of the Beholder?* TIMES (London), Jan. 18, 2003, at 24; *Networks of Trust: The Internet and the Abuse of Innocence,* Editorial, TIMES (London), Jan. 15, 2003, at 21.

3. *Father Rescues Naked Girl After Net Rendezvous*, TIMES (London), Jan. 28, 2003, at 8.

Less sensational are instances where children access material on the Internet that may not put them at risk of abuse, but that may still be harmful. Such material may include sexual content or scenes of violence, material that poses little threat to adults and which adults should be free to read. This paper investigates the approach taken to the problem of Internet material that is harmful to children in Europe and the UK, and locates the discussion within the emerging constitutional jurisprudence in Europe.[4]

In a nutshell, and inasmuch one can generalize, the current European solution, unlike the mostly unsuccessful legislative attempts in the US, tends to leave the regulation of material that is harmful to children to the market. However, this is not necessarily a civil libertarian heaven. Rather, it is a guided, or directed, legal framework which actively fosters and encourages self-regulation. In this, it is closer to—though not exactly the same as—Amitai Etzioni's suggestion that the legal response should first aim at separating children and adults so to minimize the "spillover" onto the rights of adults, and alternatively, if the first avenue is ineffective, proposing that limitations on adults are justified when the harm to children is substantial.[5]

We begin in Part I by drawing the contours of the issue at stake. We propose an intuitive metaphoric framework to examine the issues at stake by thinking of the producer of the harmful material and the child as two ends of a chain, which we call the "*pornography chain.*" In between there are various other links. We set out several baselines of the discussion. Firstly, we distinguish between material that should be put out of reach of both adults and children, such as child pornography, and that which is harmful to children but not to adults (sometimes referred to as an illegal/harmful distinction).[6] Secondly, we assume that there is such harm, and thirdly, we assume that adults do

4. "European Law" is a rather broad term, as there are several levels of legal systems in Europe; first, each country has its own legal system, second, countries which are members of the Council of Europe are bound by the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR"), and third, there is the European Union in which fifteen states are members at this point. We will discuss the different layers of legal systems in Europe, especially that of the ECHR. The legal response in the United Kingdom will serve as a leading example throughout the discussion.

5. *See* Amitai Etzioni, *On Protecting Children from Speech*, 79 CHI.-KENT L. REV. 3 (2004).

6. We adopt Dr. Etzioni's distinction between "children" (twelve years and under) and "teenagers" (thirteen to eighteen years old), and the generic term "minors," which refers to both groups together. *See id.* at 43.

have a constitutional right to access free content online.[7] We then turn, in Part II, to set out the European constitutional background, wherein free expression is recognized as a human right, and is defined both in a wider and a narrower manner than the American First Amendment, in that it explicitly covers the right to receive information, but it includes built-in limitations.

In Part III, we survey various possible legal responses to the issue. Firstly, a "direct public-ordering approach" in which the State, through a statute, administrative act, or judicial decision, announces what is prohibited and what is permitted. Thus far, European legal systems have not chosen this approach, but nevertheless, we assess the constitutional meaning of such a response. Secondly, an "indirect public-ordering approach," in which the State does not interfere in as blunt of a manner in the digital environment, but is a player in the field; it creates various incentives for the players to act in a publicly desired manner. Thirdly, a "private-ordering approach," where the State refrains from any kind of interference with the digital arena and leaves the playground to self-regulation. The approach opted for in European legal systems seems, at least at this point, a combination of the latter two.

This is evident, for instance, in the topic of filtering software and rating programs (private-ordering), public programs of hotlines for reporting illegal material, encouraging the adoption of codes of conduct (public support for private-ordering), rules that impose liability on Internet Service Providers ("ISP") (indirect public ordering), and education (public involvement). We demonstrate the legislative approaches by analyzing some of these rich regulatory tools. In way of conclusion, we raise a few thoughts as to why it is these approaches that were preferred in Europe.

I. SETTING THE PROBLEM

A. The Interest in Protecting Children and the Pornography Chain

For the purpose of this Article, we do not quarrel with the assumption that pornography does indeed harm children who are ex-

7. In this case, "free" is used both as in "free speech" and as in "free beer." The distinction was made in the context of the free software movement by Richard Stallman. *See* SAM WILLIAMS, FREE AS IN FREEDOM: RICHARD STALLMAN'S CRUSADE FOR FREE SOFTWARE ch.9 (2002), *available at* http://www.faifzilla.org/ch09.html.

posed to it. The evidence discussed in Etzioni's article suffices to establish that there is a public interest in protecting children from pornography, and more so, from violent material.[8] This interest will later be phrased in constitutional terms as "necessary in a democratic society," which is one of the conditions upon which the ECHR allows restricting freedom of speech.[9]

Fulfilling this interest does not come without a cost. The cost is one of limiting the freedom of consenting adults to access these materials. Before considering the direct clash between the public interest and the freedom to access online available material, it is first necessary to identify the *chain of pornography*.[10] There are several links in the chain of pornography, from production to consumption: the producer of the material, the web site operator who offers it, the ISP who provides access to the site or service, the institution through which access is offered, parents, and, finally, the child end-user. Not all links appear in all situations: for instance, when we surf from the privacy of our home, the institutional link drops out of the picture. One strategy to protect the child end-user might be to impose liability on one of the links in the *pornography chain*. Another strategy would be to focus not on *who* can prevent the harm, but on the *content* that passes through the *pornography chain*. We first briefly examine the various links of the chain, and examine whether we can curtail the *pornography chain* there, and whether it is a good solution. We then examine the second strategy.

1. The Producer or Web Site Operator

Regulation at this point tackles the problem at the source of the material and thereby restricts every individual's access to the material regardless of age. But directly imposed limitations on the producer of the material or the web site operator might run into both serious constitutional and technological difficulties. An adult has the right to produce certain content, as long as it in itself does not harm others (as is the case with child pornography) or where there is a constitutionally valid limitation on this right. This issue raises the need to distinguish the illegal from the legal, an issue which we will address shortly. Furthermore, due to the architecture of the Internet, especially its

8. *See* Etzioni, *supra* note 5, at 33–40.

9. In the US, this interest can be phrased as a "compelling state interest."

10. In the discussion to follow, we focus mostly on pornography, but the arguments apply to violent content as well.

borderless character, it might be inefficient to try to block the pornography at its source; end-users will access the same harmful material, now relocated on web sites operated from other countries, where the legal standard is more permissive.

2. The ISP

Perhaps we can aim at the next link in the chain: the ISP could be required to block children from accessing the harmful material. But current technology does not permit an ISP to easily identify child users, and therefore any restrictions on content are likely to apply to adults as much as children. A ten-year-old child who will seek the services of an ISP might be denied access, most likely because of her inability to provide the ISP with assurance that she can pay for the services. But once the service to a home or a public library is established, the ISP cannot effectively know whether it is an adult or a child who uses it at any given minute.

Furthermore, imposing a duty on the ISPs to block the harmful material raises a host of complex questions, as to the effect on the rights of the ISPs themselves (their right to property and contract), the effects of imposing such liability on the development of the Internet in general and of e-commerce in particular, the "chilling effect" on the ISPs and thus the speech-effects on end-users, effects on the costs which are associated with imposing liability, and much more. We will address some of these issues later on in our discussion of the *indirect public-ordering approach.*[11]

3. The Facility

Some institutions have the ability to control access to the physical facility where the computers are located, and we can assume that some of these institutions adopt a clear policy as to who may have access to the location and use of the computers. An Internet café, for example, is more likely to refuse entrance to children, perhaps because children are less likely to be able to pay for the services. In any case, the operator of the small Internet café directly faces the patron. Just like the seller at the newsstand can recognize that it is an eight-year-old who wishes to buy *Playboy*, and hence refuse to sell it to the child, so can the operator of the café refuse access. Other institutions have the power to adopt and implement clear and enforceable rules

11. *See infra*, Part III.C.

as to the access and use of the Internet within their physical boundaries. An elementary school, for example, in which there are computers and access to the Internet, is likely to prohibit access to pornographic web sites. The physical presence of both the operator and the child enables control over access.

The difficulty identified by Etzioni arises in situations where both adults and minors use the same physical location to access the Internet, such as many public libraries. Indeed, much of the legal debate has evolved around libraries.[12]

4. The Parents

The parents have a place in the *pornography chain* by providing access to the Internet in the home, or by providing the parental consent that some public facilities require before granting access. By deciding where and when the child can have access to the Internet, the parent can determine what content the child views. This approach creates the impression that the rights of a child are an adjunct to and subordinate to those of a parent. The ECHR, discussed below, gives little guidance on resolving conflicts between the rights of the child and the parent that may arise in this situation,[13] and views the family as a zone of *laissez-faire,* trusting parents to be able to make the best choices for the child. This may explain the general preference in Europe for parental restrictions on access to the Internet, rather than externally imposed limitations. While both the conservatives and civil libertarians prefer to trust the parental choices, the premise is questionable given that many parents lack the understanding to restrict what children access on the Internet and may not know much about the level of harm that may be caused.[14] Consequently, such an approach must be supported with sufficient resources and support to allow parents to make an informed choice.

12. In the US, see *Kathleen R. v. City of Livermore*, 104 Cal. Rptr. 2d 772, 777 (Ct. App. 2001); *Mainstream Loudoun v. Bd. of Trs. of the Loudoun County Library*, 24 F. Supp. 2d 552 (E.D. Va. 1998); *Am. Library Ass'n v. United States*, 201 F. Supp. 2d 401 (E.D. Pa. 2002), *rev'd*, 123 S. Ct. 2297 (2003); Mark S. Nadel, *The First Amendment's Limitations on the Use of Internet Filtering in Public and School Libraries: What Content Can Librarians Exclude?*, 78 TEX. L. REV. 1117 (2000); and Junichi P. Semitsu, Note, *Burning Cyberbooks in Public Libraries: Internet Filtering Software Vs. The First Amendment*, 52 STAN. L. REV. 509 (2000). In the UK, see *infra*, text accompanying note 147.

13. *See* Jane Fortin, *Rights Brought Home for Children*, 62 MOD. L. REV. 350, 354, 357 (1999).

14. *See* Lilian Edwards, *Pornography and the Internet*, *in* LAW AND THE INTERNET: A FRAMEWORK FOR ELECTRONIC COMMERCE 307 (Lilian Edwards & Charlotte Waelde eds., 2000).

5. Users

Perhaps we should turn to the last link in the chain—the minor consumers. Etzioni suggests that we distinguish between minors of various ages, which he roughly divides into two groups: children and teenagers.[15] This is a much-needed distinction, but the difficulty of distinguishing between these two groups is the same that drives and underlies the entire problem discussed here: the current architecture of the Internet lacks the ability to recognize the user. A famous *New Yorker* cartoon features a dog sitting by a computer, accompanied by the caption, "On the Internet, nobody knows you're a dog."[16] A web site operator cannot know who the end-user is. At most, the operator can recognize the Internet Protocol (IP) address of the user. The IP address can be analyzed, but the information recovered will only indicate the ISP used by the user to connect to the Internet. This might indicate a rough geographical location, but usually not more than that.[17] The ISP, as discussed above, is also limited in its ability to recognize the user. Hence, the way to recognize the end-user depends on the minor user's own cooperation.

But minor users cannot be trusted to identify themselves as minors or as adults. In the absence of strong social condemnation against surfing web sites with "adult content," and as long as democratic societies value the privacy of users, including children, then counting on the subjects of the public interest will not be an efficient solution. A requirement to "click here if you are under 18" is unlikely to deter many minors. Hence, using the law to curtail the *pornography chain* at the minor-user's link is unlikely to succeed. Of course, ultimately, it is all a matter of education, and the question addressed here is whether the law or technology should—or could—replace education or aid it.

6. Technology

There has been an attempt to develop and utilize technological measures to differentiate the end-users, including various age-verification measures, which ask the end-user to prove his or her age by providing a driver's license number, credit card number, and the

15. *See* Etzioni, *supra* note 5, at 43.

16. The author of the cartoon is Peter Steiner. *See* NEW YORKER, July 5, 1993, at 61.

17. Several sites offer an analysis of users' privacy in order to demonstrate the ease with which information can be retrieved. *See, e.g.*, http://privacy.net/.

like, or by using authentication certificates.[18] However, these can be easily bypassed, either technologically or by providing false information, or simply by using an adult's documents. These measures have the further unintended effect of deterring adults from accessing legal web sites and imposing heavy costs on various service providers. In addition, as the U.S. Supreme Court noted, requiring web-site operators to install age verification measures imposes heavy costs on non-commercial speakers.[19]

The intermediate conclusion is that given the practical problems in regulating the various links of the chain described above, the current solutions using technology to differentiate between children and adults are likely to be only partially successful at best. In this context, it is important to note that Etzioni's child-adult separation approach refers to the physical, off-line links in the *pornography chain*, such as the facility, rather than to the on-line links, such as the ISPs.[20] However, the physical, institutional, educational, and technological barriers are not impassable.

A different strategy to prevent harm might be to target the *content* that passes through the *pornography chain*, rather than to target the links thereof. This requires that we are able to define "good" content, or at least "harmful" content. This distinction is crucial for another basic assumption which accompanies the debate, namely, that adults have a right to produce and/or to access pornography or violent material, even if the same material is harmful to children. It also affects the scope of the rights of web site operators.[21]

B. Illegal and Legal Content

Various European institutions have explicitly made the distinction between the legal and the illegal and treated them in two different ways.[22] This brings to mind the American distinction between

18. For a discussion of authentication, see LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 30–36 (1999) (arguing that "the absence of self-authenticating facts in cyberspace reduces its regulability").

19. Reno v. ACLU, 521 U.S. 844, 880 (1997).

20. *See* Etzioni, *supra* note 5, at 29–30. Etzioni proposes that libraries allocate separate computers to children and to adults. This proposal sets out a simple and easy solution for libraries. However, it does not resolve the broader problem of children accessing harmful material in other situations.

21. Later on, we explain how this distinction between adults and children relates to another distinction we make, regarding the various kinds of regulation. *See infra*, Part III.A.

22. *See* European Commission, *Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services*, COM(96)483 final at 6 (recognizing a category

"obscene" and "indecent." While the First Amendment does not cover the former, the latter enjoys constitutional protection.[23] Obviously, the difficulty lies in drawing the line between the two kinds of content—a problem with which American courts struggle.[24] This difficulty in itself has a price—the unclear boundaries of the "illegal" might deter not only illegal speech, but also legitimate content. The laws determining what content is illegal in Europe are drawn up by each Member State, and different countries will draw the balance differently. In this section, we consider the English attempt to define the line between the legal and the illegal, and examine its applicability to the Internet.

It is obvious that it would not be satisfactory to make all material harmful to children illegal. The question of illegality raises the constitutional issue of determining what types of material no one should have access to and that deserve no protection. Powerful reasons exist to make some types of speech illegal, as, for example child pornography has been made under the Protection of Children Act of 1978 in the UK.[25] Other types of material are harmful to some parts of society but not others, thereby deserving of at least some constitutional protection. This may include written words that have some sexual or adult themes, descriptions of violence, or strong language that may be

of material that violates human dignity and that should be banned for everyone regardless of age) [hereinafter Green Paper]; *see also* Council Recommendation 98/560/EC of 24 Sept. 1998 on the Development of the Competitiveness of the European Audiovisual and Information Services Industry by Promoting National Frameworks Aimed at Achieving a Comparable and Effective Level of Protection of Minors and Human Dignity, art. 17, 1998 O.J. (L 270) 48 (noting that the distinction between materials that are offensive to human dignity and those that are harmful to minors is vital, and that the two types of problems require a different approach) [hereinafter Council Recommendation].

23. *See* Chaplinsky v. New Hampshire, 315 U.S. 568, 571–572 (1942). For what it means to be "covered," see FREDERICK SCHAUER, FREE SPEECH: A PHILOSOPHICAL ENQUIRY 89 (1982).

24. The definitive test was set forth in *Miller v. California*, 413 U.S. 15 (1973). It states the basic guidelines:

> (a) whether 'the average person, applying contemporary community standards' would find that the work, taken as a whole, appeals to the prurient interest; (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and (c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Id. at 24 (citations omitted). The digital environment raises some challenges to this test. For example, what is the "community" and according to whose standards is the decision made? The Supreme Court Justices have expressed various opinions in this regard. *See* Ashcroft v. ACLU, 535 U.S. 564 (2002). The Supreme Court remanded the case to the Third Circuit, which once again ruled that COPA is unconstitutional, albeit on different grounds than the previous holding. *See* ACLU v. Ashcroft, 322 F.3d 240 (3rd Cir. 2003), *cert. granted*, 124 S. Ct. 399 (2003).

25. Protection of Children Act, 1978, c.37.

unsuitable for a child. The difficulty with this type of material is determining the balance between the two competing groups.

The difficulties in striking this balance and the application to the Internet are illustrated by the British obscenity laws. In England and Wales, the line between illegal and harmful material is blurred by the way illegal *obscene* speech is defined. Under the obscenity laws, it is a criminal offense to publish an obscene article and to possess an obscene article with the intent to publish it for gain.[26] By focusing on the publisher, the Act tackles the dissemination of such material at the source, although the Act is enforced against those involved in dissemination lower down the chain, such as the seller. Obscene material was first defined in the common law by the courts, in the Victorian case of *Hicklin*,[27] as material that tended to "deprave and corrupt" those into whose hands the publication *may* fall. If the *Hicklin* test were to be applied "as is" to the Internet, it would have a far-reaching effect, as most material has the potential to be accessed by at least a small number of minors, on whom it may have greater corrupting effect.

The common law test has since been replaced by the 1959 and 1964 Obscene Publications Acts that retain the "deprave and corrupt" test, but provide that it is to be applied to persons who are *likely* to read, see, or hear the matter contained or embodied in it.[28] "Persons" has been held to mean both a "significant"[29] and "more than negligible"[30] proportion of those likely to read the material, and the test varies according to the circumstances of each case.[31] The Act therefore does not impose liability if the material will "deprave and corrupt" only a small number of incidental viewers. Nor does the threshold for "deprave and corrupt" assume some standard of purity in most readers. For example, if the readers were already "corrupted" and familiar with pornographic material, it can still be obscene in so far as it feeds an existing habit or makes it worse. Consequently, a different standard applies to material likely to be read by adults, as opposed to teenagers. As Lord Wilberforce stated in *DPP v. Whyte*:

26. *See* Obscene Publications Act, 1959, c.66; Obscene Publications Act, 1964, c.74. The Acts do not prohibit the possession of an obscene article for private use.

27. The Queen v. Hicklin, 3 L.R. 360, 371 (1868). The *Hicklin* test was used by the US courts, but was rejected by the Supreme Court in *Roth v. United States*, 354 U.S. 476, 489 (1957). *See also ACLU*, 535 U.S. at 574–75.

28. Obscene Publications Act of 1959 § 1(1).

29. R. v. Calder & Boyars Ltd., [1969] 1 Q.B. 151 (C.A.).

30. Dir. of Pub. Prosecutions v. Whyte, [1972] A.C. 849, 864–66 (H.L.).

31. R. v. Perrin [2002] EWCA Crim 747, ¶ 30 (C.A.).

> the tendency to deprave and corrupt is not to be estimated in relation to some assumed standard of purity of some reasonable average man. It is the likely reader. And to apply different tests to teenagers, members of men's clubs or men in various occupations or localities would be a matter of common sense.[32]

While this test creates a flexible approach that does not reduce all permissible speech to that suitable for a child, problems in controlling access could lead to greater liability for publications via the Internet. Materials that are legal in other media, such as non-hardcore pornography,[33] may be more easily accessible by children, for example, where no password or fee is required, and would have a corrupting effect on those children.[34] Consequently, a significant proportion of the likely readership of Internet material may be children, giving the Obscene Publications Act a further reach on the Internet than with traditional media.[35]

Whether such a broad application of the Act would arise in relation to the Internet is questionable, given the more liberal approach of English juries in recent decades. Section 3 of the Human Rights Act of 1998 also works against such an interpretation, as legislation has to be interpreted to give effect to the ECHR, including the right to free expression.[36] Furthermore, the police and prosecutors practice tolerance[37] and do not seek to enforce the laws on pornography in traditional formats, such as magazines, that could be accessed by children. Such tolerance prevents the Act from being used as an instrument of moral paternalism in practice, even though that is the

32. *Whyte*, [1972] A.C. at 863.

33. While the Obscene Publications Act is most frequently invoked against materials with sexual content, it can apply to any material thought to deprave and corrupt, such as materials encouraging drug use or depicting violence. *See* R. v. Skirving, [1985] 1 Q.B. 819 (C.A.); *see also* Dir. of Pub. Prosecutions v. A. & B.C. Chewing Gum Ltd., [1968] 1 Q.B. 159.

34. *See Perrin*, [2002] EWCA Crim at ¶11–12. In *Perrin*, the trial jury convicted the defendant of publishing obscene material that was featured in a trailer free of charge to anyone with access to the Internet, but acquitted for materials that required name, address, and credit card details.

35. Even when considering material that only adults can purchase, courts should still consider the likelihood of that material falling into the hands of a child. The British Video Appeals Committee thought videos sold at specialty adult stores would be accessed by children infrequently. *See* R. v. Video Appeals Committee of the British Board of Films Classification, [2000] E.M.L.R. 850, ¶ 24 (Q.B.).

36. The Human Rights Act, 1998, c. 42, has a significant impact on UK constitutional law, and we shall return to it later on.

37. Prosecutors have been reported to have policies regarding which material deserves prosecution. For example, prosecutors will tolerate material with nudity, but draw the line at images of an erect penis. *See* GEOFFREY ROBERTSON, FREEDOM, THE INDIVIDUAL AND THE LAW 190 (6th ed. 1989). Prosecutors may now demonstrate greater tolerance since those reports, given that hardcore pornography can be legally sold at some licensed stores.

rationale behind the wording of the statute, as discussed below. Such an approach has led to criticisms that the Obscene Publications Act is inconsistently applied and does not represent a clear principle.[38] The scope of the Act is further limited by the statutory defense that the article is in the public good on the grounds that it is in the interests of science, literature, art, or learning, or other objects of general concern.[39] This helps address the concern that the Act could restrict information that would be essential for children, for example, information on family planning or safe-sex education.

The focus on the likely reader contrasts with the US test for obscenity, which refers to the average person,[40] and unlike the US test, the Obscene Publications Act makes no reference to the offensiveness of the material.[41] In England and Wales, if the material is so offensive that it would repulse and thereby avert any corrupting influence, it will remain legal. The question as to what material would "deprave and corrupt" is an issue of fact to be decided by the jury and means more than just material that is loathsome or lewd.[42] The application of the standard varies according to the composition, background, and values of the jury, and will be assessed in the light of contemporary standards.[43] The question is not determined by looking at the *content* of the material, but rather on its *effect* on the mind of the reader. Consequently, demonstrating that reading the material will lead to a specific harmful activity is unnecessary.[44] In this, the Act takes a paternalistic approach to the harm; it does not aim to prevent individuals from being confronted with publications that they do not want to see, but stops readers from seeing material that they may well

38. Yaman Akdeniz & Nadine Strossen, *Sexually Oriented Expression*, *in* THE INTERNET, LAW AND SOCIETY 207, 211 (Yaman Akdeniz et al. eds., 2000) (*citing* David Pannick, *Question: When Is Disgusting Not Obscene?*, TIMES (London), Sept. 8, 1998, at 39).

39. Obscene Publications Act of 1959 §§ 4(1), (2). This defense balances the interest of the community in receiving the material against the harm to the individual identified in the first part of the offense. Compare this defense to the third prong of the *Miller* test, applied in the US. *See* Miller v. California, 413 U.S. 15, 24 (1973).

40. *See Miller*, 413 U.S. at 24; ERIC BARENDT, FREEDOM OF SPEECH 264 (1985).

41. *See Miller*, 413 U.S. at 24; BARENDT, *supra* note 40, at 264. However, offensiveness of content is still relevant to common law offenses, such as outraging public decency. *See* R. v. Gibson, [1990] 2 Q.B. 619, 622–24 (C.A.).

42. *See* R. v. Anderson, [1972] 1 Q.B. 304, 305, 311–15 (C.A. 1971).

43. *See* BARENDT, *supra* note 40, at 256–57. Compare this to the first prong of the *Miller* test, applied in the US, where the standard is that of the "average person" in the community. *See Miller*, 413 U.S. at 24.

44. For a discussion of the link between the two, see REPORT OF THE COMMITTEE ON OBSCENITY AND FILM CENSORSHIP [Cmnd. 7772], 61–95 (1979).

enjoy for fear that it undermines their moral state.[45] While the restriction may seem contrary to the principles of a liberal account of free speech that stress individual autonomy and the freedom to choose lifestyle and moral actions,[46] it may seem more suitable for children that are not yet deemed responsible enough to make their own choices as to what materials are suitable to read.[47] However, this comes at a high price if it requires restricting the choices of adults and older minors.

By defining illegal speech by reference to its audience, the Act may encourage publishers to restrict access to potentially corrupting material. However, the Act is distinct from the approach taken by Etzioni, the focus of which is to *restrict* access to the material rather than to *suppress* it.[48] By contrast, the Act is a blunt instrument in that material cannot be published at all if thought to "deprave and corrupt" the likely reader, and thereby cannot be viewed by those potential readers on whom it has little chance of harming at all. However, the types of media used at the time of enactment may have influenced the strategy employed by the Act. Suppression of the source has traditionally been thought to be easier than regulating access. However, when addressing pornography on the Internet, unlike in print media, suppressing the first link in the *pornography chain* is not always easy, to say the least. The source can hide behind anonymous names, use technical means to disguise his or her identity, and can be outside the jurisdiction. Despite these difficulties, the Act has been applied to the Internet, though the practical issues concerning enforcement in this context will be considered below.

The Obscene Publications Act provides a theoretical route for preventing the publication of materials deemed harmful to children by making such publications illegal. However, such a route is unlikely, given the more relaxed approach to the application of the Act in which only publications with an extreme sexual content are targeted for prosecution and likely to secure a jury conviction. Furthermore, the features of the Internet make this type of regulation inappropri-

45. For a criticism of such paternalism in relation to *Hicklin*, and comparable problems in the US law, see 2 JOEL FEINBERG, OFFENSE TO OTHERS 165–89 (1985).

46. *See* John Gardner, *Freedom of Expression*, *in* INDIVIDUAL RIGHTS AND THE LAW IN BRITAIN 209 (Christopher McCrudden & Gerald Chambers eds., 1994).

47. While the problems of an overbroad interpretation have been considered, the Act may offer too little protection for children from material that is thought to be harmful to them, but not enough to "deprave and corrupt."

48. *See* Etzioni, *supra* note 5, at 42–47.

ate. By making the standard dependent on the likely audience, the Act could suppress a wider range of material and thereby spill over into adult rights of expression. Furthermore, it is especially difficult to bring prosecutions that suppress the source of Internet material. Instead, the approach that is promoted by the UK government in limiting the harm caused to children on the Internet is through self-regulation and the promotion of responsible use.

C. *Adults' Rights*

The discussion thus far has assumed that adults have a different stake than children and that material that is likely to harm the latter is unlikely to harm the former. But the argument is stronger than this. It is that adults have a *right* to access this material, and that this right is part of, or derivative of, their freedom of expression. Given the much-debated nature of pornography, this assumption is not trivial and requires some elaboration. The discussion is limited to the material that is not deemed harmful to adults. In regard to such material, and given the notorious effects of pornography, what is the free-speech interest in consuming it?[49] The position described above reflects the civil libertarian view. However, under "European law" this is only the beginning of the constitutional scrutiny. Acknowledging "rights" does not necessarily infer that they are trumps. As we will discuss in the next part, there is room for balancing.

The American discourse regarding freedom of speech stems from the First Amendment, which reads in its relevant part, "Congress shall make no law... abridging the freedom of speech, or of the press."[50] This language seems to cover the rights of speakers, but does not extend to listeners. Indeed, listeners' rights were recognized only in an indirect manner. Courts acknowledged that under one of the theories of free speech—the one introduced by Alexander Meiklejohn half a century ago—protecting free speech is the means to achieve a public goal, which is the self-government of the people.[51] Under this instrumental view of the First Amendment, listeners have an important *interest* in receiving information, but not necessarily a

49. For a feminist critique of pornography, see CATHARINE A. MACKINNON, FEMINISM UNMODIFIED: DISCOURSES ON LIFE AND LAW (1987).

50. U.S. CONST. amend. I.

51. *See* ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT (1948); William J. Brennan, Jr., *The Supreme Court and the Meiklejohn Interpretation of the First Amendment*, 79 HARV. L. REV. 1, 18 (1965).

right.[52] In the liberal rights-talk[53] which dominates American legal discourse, this is an important distinction, for it means that no one has a duty to provide listeners with information.[54] The only limit imposed on the government under this liberal view is that *speakers* should not be limited. Under this rights talk, accessing information produced by another is at most a "negative liberty," *i.e.*, it implies only that the government should not interfere with the activity.[55]

The European response, under ECHR jurisprudence, is easier than the one given in the US. Article 10(1) of the ECHR instructs that

> [e]veryone has the right to freedom of expression. This right shall include freedom to hold opinions *and to receive and impart information* and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.[56]

Under these plain words, adults have the right to receive information. Indeed, the European Court of Human Rights ("the Court") interpreted the term "information" to also include information and ideas that "offend, shock or disturb."[57] The interpretation of the term "information" is informed by the underlying rationale of freedom of expression, as the Court stated:

> Freedom of expression is one of the essential foundations of a democratic society, one of the key requirements for progress and for the development of every individual. Subject to paragraph 2 of Article 10, it applies not only to "information" and "ideas" that are viewed favourably or regarded as inoffensive or immaterial, but also to those that are conflicting, shocking or disturbing: this is the meaning of pluralism, tolerance and the spirit of openness, without which there is no "democratic society."[58]

52. In *Board of Education v. Pico*, 457 U.S. 853, 866–68 (1982), Justice Brennan recognized "the right to receive ideas," basing this conclusion on the Meiklejohnian theory of the First Amendment. For a theoretical discussion, see SCHAUER, *supra* note 23, at 35–56 .

53. The term is borrowed from MARY ANN GLENDON, RIGHTS TALK: THE IMPOVERISHMENT OF POLITICAL DISCOURSE (1991).

54. As Professor Ronald Dworkin explains, the public has an important interest in receiving information, but not a "right." *See* RONALD DWORKIN, A MATTER OF PRINCIPLE 76 (1985).

55. For the meaning of "negative liberty" vis-à-vis positive liberty, see ISAIAH BERLIN, *Two Concepts of Liberty*, *in* FOUR ESSAYS ON LIBERTY 118, 122 (1969).

56. ECHR, Art. 10(1) (emphasis added).

57. *See* Handyside v. United Kingdom, 24 Eur. Ct. H.R. (Ser. A) (1976). See also the opinion of the ECHR Commission, as incorporated in the Court's judgment in *Jersild v. Denmark*, 19 Eur. H.R. Rep. 1, 14 (1995) (in regard to racist speech) (quoted in Fressoz v. France, 31 Eur. H.R. Rep. 2, 56 (1999)).

58. Aksoy v. Turkey, 34 Eur. H.R. Rep. 57, ¶ 51 (2002). *See also* Da Silva v. Portugal, 34 Eur. H.R. Rep. 56, ¶ 30 (2002).

The right to receive information, whether we like the information or not, and as long as it is not illegal, is thus considered to be an inseparable part of freedom of speech.[59] The emerging European jurisprudence of freedom of expression focused mostly on political speech, but the same reasoning applies to the harmful material discussed here: it is offensive to children and many adults, and it might be shocking and disturbing, but for consenting adults it is nevertheless "information."

We are now back to the fundamental conflict: on the one hand we have a valid public interest in protecting children from harmful material, and on the other hand we have an important freedom of consenting adults to access the very same content, a freedom which enjoys a constitutional anchor. Various mechanisms to differentiate adults from minors are either not satisfactory (as in the case of public libraries), or impractical (as in limiting the speakers), or partial (as in using age verification mechanisms), or have negative unintended consequences (as in imposing liability on ISPs). What then should be the legal response in the face of a frontal conflict of this kind? This is the question addressed in the next part.

II. CONSTITUTIONAL PROTECTION OF EXPRESSION UNDER THE EUROPEAN CONVENTION ON HUMAN RIGHTS AND IN THE UK

Before considering actual examples of the attempts to control the various links in the *pornography chain*, it is first necessary to outline the scheme for protecting speech rights. The hurdles that must be overcome to survive such scrutiny will make certain types of control more desirable. In this section, the differences between the US, European, and UK approaches will be examined. The constitutional methodology is important here, for if our starting point is one that does not value free speech as one of the most important human rights, if not the most important one, we might slip down the slippery slope.[60] But even those who believe it to be a fundamental human

59. Thus, in *Jersild*, 19 Eur. H.R. Rep. at 25–26, where the Court interpreted the free speech rights of a journalist, the Court stated that "the public also has a right to receive [information and ideas]. Were it otherwise, the media would be unable to play their vital role of 'public watchdog.'" *See also Fressoz*, 31 Eur. H.R. Rep. at 59.

60. In fact, Dr. Etzioni argues that "free speech can be highly valued even if one ranks it somewhat lower than it has been recently held and that children are now to be more highly regarded." Etzioni, *supra* note 5, at 41. This attitude allows him to trade-off free speech with the interest of protecting children. While we fully accept Etzioni's ultimate conclusion, we disagree with this constitutional methodology. Categorical balancing can take place, but at the same time, we should explain and justify the compromise of free speech rights, which in itself should

right do not argue that it is an absolute imperative.[61] There are countervailing interests (whether just "interests" in liberal rights talk, or "rights"), important in themselves; protecting children from harmful material is one of them.

A. *United States*

The American approach is to examine the clash by way of *categories*: first, is the content at stake covered by the First Amendment?[62] If it is, the next step would inquire what sort of regulation is at stake: is it content-based or content neutral? And if the former, is it viewpoint neutral?[63] "Balancing" is a foreign concept in the official methodology of American constitutional law.[64] The categorical constitutional methodology has the effect of channeling the complex picture of rights, freedoms, and interests into a binary juxtaposition: if there is a First Amendment right at stake, it is almost certain to overcome the opposite interest.[65] Hence, it is surprising that Congress opted first for a rather blunt direct regulation in order to protect children,[66] and later for a narrower regulation,[67] but nevertheless, one of

come with an acknowledgment of the "price" society pays—a moral regret—when compromising speech. This argument requires much elaboration, which we cannot conduct here. For more on the meaning of constitutional tests and the notion of moral regret, see Lawrence G. Sager, *Some Observations About Race, Sex, and Equal Protection*, 59 TUL. L. REV. 928 (1985).

61. In the US, the view that the First Amendment is an absolute has not gained support beyond Justice Black's positions. *See* Hugo L. Black & Edmond Cahn, *Justice Black and First Amendment "Absolutes": A Public Interview*, 37 N.Y.U. L. REV. 549 (1962).

62. *See* Miller v. California, 413 U.S. 15, 25–26 (1973).

63. Compare the majority's opinion in *Turner Broadcasting System, Inc. v. FCC*, 512 U.S. 622, 642–677 (concluding that the must-carry rules imposed on cable television operators are content neutral), with Justice O'Connor's opinion, *id.* at 677 (concluding that the same rules are content-based). *See also* Thomas v. Chi. Park Dist., 534 U.S. 316 (2002) (content neutral scheme for issuing permits for rallies).

64. The term, though, is more complex. *See* T. Alexander Aleinikoff, *Constitutional Law in the Age of Balancing*, 96 YALE L.J. 943 (1987). Not all constitutional systems shy away from balancing, though. *See, e.g.*, Aharon Barak, *A Judge on Judging: The Role of a Supreme Court in a Democracy*, 116 HARV. L. REV. 16, 93–97 (2002) (President of the Israeli Supreme Court outlining the constitutional methodology of balancing).

65. Once the examined regulation is identified as content-based, it takes a compelling state interest to overcome it. One of the rare cases in which this has happened is *Burson v. Freeman*, 504 U.S. 191 (1992) (holding that a statute limiting political canvassing near polling places was constitutional). However, in contemporary terms, this regulation will be considered content-based, but view-point neutral.

66. Communications Decency Act ("CDA"), Pub. L. 104-104, 110 Stat. 133 (1996). The CDA was declared unconstitutional in *Reno v. ACLU*, 521 U.S. 844 (1997).

67. Congress next enacted the Child Online Protection Act ("COPA"), Pub. L. 105-227, 112 Stat. 2681-736 (1998) (codified as amended at 47 U.S.C. § 231 (2000)). COPA was subsequently declared unconstitutional for the purposes of granting a preliminary injunction in *ACLU v. Reno*, 217 F.3d 162 (3d Cir. 2000). The Supreme Court reversed and remanded in

direct public-ordering. It is less of a surprise that, thus far, this direct public-ordering approach has failed in the courts and the First Amendment has prevailed.

B. Europe

The emerging constitutional and Human Rights jurisprudence in Europe does not shy away from explicit balancing.[68] In fact, balancing is a concept embedded in Article 10 of the ECHR itself. Contracting States to the ECHR enjoy a margin of appreciation in striking the balance,[69] but the article spells out the guidelines for doing so, though the Court repeatedly held that this does not exclude European supervision.[70] After outlining the contours of the right,[71] Article 10(2) states:

> The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are *prescribed by law* and *are necessary in a democratic society*, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or *morals*, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.[72]

This structure of the limitation allows overriding freedom of expression if, and only if, several conditions are met, and these exceptions should be interpreted narrowly, as follows:[73]

Ashcroft v. ACLU, 535 U.S. 564 (2002). The Third Circuit again held that COPA was unconstitutional, albeit on different grounds, for purposes of granting a preliminary injunction, 322 F.3d 240 (2003), and the Supreme Court has recently granted certiorari to hear the case again. 124 S. Ct. 399 (2003).

68. For an overview of European constitutionalism, see J.H.H. WEILER, THE CONSTITUTION OF EUROPE: "DO THE NEW CLOTHES HAVE AN EMPEROR?" AND OTHER ESSAYS ON EUROPEAN INTEGRATION (1999).

69. The margin might change according to the kind of speech being regulated and the goal the restrictions aims at. Thus, for instance, when political speech is at stake, the margin is rather narrow, whereas in the "sphere of morals," such as blasphemy, member states enjoy a wider margin of appreciation. *See, e.g.*, Wingrove v. United Kingdom, 24 Eur. H.R. Rep. 1, 30 (1997). For elaboration on the concept of "margin of appreciation," see *Handyside v. United Kingdom*, 1 Eur. H.R. Rep. 737, 754 (1976). For application in the context of Article 10(2), see *Bowman v. United Kingdom*, 26 Eur. H.R. Rep. 1 (1998).

70. *See, e.g.*, *Wingrove*, 24 Eur. H.R. Rep. at 3.

71. ECHR, Art. 10(1).

72. ECHR, Art. 10(2) (emphasis added).

73. For the judicial instruction to interpret the exceptions narrowly, see *Da Silva v. Portugal*, 34 Eur. H.R. Rep. 56, ¶¶ 30, 33 (2000).

Restriction of Speech: First, there is a dual preliminary condition: that the regulated act is considered "expression," and that the regulation restricts it.[74] It does not matter whether the restriction is direct or indirect. In a leading case on this issue, the European Court found that an English statute that limited the expenditures of people who were not standing for election, in connection with the elections, was to be considered a "restriction."[75] In another case, the Court found that a sanction imposed after a defamatory publication took place "hampers" the press.[76] Closer to the subject discussed here, the European Commission[77] found that the screening of a gay porn movie in a back room of a sex shop was within the realm of freedom of expression.[78]

"Prescribed by Law": Secondly, Article 10(2) sets a formal condition: that the limitation of the right should be "prescribed by law."[79] This term was interpreted to include not only statutes and constitutions,[80] but also unwritten law like the English Common Law.[81] In any case, the law should be formulated with sufficient clarity to enable foreseeability.[82] Thus, when interpreting the Swiss Criminal Code's prohibition of making or possessing *obscene* material—a term which is not defined in the Swiss Code—the Court pointed to several consistent decisions by Swiss courts and found them to supplement the let-

74. This is parallel to the US requirements which trigger the First Amendment—that the speech is "covered" by the First Amendment and that the regulation abridges the First Amendment right.

75. *See Bowman*, 26 Eur. H.R. Rep. at 9–10. For a discussion of the impact of free expression rights on political funding in the United Kingdom, see Jacob Rowbottom, *Political Donations and the Democratic Process: Rationales for Reform*, 2002 Pub. L. 758, 771.

76. *See* Lingens v. Austria, 8 Eur. H.R. Rep. 407, 420 (1986).

77. The ECHR initially provided a procedure for individuals to complain of breaches by the states that are a party to it. The European Commission on Human Rights received and investigated initial complaints of a breach of the Convention. If the dispute was not settled, a report was provided to the state involved and the Committee of Ministers. The state concerned or the Commission could then bring the complaint before the European Court of Human Rights. The Commission has since been abolished and a full time court established. *See* A.W. BRADLEY & K.D. EWING, CONSTITUTIONAL AND ADMINISTRATIVE LAW 417–418 (11th ed. 1993).

78. *See* Scherer v. Switzerland, 18 Eur. H.R. Rep. 276, 284–285 (1994). The Commission subsequently concluded that the applicant's conviction for showing the film violated Article 10 of the Convention. However, the applicant died before the Court reached a decision and the Court thus struck the case out of its list.

79. See *Ek v. Turkey*, 35 Eur. H.R. Rep. 41 (2002), in which the Court found that the law according to which the applicant was convicted was no longer in force, and hence was a breach of Article 10(2).

80. *See e.g.*, Refah Partisi (Welfare Party) v. Turkey, 35 Eur. H.R. Rep. 3, 67 (2002).

81. *See* Wingrove v. United Kingdom, 24 Eur. H.R. Rep. 1, 26–27 (1996) (finding that the English Common Law of blasphemy is "law" within the meaning of Article 10(2)).

82. *See id.* at 26.

ter of the Code, and thus to meet the condition of "prescribed by law."[83] As for administrative decisions, the Court ruled that as long as the discretion is conferred by law, and the scope of the discretion and manner of exercise are clear, the condition is satisfied.[84]

Legitimate Aim: The restriction on expression must fulfill a "legitimate aim." This requirement, though not explicit in the ECHR, refers to the list of enumerated causes which allow the restriction of freedom of expression.[85] The list includes "morals," a term which was applied in several obscenity cases, where the Court found that, given the margin of appreciation accorded to Member States, regulation which targets pornography aims at protecting the (public) morals, and thus satisfies this condition.[86]

Proportionality: The European judiciary added one more important condition not found in the text of Article 10(2), that of proportionality:[87] the restriction on freedom of expression should be proportionate to the legitimate aim pursued.[88] The principle of proportionality is the heart of the balancing of freedom of expression with the opposing interests. It was developed and elaborated by European courts[89] to include several prongs. *Firstly*, a connection be-

83. *See* Müller v. Switzerland, 13 Eur. H.R. Rep. 212, 226 (1988).

84. *Wingrove*, 24 Eur. H.R. Rep. at 26–28 (discussing the authority of the British Board of Film Classification, which derives from the Video Recordings Act 1984).

85. *See* Bowman v. United Kingdom, 26 Eur. H.R. Rep. 1, 10 (1998); Aksoy v. Turkey, 34 Eur. H.R. Rep. 57, ¶47 (2000).

86. *See, e.g.*, *Müller*, 13 Eur. H.R. Rep. at 230; Scherer v. Switzerland, 18 Eur. H.R. Rep. 276, 285–87 (1994) (Commission's position).

87. See, *e.g.*, *Bowman*, 26 Eur. H.R. Rep. at 13. For discussion of the principle of proportionality in the UK, see Richard Clayton, *Regaining A Sense of Proportion: The Human Rights Act and the Proportionality Principle*, 2001 EUR. HUM. RTS. L. REV. 504.

88. *Bowman*, 26 Eur. H.R. Rep. at 13. The principle of proportionality has also been applied in regard to other rights which are enumerated in the ECHR. For further discussion, see Michael Supperstone & Jason Coppel, *Judicial Review After the Human Rights Act*, 1999 EUR. HUM. RTS. L. REV. 301, 312–13. For a thorough discussion of the principle of proportionality in the European Community ("EC"), see TAKIS TRIDIMAS, THE GENERAL PRINCIPLES OF EC LAW 89–94 (1999).

89. The principle was especially developed by the European Court of Justice (of the EC) and the European Court of Human Rights (of the Council of Europe). For discussion of the relationship between EC law and the ECHR, see TRIDIMAS, *supra* note 88, at 236–43 (explaining that the EC is not formally bound by the ECHR, though the Treaty on the European Union refers to the ECHR and commits the EU to respect basic rights, and concluding that the "two jurisdictions are in a relationship of co-operation and not one of confrontation"). Indeed, the Treaty reads, in Article 6(2) (formerly article F(2)): "The Union shall respect fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms signed in Rome on 4 November 1950 and as they result from the constitutional traditions common to the Member States, as general principles of Community Law." In the preamble of its 2000 Charter of Fundamental Rights of the European Union, the EU reaffirmed its commitment to the ECHR. Article 11(1) of the Charter reads: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive

tween the restriction and the legitimate aim should be shown. This prong requires more of a general observation: Are the means suitable to the aim?[90] *Secondly*, a direct connection and proportion between the goal and the means is required: Are the means applied to achieve the interest necessary to the restriction of freedom of expression? This is the "necessity" prong, and the question asked is often: Are there alternative, less restrictive means that could be applied to achieve the same goal? *Thirdly*, though this is sometimes a neglected prong, the question to be asked is: Has the measure chosen had an excessive effect?[91]

Proportionality requires examining the facts of the legislation at stake.[92] Any law that will attempt to protect children in a manner that will restrict the freedom of expression of adults would have to pass this barrier. It is our opinion that any restriction that limits adults' opportunities to those that are permissible for children fails at least the second prong: there should be less restrictive means applied. We will return to this point later on.

C. *United Kingdom*

The protection of expression has not traditionally played as fundamental role in the UK Constitution as the First Amendment has in the US. Traditionally, under the principle of Parliamentary sovereignty, the legislature is free to pass whatever laws it likes regardless of whether it violates fundamental rights. In this sense, rights to speech are merely residual, as people are free to say whatever they want in so far as it is not otherwise restricted. This did not mean that rights were ignored under the traditional approach, but rather that

and impart information and ideas without interference by public authority and regardless of frontiers." Article 52(3) of the Charter instructs that the meaning and scope of the rights recognized in the Charter are the same as in the ECHR. *See also* COUNCIL OF THE EUROPEAN UNION, CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION: EXPLANATIONS RELATING TO THE COMPLETE TEXT OF THE CHARTER (2000).

90. *See* Supperstone & Coppel, *supra* note 88, at 313.

91. See TRIDIMAS, *supra* note 88, at 91–93, for a discussion of the three-part test. An ancillary test looks at the reasons given by the state (or its relevant authority) for the measure it chose to apply, and queries whether they are "relevant and sufficient." *See, e.g.*, Worm v. Austria, 25 Eur. H.R. Rep. 454, 455–456 (1997); Tidende v. Norway, 31 Eur. H.R. Rep. 16, 434 (2000). Various scholars present these three prongs in slightly different terms. *See, e.g.*, Supperstone & Coppel, *supra* note 88, at 313–14 (defining the three prongs as "suitability," "necessity," and "balance").

92. For example, see the factual analysis in *Jersild v. Denmark*, 19 Eur. H.R. Rep. 1, ¶¶ 33–45 (1994). Many cases in various contexts were decided on this point. *See, e.g.*, Lingens v. Austria, 8 Eur. H.R. Rep. 407 (1986); *Tidende*, 31 Eur. H.R. Rep. 16; Aksoy v. Turkey, 34 Eur. H.R. Rep. 57 (2000); Da Silva v. Portugal, 34 Eur. H.R. Rep. 56 (2000).

they were protected by individual members of Parliament committed to a culture of liberty who were democratically accountable. By the early 1980s, when the political consensus broke down and the Thatcher government was able to dominate the House of Commons, greater concern arose that individual rights were too easily bypassed. By this time, the ECHR had given the legal protection of rights, such as expression, a more prominent role in the UK. In 1991, the House of Lords recognized that ambiguous legislation should be construed to be in conformity with the ECHR.[93] However, the Lords noted that the ECHR was not incorporated into UK law and held that there was no presumption that a statutory discretion should be exercised in conformity with the ECHR.[94] Consequently, while rights gained some recognition, UK law was still nowhere near the rights talk of the US. During this time, a similar channel of protection found favor in the courts, in which rights were not embodied in a constitutional provision, but rather were found in the principles of the Common Law. This meant that it was open to the legislature to restrict rights, but an interpretive presumption existed that they would not intend to do so. Consequently, restrictions imposed on prisoners' rights to free speech could not be imposed using powers granted under an ambiguous or generally worded statute.[95] This seemed to go beyond the approach in *Brind*, and required a presumption that discretionary powers would be exercised in conformity with basic rights, to be displaced only through express words or by necessary implication of an Act of Parliament.

A more active approach from the courts emerged as greater concern arose in relation to the orthodox constitutional theory. The huge majorities of the Thatcher and Blair governments meant Parliament gave little chance for political channels to protect these rights, creating a dissatisfaction that led to calls for the ECHR to be incorporated into domestic legislation. These calls were met in 1998 when the Human Rights Act ("HRA") was passed by the UK Parliament and came into effect in October 2000. The operation of the Act is devel-

93. Brind v. Sec'y of State for the Home Dept., [1991] 1 A.C. 696, 703 (1990).

94. *Id.* at 708–09. In *Brind*, the House of Lords upheld an executive order banning the broadcast of statements of certain organizations using the actual voice of the speaker. As no ambiguity or uncertainty existed in the statutory provision granting the Secretary of State's power to issue the ban, the discretion conferred by that provision did not have to be exercised in accordance with the ECHR.

95. *See* R. v. Sec'y of State for the Home Dept., ex. parte. Simms, [1999] E.M.L.R. 689 (H.L.).

oping fast, and space precludes a detailed discussion.[96] By incorporating the ECHR, the scheme for protecting rights is similar to that of the Strasbourg court outlined above.[97] The Act does not adopt an absolutist approach to speech rights, and the limitations in Article 10(2) are generic, leaving it for the courts to determine the scope and extent of protection.[98]

The HRA is designed to leave the last word on the meaning of rights with Parliament. The courts cannot strike down legislation as invalid, but under Section 4, they can make a declaration of incompatibility. The Act envisages a political pressure on the government to change the terms of legislation in the event of a declaration, or at least to justify the restriction. However, Section 3 places a significant obligation on the courts to read legislation as compatible, even if this means departing from the literal meaning of the text. The House of Lords' decision in *Regina v. A* demonstrates the importance of this power, arguably giving the court a role in re-writing legislation to make it compatible with the ECHR.[99] Such a power may be equal to, or even greater than, the power to strike down legislation.[100]

Under Section 6 of the HRA, it is unlawful for a public authority to act in a way incompatible with an ECHR right, unless required by an act of Parliament. The term "public authority" clearly includes local authorities responsible for public libraries and schools that provide Internet access.[101] If incompatibility is found in the public authority's act, the court can award whatever remedy it thinks is necessary, as opposed to the declaration in the case of primary legislation.[102] The influence of local level public authority in drawing the balance be-

96. For an overview, see K.D. Ewing, *The Human Rights Act and Parliamentary Democracy*, 62 Mod. L. Rev. 79 (1999). For a discussion on some of the major decisions in the first two years of the Act, see Francesca Klug & Claire O'Brien, *The First Two Years of the Human Rights Act*, 2002 Pub. L 649; Keir Starmer, *Two Years of the Human Rights Act*, 2003 EUR. HUM. RTS. L. REV. 14.

97. *See, e.g.*, O'Shea v. MGN, [2001] E.M.L.R. 943 (holding that a pornographic advertisement was protected expression).

98. In contrast to other rights that do not have such a provision.

99. R. v. A. *(No. 2)*, [2001] 1 A.C. 45, 67–68.

100. Of course, striking down legislation is a powerful tool, but it is a binary decision. Re-writing legislation, on the other hand, is a creative task that goes beyond judicial review, in that it is not just stating what the legislature can do, but de facto, replacing it.

101. *See* Poplar Housing & Regeneration Cmty. Assoc. Ltd. v. Donoghue, [2002] Q.B. 48, 66 (C.A. 2001) (providing that "public authority" includes persons, even private persons, performing functions of a public nature); Heather v. Leonard Cheshire Foundation, [2002] H.R.L.R. 30, 838 (C.A.).

102. Human Rights Act, 1998, c. 42, § 8 (providing that "in relation to any act (or proposed act) of a public authority which the court finds is (or would be) unlawful, it may grant such relief or remedy, or make such order, within its powers as it considers just and appropriate.").

tween the right and the competing aim depends on the level of deference the courts accord to the primary decision maker when applying the proportionality standard. While accepting proportionality as more intense than the traditional standard of review,[103] the appropriate level of deference to be shown to the primary decision maker is still debated. A more stringent and less deferential approach will be granted depending on the nature of the speech in question. For example, political speech is granted a higher level of protection than most other types of expression.[104] By contrast, sexually oriented speech would receive a much weaker standard of protection, thereby rendering the state controls discussed in this paper more likely to survive scrutiny. A further question of deference depends on the nature of the primary decision maker. At the European level, the European Court of Human Rights applies the doctrine of margin of appreciation, in which the court shows deference to the different cultures that might result in different balances in signatory states.[105] While there is no reason this should apply in the UK, a similar doctrine of deference may apply to show respect to the competence or democratic legitimacy of other institutions.[106] The approach taken by the courts to this question will determine whether the restriction of expression on the Internet is compatible with the Act. However, under the approach developing under the HRA, and following the Strasbourg jurisprudence, attempts to prevent harmful material from

103. R. v. Sec'y of State for the Home Dept., ex parte Daly, [2001] 2 A.C. 532, 547. For a discussion of the standard of review before and after the Human Rights Act, see Mark Elliott, *Scrutiny of Executive Decisions Under the Human Rights Act 1998: Exactly How "Anxious"?*, 2001 J.R. 166; Clayton, *supra* note 87, at 507.

104. R. (ProLife Alliance) v. British Broad. Corp., [2002] E.M.L.R. 41, 921–22; *see also* N.W. Barber, Note, *A Question of Taste*, 118 L.Q. REV. 530, 531 (2002).

105. Handyside v. United Kingdom, 1 Eur. H.R. Rep. 737, 754 (1976).

106. The deference can arise at different stages of the review, such as the consideration of whether the subject matter precludes judicial intervention, and the determination as to whether the limitation is unlawful. For a discussion of deference, see *R. v. Dir. of Pub. Prosecutions, ex parte Kebilene*, [2000] 2 A.C. 326, 380–81; *R. (Alconbury Developments Ltd) v. Secretary of State for Transport the Environment and the Regions*, [2003] 2 A.C. 295, 320–22 (2001); *Brown v. Stott*, [2003] 1 A.C. 681, 694–95, 703 (P.C. 2000); *R. v. Lambert*, [2002] 2 A.C. 545, 623 (2001); and *R. v. Sec'y of State for the Home Dept.*, [2001] 2 AC 532, 535–36. For a discussion of the case law, see Paul Craig, *The Courts, The Human Rights Act and Judicial Review*, 117 L.Q. REV. 589 (2001); Richard A. Edwards, *Judicial Deference Under the Human Rights Act*, 65 MOD. L. REV. 859 (2002); Ian Leigh, *Taking Rights Proportionately: Judicial Review, the Human Rights Act and Strasbourg*, 2002 PUB. L 265; Nicholas Blake, *Importing Proportionality: Clarification or Confusion*, 2002 EUR. HUM. RTS. L. REV 19. The approach has been criticized for lacking a coherent principle and that the courts have acted pragmatically. For example, Richard Edwards argues that the courts should not shy away from morally complex decisions as the purpose of the Human Rights Act is to create a culture of justification from the decision making bodies and that deference should not simply grant a license to the legislatures. *See* Edwards, *supra*, at 878.

being accessed on the Internet by children are less likely to fall foul of the courts than in the US, even if they entail some degree of overspill into the protected speech of adults. The way in which the courts approach this issue will be examined in the next section.

III. LEGAL RESPONSES AND THEIR CONSTITUTIONAL MEANING

A. The Various Kinds of Regulation

Regulation of expression is a tricky task. Almost any interference in the "marketplace of ideas" has a negative effect on the free expression rights of some participants in the market. Hence, direct regulation, which interrupts "normal" market behavior and rules out some of the activities going on within it, needs to pass a rather high threshold. But there are other narrowly tailored, less intrusive ways to achieve more of the public interest while causing less harm on the free speech side. For example, opting for a shift in the regulatory mode—from a *direct public-ordering approach* to an *indirect public-ordering approach*—is one such way. Instead of the government explicitly declaring which activities are allowed and which are prohibited, the government creates a mechanism that provides the players within the market with incentives to reevaluate their behavior, and adapt it toward the public interest. They are not obliged to comply, but are encouraged to do so.

Yet another way is even less intrusive, and it is one which leaves the market (or field, for those who prefer a less capitalistic metaphor) entirely in the hands of the players: if they wish, they can undertake self-regulation. The motivation to do so might be the players' own sense of responsibility, or their commercial fear of the market's reaction, or the political fear that if they stay idle, government will eventually interfere. This is an approach of *private-ordering*.

The legal experience thus far in the area of protecting children has provided us with examples of all three possible avenues and various combinations thereof. The US first attempted a direct public-ordering approach and, later, an indirect one, whereas the European way tended from the very start towards a *private-ordering approach*. The kinds of regulation described above will generally focus on different stages of the *pornography chain*.[107] Direct controls on content,

107. *See supra* Part I.A.

in aiming to suppress the dissemination of material, will be most effective against the producer/speaker (the first link of the *pornography chain*). Indirect public-ordering and private-ordering are similar in that they attempt to create self-regulatory, flexible, or individualized controls, and will often be targeted at the later links of the chain, such as the ISP, facility, or user. These later stages allow for greater variation in regulation according to the potential recipient, whereas targeting the producer of material will result in a uniform restriction of the material.

At first sight, then, the different regulatory strategies might seem to parallel the links in the chain of pornography; direct public-ordering aims at the producer of the material, whereas indirect public-ordering and private-ordering aim at other links in the chain. However, the parallel between strategy and link is not inevitable. For example, restraints on content may be applied against not only the producer, but also the individual user or library to prevent the downloading of unlawful material. The discussion below will illustrate that the parallel is kept in place by problems of enforcing such restraints at the lower levels.[108]

B. Direct Public-Ordering

Direct public-ordering poses the greatest difficulty in terms of free expression, in that it is a state intervention that rules out certain types of activities. The approach taken may be to prohibit certain activities or types of speech, thereby rendering speech that was previously thought of as harmful to be unlawful. The methods and problems of this type of control have been discussed in relation to the illegal/harmful distinction above. For such reasons, direct public-ordering is the bluntest method and has the greatest incidental impact. An example of this would arise if a country within Europe attempted to pass its own version of the American Communications Decency Act ("CDA") or the Child Online Protection Act ("COPA"). The question therefore arises as to whether this legislation would survive the ECHR or domestic protection of rights. It seems that the production of the material would be considered "expression," and that such a measure restricts it. In order to survive, the "Europeanized CDA" would have to be prescribed in a law, or at

108. Enforcing content restraints on individual users, while possible, would require extensive policing in order to suppress the material. It is likely to be found only in combination with attempts to retrain the higher levels of the *pornography chain*.

least an anchor in a law, that outlines the contours of discretion of an administrative body, and it would have to address the definitions of the prescribed material in as clear of a manner as possible. Such legislation would be likely to be considered as furthering a legitimate aim, and "necessary in a democratic society." The focus would be on the proportionality of such a measure, and especially, we anticipate the question to be whether there are less restrictive means to achieve the legitimate goal without impacting the freedoms of adults. Etzioni's proposal to adopt an adult-child separation approach, *i.e.*, allocating separate computers to children and adults in public libraries, perfectly fits this test. This would be a completely different way of looking at things, compared to the US; the legislation is not thought of in terms of one legal regime (*i.e.*, the First Amendment), but rather as a *balance* between the competing social interests of protecting free speech *and* protecting children. At the end of the day, the details of each legislation will determine its fate.

Direct measures that proscribe expression harmful to children have already reached the European Court, for example in *Handyside*, a pre-Internet case. In that case, the publishers of *The Little Red Schoolbook* claimed that their expression rights were infringed by the seizure of books and prosecution under the UK Obscene Publications Acts. The book contained a twenty-six-page section on sex, including such topics as masturbation, pornography, venereal disease, and abortion—subjects that would not be thought of as harmful to an adult reader. Although the book was distributed through ordinary channels, it was aimed at school children age twelve and older. The European Court held the protection of morals and of young people to be a legitimate aim under Article 10(2).[109]

The Court placed importance on the fact that the book was aimed at young persons and had a factual style that would be easily understandable, even by readers younger than the targeted group, and that the book was to be distributed widely.[110] The Court stated that this case was not analogous to pornographic publications, sex shops, and adult entertainers that might be exposed to young people in some circumstances, because the *Little Red Book* was aimed at and easily accessible to young people.[111] Consequently, on the necessity of the measures, the Court in *Handyside* rejected the argument that a

109. *Handyside*, 1 Eur. H.R. Rep. at 753, 755.
110. *Id.* at 755.
111. *Id.* at 758.

restriction on the sale of the book (for example, to adults only) would suffice,[112] as there was no sense in restricting to adults the sale of a work destined for the young.[113]

As noted in earlier sections, similar considerations apply to the Internet where minors can easily access material aimed at adults, especially if a password or a fee is not required. Such an approach has been followed in relation to the Internet in *Perrin*, where the UK Court of Appeal rejected the argument that self-regulation or blocking software was the only proportionate way to pursue the aim of protecting children.[114] The restriction of content at the source may be suitable where the material is aimed at or easily accessed by minors. However, where the harmful material is produced with adults as the intended consumers and is not targeted to minors, a direct restriction that limits adult access is more likely to fall foul of the ECHR. The possibility of restricting access to such sites may be thought sufficient to protect children when the material is aimed at adults and access by minors is incidental.

It is interesting to note that the approach in *Handyside* balanced the adult's right to produce and impart expression with the interest in protecting the child's welfare. Even though children contributed to *The Little Red Book*, the rights of children to produce and receive information were not considered.[115] An approach based on the child's right to produce would have similarities with Etzioni's distinction between the First Amendment rights of children and teenagers, although it remains unclear whether such a framework would have made a difference to the outcome of the case.[116] *Handyside* demonstrates that in some circumstances, the ECHR permits direct re-

112. *Id.*

113. *Id.* at 759.

114. R. v. Perrin, [2002] EWCA Crim. 747 (C.A.). In *Perrin*, the Court noted that impact on freedom of expression was limited, as the prosecution had only been successful in relation to a trailer that did not require a password or credit card details. The jury did not convict on material that was accessible only through membership. *See id.* at ¶ 50.

115. Fortin, *supra* note 13, at 353.

116. Geraldine Van Bueren argues that if the action was framed in terms of an older child's right to receive information, the Court may have considered the total prohibition of the book as disproportionate to the aim, thereby focusing more on proportionality than margin of appreciation. GERALDINE VAN BUEREN, THE INTERNATIONAL LAW ON THE RIGHTS OF THE CHILD 135 (1995). Ursula Kilkelly notes that the Commission on Human Rights dismissed a complaint brought by a mother and her thirteen- and seventeen-year-old children, alleging that the ban infringed their right to receive information. However, the application failed as a second, modified, edition of the book was freely available. URSULA KILKELLY, THE CHILD AND THE EUROPEAN CONVENTION ON HUMAN RIGHTS 131 (1999).

straints on adults' expression rights in relation to materials that would not harm adults in order to protect children.

This jurisprudence appears to leave open the option of suppressing material on the Internet in some circumstances to protect the welfare of children without falling foul of the ECHR. Given this, it may come as a surprise that the principal means of combating harmful material in Europe has not been through direct restrictions on permissible content. One reason may be that European countries have benefited from the American experience of the CDA and do not want to be vulnerable to such challenges. Another factor is the sheer difficulty in enforcing such laws.

Several problems have already emerged when attempting to enforce the Obscene Publications Act in the UK in relation to the Internet. Initial uncertainty over the applicability of the law to the Internet was resolved in 1994, when the Act was amended to include data stored on a computer disc as an "article,"[117] and covered the transmission of data as publication. However, even if the Act does apply to the Internet, the problem remains in deciding *whom* to prosecute. The global nature of the Internet means obscene material can be downloaded from sites outside the UK. The legal response has been to take a broad interpretation of the Act and define "publication" as occurring when the information is downloaded in the UK, as the electronic data stored overseas is transmitted into the UK.[118] As a

117. Criminal Justice and Public Order Act, 1994, c.33, Sched 9 ¶ 3. For a discussion of these issues, see Colin Manchester, *Computer Pornography*, 1995 CRIM. L. REV. 546, 548–52. The Act has been applied to activity on the Internet on a few occasions, mainly in relation to hardcore pornography that is corrupting to adults. *See* Akdeniz & Strossen, *supra* note 38, at 210 (referring to *R. v. Jack (Colin Mason)*, Norwich C.C., 4 July 1994).

118. In *R. v. Waddon*, [2000] All E.R. 502, a businessman was prosecuted even though the websites concerned were based in the US. The materials were, however, prepared and uploaded to the website in the UK. The Court of Appeal suggested that publication can occur when images are downloaded from a foreign website. Rose, L.J., stated,

> As it seems to us, there can be publication on a Web site abroad, when images are there uploaded; and there can be further publication when those images are downloaded elsewhere. That approach is, as it seems to us, underlined by the provisions of s.1(3)(b) as to what is capable of giving rise to publication where matter has been electronically transmitted.

Id. at ¶ 12. That approach was confirmed by the Court of Appeal in *Perrin*, [2002] E.W.C.A. Crim 747, in which a man was prosecuted for publishing an obscene article when the material was prepared and uploaded abroad into a foreign website. The Court rejected a parallel with *ACLU v. Reno*, 521 U.S. 844 (1997), given the difference in constitutional protection and relations between the states, and decided there was no need to show that major steps in relation to publication were taken within the jurisdiction of the court. The Court of Appeal held that the images were published in England when downloaded by the police in the UK. For a criticism of the decision in *Perrin*, see Michael Hirst, *Cyberobscenity and the Ambit of English Criminal Law*, 13 COMP. & L. 25, 28 (2002).

consequence, producers of obscene content based overseas can be liable in the UK for publishing materials that are downloaded in the UK. This does not, however, resolve the problem of enforcing this provision where the publisher remains based overseas. Consequently, strategies seeking the cooperation of those at every stage in the chain have more chance of being effective and practically implemented, even if direct ordering may be constitutionally permitted.

C. *Indirect Public-Ordering*

A less restrictive measure to achieve the goal of protecting children from harmful material is to offer a set of incentives to various players in the field: if they act in a certain manner, they will enjoy some benefits, and if they behave in a different manner, they might suffer some losses. In the digital environment, the prominent example of such a regulatory approach is the liability of Internet Service Providers ("ISP") for third-party content.[119]

There are various kinds of ISPs. Some offer only access to the Internet and, in this respect, are similar to telephone companies ("common carriers"). Others offer content produced by users, such as web sites which allow the posting of comments, including links and files. These are either supervised or unsupervised, and operate either synchronically (chat rooms) or a-synchronically ("forums" or bulletin boards). Accordingly, the services offered range from a mere platform to a more active role. Yet other services offer location tools, such as search engines or indexes, or technology which enables users to communicate directly, such as Instant Messaging or peer-to-peer systems like Kazaa.

Imposing liability on ISPs seems, at least at first, to be a reasonable measure; if aiming at the speakers might limit their freedom of expression, why not aim at another link in the chain, which is, in many cases, also a technological bottleneck, since much of the communication passes through its services. Since it is not the ISPs who produce the speech, the argument continues, imposing liability does not raise

119. The discussion that follows does not purport to be exhaustive. There is abundant literature on this topic. *See, e.g.*, Assaf Hamdani, *Who's Liable for Cyberwrongs?*, 87 CORNELL L. REV. 901 (2002). The problem has arisen in the context of copyright infringement by third parties, with some similar considerations. *See, e.g.*, Niva Elkin-Koren, *Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators*, 13 CARDOZO ARTS & ENT. L.J. 345, 372–380 (1995); Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1840–44 (2000).

any particular free-expression difficulties. The latter argument depends, of course, on the kind of service imposed: a common carrier or a search engine does not have a free expression interest in the communication it carries or points to, just like the telephone company does not have such an interest in the communication of the users, but a web site that offers editorial services might have such an interest, and thus its freedom of expression will be triggered. However, given the application of Article 10 discussed above, and the more limited nature of the restraint here, a challenge asserting the expression rights of the ISP seems less likely to succeed.

Imposing liability on ISPs would cause them to undertake measures to avoid the risk of liability. An ISP may adopt a reviewing procedure to evaluate the material users wish to post on-line, either before the message is posted, or to adopt a "take down" policy, where the ISP reviews the material *after* it is posted, and then deletes whatever it believes is harmful (or for that matter, any illegal material). Another possible policy would be to "take down" content only after a specific complaint is made ("notice"), accompanied with a procedure to inform the person who posted the material in the first place. These policies can be accompanied with specific terms embodied in the contract between the ISP and the user.

It is easy to see that this system is much more attractive than direct public-ordering. However, it also has quite a few apparent unintended consequences. Firstly, it imposes costs on ISPs. Establishing and operating a "notice and take down" policy, for example, requires substantial amounts of money, and a review mechanism requires even higher amounts. There is also a question of the technological possibility: can there be a meaningful review process in a system where millions of messages are exchanged every minute? If we do impose liability, the result would be that fewer operators will be able to undertake their operations. This would result in concentration of ownership,[120] impediment to competition, and raising prices. The users, needless to say, would be those who would eventually bear the costs.

Secondly, since the ISP would naturally wish to avoid liability, it would have to make decisions regarding the legality of the content. This task is almost impossible, given the global nature of the Internet:

120. This concentration of private power might later on become attractive for the state, for example, in pursuing its battle against terror. This raises another host of questions. For discussion, see Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. (forthcoming) (on file with authors).

what is legal in one place might be illegal elsewhere.[121] Such liability will cause ISPs to remove any material about which a complaint is made, even where the complaint lacks merit.[122] Hence, we can expect that the ISP will act in a censorial spirit; whenever there would be a doubt as to whether some material is harmful to children, the ISP would be quick to click on the "delete" key. In other words, imposing liability on ISPs results in a chilling effect on the ISPs, and it would affect quite immediately the rights of users—the potential speakers and receivers of information.[123]

The fact that the legal environment would now be that of private law—the question being whether the ISP violated the contract with the user—further limits the rights of users. The ISP is not obliged to provide service; it is not accountable and does not have to explain its decision (especially in light of the broad disclaimers which are often included in "terms of use" contracts). In other words, replacing direct public-ordering with indirect public-ordering has the effect of privatizing the enforcement of the protection of freedom of expression, in a manner that expression is likely to lose. A challenge by a user would be dependent on some horizontal effect of the rights.[124]

Thirdly, in light of rules of liability, some ISPs might be drawn to change their business model: they will reduce their involvement and strive to offer less editorial services and more of a "common carrier" service. Liability will actively discourage ISPs from taking responsibility, and attempting to monitor content, as ignorance could act as a

121. The Yahoo! controversy in France is a clear example. Whereas trading Nazi memorabilia is illegal in France, it is "covered" by the First Amendment. This did not deter a French court from ruling that the French subsidiary of the American Yahoo! is bound by French law when operating in France. *See* LICRA (League Against Racism and Antisemitism) v. Yahoo! Inc., (County Court, Paris, Nov. 20, 2000), *available at* http://www.cdt.org/speech/international/001120yahoo.france.pdf. Following this decision, an American court declared the French ruling to be unenforceable in the US. *See* Yahoo!, Inc. v. La Ligue Contre le Racisme et L'Antisemitisme, 169 F. Supp. 2d 1181, 1194 (N.D. Cal. 2001).

122. *See* Press Release, Cyber-Rights & Cyber-Liberties (UK), *U.K. ISP Found Liable for Defamation*, http://www.cyber-rights.org/press/1999.htm (Mar. 26, 1999); Yaman Akdeniz, *Case Analysis of* Laurence Godfrey v. Demon Internet Limited, 1999 J. CIV. LIBERTIES 260, 260–67, *available at* http://www.cyber-rights.org/reports/demon.htm; Kit Burden, *Damned for Defamation*, 15 COMP. L. & SECURITY REP. 260 (1999); Lillian Edwards, *Defamation and the Internet*, *in* LAW AND THE INTERNET: A FRAMEWORK FOR ELECTRONIC COMMERCE, *supra* note 14, at 267.

123. This seems to be the main consideration which led the U.S. Congress to accord ISPs strong immunity in many situations. *See* 47 U.S.C. § 230(c)(2) (2000); Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997).

124. Space precludes a detailed discussion, but in the context of the UK Human Rights Act, see Murray Hunt, *The "Horizontal Effect" of the Human Rights Act*, 1998 PUB. L. 423; Richard Buxton, *The Human Rights Act and Private Law*, 116 L.Q. REV. 48 (2000); H.W.R. Wade, *Horizons of Horizontality*, 116 L.Q. REV. 217 (2000).

shield for liability.[125] If this is the effect, then society loses twice: it has less valuable services to choose from and the content is not reviewed by anyone. Thus, the harmful material will find its way to the "market."

After some experiments, the European Community opted for a rather general structure of liability imposed on ISPs. Before we look into this scheme, it might be a good idea to look at a couple of prior events. One is the *Somm* case in Germany, the other being the English case of *Godfrey v. Demon.*

The *Somm* case illustrates some of the difficulties of imposing liability on ISPs.[126] Felix Somm was the chief executive of CompuServe, Germany, a subsidiary of CompuServe USA. The German company provided access services to the Internet, including access to material stored on the servers of the American company. Some users posted material such as child pornography, bestiality, and violent games on various Usenets. The distribution of these was illegal in Germany (and probably in other jurisdictions as well).[127] In 1995, the German police acted and informed Somm of the illegal material. Immediately thereafter, CompuServe blocked access to all Usenet newsgroups, all over the world.[128] That was an unprecedented response (which has apparently not since repeated itself). The access remained blocked for two months.

Somm was charged and, in May 1998, convicted by the Munich Local Court of assisting the dissemination of material harmful to minors.[129] The case raises many interesting and important issues, such as conflict of laws and choice of law, but for the current purpose we should note the ability of Somm to control the material and delete it: he had no such control, since the material was stored on servers owned by another company (though not a stranger to the German subsidiary) in another country. All Somm did was to provide access.

125. *See* Andrew Joint, *Paedophiles and Their Use of Online Chat Facilities*, 152 NEW L.J. 1602, 1602 (2002).

126. *See* People v. Somm, Amtsgericht, File No. 8340 Ds 465 Js 173158/95 (1998) (English translation by Christopher Kuner available at http://www.cyber-rights.org/isps/somm-dec.htm (Sept. 1998)).

127. Thus, for example, the German Federal Review Board listed the games at stake as morally harmful to minors. *See id.* at § II.2.

128. *See* Mark Konkel, Comment, *Internet Indecency, International Censorship, and Service Providers' Liability*, 19 N.Y.L. SCH. J. INT'L & COMP. L. 453, 454–55 (2000). The number of users affected was reported to be as high as 4.3 million. *See* MARGARET JANE RADIN ET AL., INTERNET COMMERCE: THE EMERGING LEGAL FRAMEWORK 1058 (2002).

129. *See Somm*, *supra* note 126.

Even if Somm did have the technical ability, what should he have done, given that 99 percent of the material available in the Usenets was legal?[130] Furthermore, it is quite likely that some of the material was illegal in Germany but legal elsewhere (we can assume that at least the games were legal in the US).

The events that accompanied the case were no less interesting. The German legislature amended the relevant statutes so as to clarify that ISPs are immune from liability for third-party content, and the prosecutors changed their minds. They themselves appealed the conviction, and in 1999, the appellate court acquitted Somm.[131]

Although the case dealt with illegal material, it illustrates the difficulties of imposing liability on ISPs. Not all ISPs are technical bottlenecks. In addition, it is difficult, if not impossible, to separate the legal from the illegal. Furthermore, the potential liability has a "freezing" effect on speech. The difficulty to identify the unwanted content is even more acute when the legality turns not only on the content, but on the user—that is, whether she is an adult or a minor.

In the English case of *Godfrey v. Demon Internet Ltd.*,[132] the ISP (Demon) offered a Usenet service in which users' postings were stored for two weeks. An unknown person made an obscene and defamatory posting purporting to be written by Godfrey. Godfrey informed Demon that the posting was a forgery and requested that it be removed. Demon failed to do this, and the message remained until its expiry. The libel proceedings subsequently brought by Godfrey tested the issue of ISP liability in the UK. Under the Common Law standard, Mr. Justice Morland held that Demon was the publisher and that the transmission of such a posting from the service provider to any person accessing it was publication:

> the defendants, whenever they transmit and whenever there is transmitted from the storage of their news server a defamatory posting, publish that posting to any subscriber to their ISP who accesses the newsgroup containing that posting.[133]

Demon was not just the mere passive conduit of information, but chose to receive the postings, to store them, to make them available to users, and could have removed them. Demon's defense of "innocent dissemination" under Section 1(1) of the Defamation Act of

130. *See Somm*, *supra* note 126, at § V.
131. For a discussion of these events, see Konkel, *supra* note 128, at 463–65.
132. [2001] Q.B. 201.
133. *Id.* at 208–09.

1996 was rejected as Demon had been given notice of the posting by Godfrey.[134] The effect of the decision is to require ISPs providing that type of service to remove the material once they acquire knowledge of the unlawful content.

This approach indeed fits the requirements of the EC E-Commerce Directive[135] that was implemented in the UK in August 2002.[136] Unlike the US, which has two separate legal regimes that govern liability of ISPs—one in regard to copyright law and one for all other kinds of content—the European Directive determines a unified system.[137] The European regime differentiates between the kinds of service provided. Firstly, it assures immunity to ISPs who are mere conduits. Article 12 sets a few conditions which ensure that the ISP is indeed a conduit and is not involved in initiating or editing the message transmitted, or editing it, and does not determine the parties of the transmission.[138] Secondly, it provides the ISP with immunity for caching, *i.e.*, automatic, intermediate, and temporary storage. Caching is a vital technological step for transmission of information under the current architecture of the Internet, in that it eases the traffic over the Internet and enables a rather quick and accurate transmission.[139] This immunity is subject to the ISP not interfering with the transmissions, and to its removal of material upon requiring knowledge that the original material is no longer available. Thirdly, the Directive requires that ISPs be awarded immunity for content stored on their servers by users.[140] This immunity is subject to lack of knowledge on

134. Section 1(1) of the Defamation Act, 1996, c.31, provides:

In defamation proceedings a person has a defence if he shows that—

(a) he was not the author, editor or publisher of the statement complained of,

(b) he took reasonable care in relation to its publication, and

(c) he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.

135. *See* Council Directive 2000/31/EC of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1–16 [hereinafter E-Commerce Directive].

136. *See id.*; Electronic Commerce (EC Directive) Regulations 2002, No 2013; Graham Smith & Alex Hand, *Implementing the E-Commerce Directive*, 152 NEW L.J. INFO. TECH. SUPPLEMENT 1597, 1597–99 (2002). Under European Community law, a directive requires the Member States to adopt their local law so as to comply with the general principles enumerated in the Directive.

137. The liability of ISPs for copyright infringement is defined in 17 U.S.C. § 512 (2000), and for any other content, in 47 U.S.C. § 230 (2000), notwithstanding the effect of criminal law, intellectual property law, state law, and the Electronic Communications Privacy Act of 1986. *See* 47 U.S.C. § 230(e) (2000).

138. E-Commerce Directive, *supra* note 135, Art. 12. Article 12 further clarifies that it refers to "automatic, intermediate and transient storage of information."

139. E-Commerce Directive, *supra* note 135, Art. 13.

140. E-Commerce Directive, *supra* note 135, Art. 14.

behalf of the ISP, and to the condition that once such knowledge is acquired, the content is removed. This is usually referred to as the "notice and take-down" principle. Whether an ISP can be deemed to have such constructive knowledge will depend on the circumstances; it may in some cases be blatantly obvious from the name of the Usenet group that it is to be used for obscenity or defamatory purposes.[141] Finally, the Directive requires that "Member States shall not impose a general obligation on providers... to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity."[142]

This is not a perfect system either, and it does impose costs on the ISPs, as well as risks. If the ISPs, upon receiving a notice of harmful content, take it down, and it later turns out that the material was perfectly legal, they face the risk of being sued by the user who posted the content at stake.[143] In the UK, the police had initially considered pursuing ISPs to combat the problems of pornography.[144] However, a balance seems to have been struck between increasing the expense of monitoring and risking liability, since now the Internet Watch Foundation ("IWF") notifies the ISPs of any unlawful material, and the ISP can then take the necessary steps to avoid liability.[145]

The overall result is one of a careful regulation that adopts an indirect public-ordering approach. It provides the ISPs with an option to choose immunity, so as not to act in a censorial mode, and thus protects both the ISPs' commercial and proprietary interests and, more importantly, does not interfere with the "marketplace of ideas" since the users are not affected. But, unlike the US regime regarding defamation, violations of privacy, or even negligence to remove child pornography,[146] this immunity is not absolute. Upon notice, the ISP

141. Gavin Sutter, *'Nothing New Under the Sun': Old Fears and New Media*, 8 INT'L J.L. & INFO. TECH. 338, 365–66 (2000).

142. E-Commerce Directive, *supra* note 134, Art. 15.

143. *See* Reuters' Report, *Europe's ISPs Overrun with Website Take-Down Orders* (Dec. 11, 2002), *available at* http://www.ispa.org.uk/html/media/coverage.html.

144. *See* Sutter, *supra* note 141, at 368–70.

145. The Internet Watch Foundation ("IWF") is one of the means of private ordering, which we discuss *infra*, text accompanying note 214. This is a clear example of the mixed European approach, of combining an indirect public ordering approach (rules pertaining to ISP liability) and private action (the IWF).

146. This is the immunity provided under 47 U.S.C. § 230 (2000). In one horrifying case, the Florida Supreme Court found that an ISP enjoyed immunity, despite its refusal to take down advertisements for the sale of videotapes and photographs posted in chat rooms depicting the rape of an 11-year-old child. The child's mother sued the ISP for negligently failing to act to remove the messages. The majority found the ISP to enjoy immunity, over the dissent of Justice

must act. In this manner, the cost imposed on it is minimized; it is cheaper to establish a system to receive notices and act upon their receipt than to build and maintain a monitoring system. The protected interest (privacy, reputation, etc.) is protected. The ISP need not act accordingly, and then it might risk a suit, in which it will be able to litigate the issue and raise "regular" defenses under the relevant cause of action.

Another form of public-ordering operates through the kind of policies at libraries and other areas where the public can access the Internet. In the UK, public libraries are run by local authorities (or library authorities) and have a duty "to provide a comprehensive and efficient library service for all persons desiring to make use thereof."[147] However, this duty does not extend to stocking pornography. Some materials stocked may be suitable for adults but deemed harmful to children. In this case, a restriction to prevent offense or any other harm being caused by stocked materials may not be out of step with the past practices of some libraries. In the past, libraries have been reported to have taken controversial books off the shelves but made them available upon request, for example with *The Satanic Verses*.[148] The problem discussed in this paper is distinct in that it is not practicable to request permission for access to every web site. The closest control is to provide filtering software or a system of ratings and to require permission before the software is to be disabled, which will be discussed below. Such measures would also raise the issues of privacy and the chilling effect considered by Etzioni.

D. Private-Ordering

A third regulatory regime avoids any public interference with the market, including the *pornography chain*. It leaves the regulation to the market. Obviously, this approach might not satisfy many. In the absence of regulation, some players will do nothing to prevent the distribution of harmful material, as well as illegal material, or children's access thereto. But quite a few will opt for this approach on

Lewis. *See* Doe v. Am. Online, Inc., 783 So. 2d 1010 (Fla. 2001) (applying *Zeran v. Am. Online, Inc.*, 129 F.3d 327 (4th Cir. 1997)).

147. Public Libraries and Museums Act, 1964, c.75, § 7(1). While this service is provided by local authorities, the Secretary of State for Culture Media and Sport superintends the system under Section 1. If a complaint is made that a library authority has failed to fulfill its duty, then the Secretary of State can hold an enquiry on the matter, after which an order declaring it in default and directing it to carry out its duties can be made.

148. Nicolette Jones, *For Your Eyes Only?*, TIMES (London), Jan. 7, 1999, at 36.

their own initiative, and the stronger players in the market are more likely to do so. The reason is simple: it is good for their business.[149] The ISPs, like any player in the market, prefer to take care of their own business and avoid external interference. ISPs know that in the absence of a serious effort on their behalf, the legislature or the courts are likely to fill the vacuum. In addition, the ISPs are interested (or should be interested) in providing a better service to their clients. If clients demand a "clean" environment, the wise ISP will do its best to supply it. A refusal of an ISP, for instance, to remove child pornography from its servers and block access to it might result in a public relations disaster.[150] Furthermore, as long as the legal climate is uncertain, ISPs fear they might be found jointly liable for the illegal acts of third parties.

Private-ordering can take many forms. Establishing a clear method of communication of users to the ISP for complaints of harmful or illegal material, *i.e.*, a "notice" system, followed by a "take-down" policy, is one example.[151] Adopting a clear code of conduct aimed at both the employees and the users, accompanied with sanctions, is another way. The "terms of use" can embody this code of conduct, and if formalities are met, they can be designed as a valid and enforceable contract. The contract can determine, for example, that a user who posts harmful material will be disconnected and his or her service terminated. The contract can further include a disclaimer that will immunize the ISP from breach of contract if it terminates an account in such circumstances. Another mechanism is one of labeling, or rating, which we will discuss shortly.

Private-ordering, or self-regulation, can also make use of technology. There are some technologies, and we are likely to see more in the future, that purport to "take care" of some of the concerns discussed here. Age-verification technologies, discussed earlier, are one example.[152] Filtering software is another interesting technology which we examine.

Self-regulation need not be left all to its own. Government can provide "background rules" either in the form of direct requirements (in which case it is no longer *self*-regulation), or a sanction for misrep-

149. Obviously, there might be other reasons as well, such as the moral views of the shareholders and executives of the ISPs.

150. *See, e.g.*, the sad case of *Doe v. Am. Online, Inc.*, 783 So. 2d at 1010.

151. *See supra* text accompanying note 140.

152. *See* Reno v. ACLU, 521 U.S. 844 (1997); *supra*, text accompanying note 19.

resentation,[153] in which case it is better to view this as an indirect public-ordering. But government can have an active role in supporting self-regulation, without direct or indirect interference. This is the European way thus far.

We begin by surveying the rating system and the filtering software, and then turn to survey the European measures undertaken thus far.

1. Ratings

The Platform for Internet Content Selection ("PICS") provides a technological method for rating the content of web sites. PICS is an industry standard that allows labels to be attached to web materials that can be read by a computer receiving the information. The technology differs from a filtering system which blocks sites that contain certain keywords.[154] Instead, PICS recognizes a predetermined label for the material. It has been used to develop ratings systems in which pages are given a label describing the content. Much depends on which system is used. Initial ratings were developed by the Recreational Software Advisory Council ("RSACi"), and its successor was launched in December 2000 by the Internet Content Rating Association ("ICRA").[155] This system is the most prominent and is built into both Internet Explorer and Netscape Navigator. The system places material into categories, including language, nudity, sex, and violence. The producers of the web pages then provide details of the content of their material in accordance with these categories.

The PICS standard was devised to create a means for material to be rated by content providers and by third parties for use by parents and teachers.[156] It allows the users to choose what sort of content they would like to see, and allows sites to be blocked according to those preferences. For example, if a viewer wishes to view violence but not nudity, then the software can be set in such a way. Those developing PICS recognized that a diversity of standards exists among Internet users and that access should be provided to a wide range of ratings

153. Compare to the U.S. Federal Trade Commission's power to prevent the use of "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce." *See*15 U.S.C. § 45(a)(1) (2000).

154. Harry Hochheiser, Computer Professionals for Social Responsibility, *Filtering FAQ*, http://www.cpsr.org/filters/faq.html#3.1 (Apr. 6, 2001).

155. *See* Internet Content Ratings Association, http://www.icra.org/.

156. World Wide Web Consortium, *PICS Statement of Principles*, http://www.w3.org/PICS/principles. html (last visited Nov. 3, 2003).

products.[157] In theory, PICS allows a method of preventing access to harmful material, but in a manner that is not imposed from a centralized source unrepresentative of any views as to what is harmful and what is not.

In practice, PICS raises some difficulties similar to filtering, which we will discuss shortly. PICS has been criticized, as one or two ratings systems dominate the market and create a uniform method of rating content that is built into Internet software.[158] Most users are likely to use whatever software comes with the browser, thereby undermining the commitment to diversity that is cited as one of PICS' strengths. Not every producer of material has the expertise or resources to provide a rating. However, some of the filtering software will automatically prevent access to sites that are unrated. Web content that goes unrated will thereby be harder to access, unless the user has the knowledge to remove the ratings software.[159] Consequently, large corporate sites that have the support and resources to self-rate may dominate the Internet. In addition, fears exist that rating will become the first step on a path to greater regulation—that when the software is found not to fulfill the high expectations of preventing access to harmful content, as seems inevitable, calls will be made for more direct censorship.[160] Furthermore, critics argue that it is impossible for all types of speech to neatly fall into the categories of rating.[161] If a website about sexually transmitted diseases is labeled as sexual content, then it may be placed out of the reach of younger users. The last concern, but not the least, is who determines the standards. PICS envisions that software companies or website operators determine the rating. But these companies, benevolent as their motivations might be, are unelected and are not accountable. If PICS succeeds, the result is that the public has delegated its power to make moral judgments to technology designed by for-profit corporations.

2. Filtering Software

Filtering software purports to identify the content of on-line material and, accordingly, separate the "good" from the "bad." At the

157. World Wide Web Consortium, *Statement of the Intent and Use of PICS: Using PICS Well*, http://www.w3.org/TR/NOTE-PICS-Statement (June 1, 1998).

158. American Civil Liberties Union, *Fahrenheit 451.2: Is Cyberspace Burning?*, http://archive.aclu.org/issues/cyber/burning.html (Mar. 17, 2002).

159. *Id.*

160. *Id.*

161. *Id.*

heart of the software lie lists of URLs,[162] and IP addresses,[163] or an algorithm that reflects the choices and decisions of the code's designers. Today there are several commercial products available on the market, at an average annual cost of less than a $100. The software can be installed at various points, either on the user's computer or the ISP's servers. The technology aims at breaking the *pornography chain* just before it arrives at its destination: the minor user. The software, once installed, is supposed to block access to sites and other content it recognizes as harmful.

How is the algorithm composed? The various corporations engaging in this field adopt various methods.[164] Some employ parents who simply check websites and label them according to their content and according to the corporation's criteria; the label is then used to classify the website into "white lists" and "black lists." The algorithm reflects the lists. A second method is based on the software "reading" the web site, access to which is requested by the user. If the software identifies certain words (in the URL (the web address), the meta-tags, or the body of the website) such as "sex," it will block access. A third method is more sophisticated and is based on as many features as possible of pornographic web sites, such as the size of the letters, internal and external links, colors, text, etc. These are combined into a complex algorithm.[165] Of course, the various methods can be used in conjunction with each other.[166]

What are the exact criteria that guide each software-producer? The designers maintain this as a secret, or to be more precise, a trade secret.[167] This is not just a peculiar feature of intellectual property law.

162. A URL is a "Uniform Resource Locator," which is the "web address" of a web site, either numerically (the IP address) or a textual domain name. *See* Am. Library Ass'n, Inc. v. United States, 201 F. Supp. 2d 401, 417 (2002).

163. For an analysis of the limits of IP-based filtering software, see Benjamin Edelman, Berkman Center for Internet and Society, Harvard Law School, *Web Sites Sharing IP Addresses: Prevalence and Significance*, http://cyber.law.harvard.edu/people/edelman/ip-sharing/ (last updated Sept. 12, 2003).

164. For discussion of some of these methods, see *Am. Library Ass'n, Inc.*, 201 F. Supp. 2d at 427–36.

165. *See* iCognito, *Technology Overview*, http://www.puresight.com/technology/about.shtml (last visited Nov. 3, 2003).

166. *Am. Library Ass'n, Inc.*, 201 F. Supp. 2d at 427–36.

167. Trade secret law allows reverse engineering of the product, to reveal its "secret." However, reverse engineering of software inevitably requires its temporary copying. One US court found such a copying which was accompanied with a "bypass" code, to be copyright infringement. *See* Findings of Fact and Conclusions of Law at 11, Microsystems Software, Inc. v. Scandinavia Online AB (D. Mass. 2000) (No. 00-10485-EPH), *available at* http://www.epic.org/free_speech/censorware/cp_conclusions.html. Later on, the Librarian of Congress exempted this kind of reverse engineering from liability under the anti-circumvention

It is a matter of freedom of expression; it disables public supervision of the moral criteria chosen by unelected and unaccountable corporations. Indeed, the software producers can do so, and parents can buy the product. A parent is allowed to knowingly substitute his or her own moral reasoning and beliefs about education with the unknown choices of a corporation. The free speech problem arises when the software is installed in public institutions, such as public libraries. By installing filtering software, a public library in practice delegates its constitutional obligation not to interfere with freedom of speech, though it may itself be vulnerable to constitutional challenge.[168] This is an unfortunate event, especially in light of the many shortcomings of the software.

This problem is enhanced by the features of the industry at stake. There is a fierce competition among the producers of filtering software, and it seems that the competition drives them to block more rather than less. Another deficiency is that most of the programs are aimed at the American market, *i.e.*, at English content, and to the extent that moral judgments are made, they attempt to address the American taste.[169]

The current level of technology does not filter out 100 percent of pornographic content; it filters much more and, at the same time, much less. There is a long list of web sites which were erroneously blocked,[170] ranging from sites on breast cancer, sexual education, gays and lesbians, and planned parenthood, to sites of political organizations and candidates, a site which watches and criticizes the filtering software industry,[171] and even some sites containing legal documents

rules of the Digital Copyright Millennium Act, according to the authority given to him to do so under 17 U.S.C. § 1201(a)(1)(C) (2000). *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64556 (Oct. 27, 2000) (to be codified at 37 C.F.R. pt. 201).

168. Indeed, a US court found that a public library's decision to install filtering software runs afoul of the First Amendment. *See* Mainstream Loudoun v. Bd. of Trs. of the Loudoun County Library, 24 F. Supp. 2d 552, 570 (1998). An act that conditioned certain financial support to public libraries on installing filtering software has also been found unconstitutional, *Am. Library Ass'n v. United States*, 201 F. Supp. 2d 401 (E.D. Pa. 2002), but this decision was reversed by the Supreme Court, 123 S. Ct. 2297 (2003). *See* Children's Internet Protection Act ("CIPA") § 1712, Pub. L. No. 106-554, 114 Stat. 2763A-335, 2763A-340 (2000).

169. For a similar argument, see Carolyn Penfold, *The Online Services Amendment, Internet Content Filters, and User Empowerment*, 2000 NAT'L L. REV. (Austrl.), *at* http://pandora.nla.gov.au/parchive/2001/Z2001-Mar-13/web.nlr.com.au/nlr/HTML/Article/penfold2/ penfold2.htm.

170. Some of these cases are mentioned in *Mainstream Loudoun*, 24 F. Supp. 2d at 556 n.2; *Am. Library Ass'n, Inc.*, 201 F. Supp. 2d at 446–47, and others are documented in a web site devoted to critically analyzing filtering software. *See* PeaceFire, http://www.peacefire.org/.

171. *See* Peacefire, *Blocking Software FAQ*, http://www.peacefire.org/info/blocking-software-faq.html (last visited Nov. 3, 2003).

and cases.[172] At the same time, independent surveys and studies found that the current software fails in filtering up to 20 percent of the pornographic sites.[173]

For the sake of the discussion, we are willing to assume that this is a transitional problem, and that technology will be developed that can block no more and no less than it is designed to. In many cases, this is a rather easy task which does not raise many constitutional difficulties. If an image of child pornography is blocked, neither an American nor a European court will object. But here lies the problem: in many cases it is unclear, and it cannot be made clear, in advance whether the content at stake is harmful to children or not. A court can decide so in retrospect, but what is the line between that which is harmful to a child and that which is not? Is an image of a naked person necessarily harmful? It might be a picture in a biology book, or a painting in a museum, or Michelangelo's statute of *David*. The answer lies in several factors that technology cannot "know" and cannot "understand": the context in which the content appears, the age of the user, the time and place, and the community's moral standards.[174] The conclusion is that the filtering software limits the "breathing space" which is so necessary for free speech. All of these problems are further enhanced by the inability to distinguish a child from a teenager from an adult, for whom the same content is not considered "harmful."

The problems caused by filtering can be illustrated by the experience in the UK. The UK government is committed to extending access to the Internet in schools and public libraries. No obligation exists in the UK for libraries to use filtering and rating software on public Internet stations. Instead, whether such guards are to be used is the decision of the local authority responsible for the library. The Library Association, in not endorsing filtering software, warns that it

172. Thus, for instance, a decision of the Israeli Supreme Court on gays' rights was blocked by a filtering program installed in the Hebrew University of Jerusalem. *See* Letter of Adv. Dori Spivak to Adv. Pappi Yakirevitch (July 19, 2000) (on file with the authors).

173. *See* Consumer Reports, *Digital Chaperones for Kids: Which Internet Filters Protect the Best? Which Get in the Way?*, March 2001, *available at* http://www.consumerreports.org/main/detail.jsp?CONTENT%3C%3Ecnt_id=18867& FOLDER%3C%3Efolder_id=18151&bmUID=996766578117; Victoria Rideout et. al., Henry J. Kaiser Family Foundation, *See No Evil: How Internet Filters Affect the Search for Online Health Information* (Executive Summary), http://www.kff.org/content/2002/3294/Internet_Filtering_exec_summ.pdf (Dec. 2002).

174. The *Miller* test, applied in the US to define obscenity relies, *inter alia*, on "community standards." But once we go online, what is the relevant "community"? The Supreme Court struggled with this issue in *Ashcroft v. ACLU*, 535 U.S. 564 (2002), concluding that the statute's failure to define "community" does not in itself render it unconstitutional. *Id.* at 585–86.

is not always effective and may lead to a false sense of security that harmful material can no longer be accessed.[175] The Association further argues that "such software is inconsistent with the commitment or duty of a library or information service to provide all publicly available information in which its users claim legitimate interest."[176] Before allowing public access, libraries are encouraged to develop an "Acceptable Use Policy," which will determine who has access, what charges apply, whether it is filtered, and a code of conduct for users. This may include whether users will be required to have a user password or at least register their name at the time of use, either of which can raise privacy issues. A policy paper issued by the Networked Policy Task Group advises those managing libraries on the pros and cons of filtering, and while not coming to any specific recommendation, emphasizes the need to have a policy in place.[177] While the government has not legislated or made funding conditional on installing filtering software, information is provided to schools and on-line centers to help decide what measures are most suitable to limit harmful Internet content.[178] Such guidance accepts that some people may find a "culture of responsible use amongst their adult users is preferable to software filtering," and directs centers to consider the flexibility of a system for different-aged users before fitting filtering software.[179]

Much is therefore left to the local authorities to decide what approach to take. The different approaches taken in various areas have been shaped by a process of trial and error, rather than through courtroom battles as in the US. For example, Gloucester Council initially required written parental consent for children to gain unfiltered access to the Internet in a public library, as filtering software was thought to block out legitimate sites.[180] However, this was argued to be inadequate, as parents do not always know what sites their children will access once on-line.[181] Consequently, the policy was changed so that children were allowed access only to computers fitted with a

175. Library Association, *Guidance Notes on the Use of Filtering Software in Libraries*, http://www.la-hq.org.uk/directory/prof_issues/filter2.html (2000).

176. Library Association, *The Use of Filtering Software in Libraries*, http://www.la-hq.org.uk/directory/prof_issues/filter.html (1999).

177. Sara Ormes, *An Introduction to Filtering*, http://www.ukoln.ac.uk/public/earl/issuepapers/filtering.html (last visited Nov. 25, 2003).

178. *See, e.g.*, Superhighway Safety, http://www.saftey.ngfl.gov.uk/.

179. Superhighway Safety, *Internet Filtering Systems*, http://safety.ngfl.gov.uk/ukonline/pdf/d3.pdf (last visited Nov. 3, 2003).

180. GLOUCESTER ECHO, Apr. 30, 2002.

181. *Id.*

filter, with a number of unfiltered machines being left aside for adult use only.[182] Other libraries are more stringent and fit all computers with a filter, allowing teenagers and children under sixteen access to the machines only with parental permission.[183] On one occasion, a local authority in Glasgow shut down all access to the Internet temporarily after a school child gained access to pornography in a public library.[184] Prior to this, filters on all computers had been scrapped as they were found to be blocking legitimate sites.[185]

While the policies of these libraries may not have been met with same legal challenges as were libraries in the US, that is not to say that all attempts to protect children have been met with approval. Complaints have been made that blocking software prevents access to certain political and religious sites.[186] In one instance, a local authority was threatened with legal action after the filtering software blocked the far right British National Party web site, and later allowed the site to be accessed.[187] Such complaints are supported by concerns voiced in a recent study that that filtering software can block access to important information on health issues.[188]

The lesson is that technology can be an aid in shielding children from on-line pornography, but it has a substantial social cost: it means that, in essence, we desert the educational avenue; it means we delegate our moral judgments as moral agents and as a society at large to technology, a technology that is quite resistant to inspection; and it means we pay a price in terms of free speech. At the end of the day, technology cannot, and should not, substitute for human judgments.

3. The European Action Plan

The institutions of the European Union started looking into the matter of protecting children from harmful material available in the

182. Gloucester Council fitted eighty of its 200 library computers with filters following a complaint from a mother that witnessed teenagers accessing indecent images in a library. GLOUCESTER ECHO, Nov. 21, 2002.

183. For the Manchester Library Policy, see Manchester City Council, *Using the Internet*, http://www.manchester.gov.uk/libraries/ict/internet.htm (last updated Jan. 20, 2003).

184. Graeme Murray, *Schools in New Bid to Block Web Porn*, EVENING TIMES (Glasgow), Sept. 16, 2002, at 2 (referring to the East Ayrshire Council).

185. Gerry Braiden, *New Rules to Protect Scots Pupils from Net Perverts: Youngsters Will Not Be Given E-Mail Names*, EVENING TIMES (Glasgow), Mar. 21, 2001, at 5.

186. *See Censorship Concern*, ESSEX CHRON., Nov. 15, 2002, at 2.

187. *Around Wales: Monmouthshire*, WEST. MAIL, Oct. 29, 2001, at 6.

188. Rideout et. al., *supra* note 173.

digital environment in the mid-1990s.[189] From the very beginning, it was determined that the interest in protecting children was an issue of "overriding public interest."[190] In 1996 a comprehensive study, the *Green Paper*, was published, and set the agenda:

> The full potential of such developments will depend on society as a whole striking the right balance between freedom of speech and public interest considerations, between policies designed to foster the emergence of new services and the need to ensure that the opportunities they create are not abused by the few at the expense of the many.[191]

The goal was carefully crafted so not to cover illegal materials.[192] It was further observed that adults have a different interest than children: "[t]he aim is therefore limited to preventing minors from encountering, by accident or otherwise, material that might affect their physical and/or mental development."[193] Interestingly, the document also raises the issue of variance between minors of various ages.[194] These principles were expressed based on the assumption that the digital environment carries with it many advantages, and that the new technology requires a different treatment than the old media.[195] Accordingly, the *Green Paper* proposed that different solutions are adopted for these different problems.

The possible negative effect on freedom of expression was also recognized, as the above quoted passage illustrates.[196] The *Green Paper* instructed that any regulation should take it into account under the criteria set forth in the ECHR.

Private-ordering was the option advocated by the *Green Paper* (termed there self-regulation), and was then adopted by the Euro-

189. *See* European Union Communication on Illegal and Harmful Material, COM(96) 487 (proposing policy options for immediate actions); Telecommunications Council of Ministers' resolution concerning dissemination of illegal material over the Internet (Sep. 1996), *available at* http://europa.eu.int/ISPO/legal/en/internet/98-97en.html.

190. *See* Green Paper, *supra* note 22, at 1.

191. *Id.*

192. *Id.* at 6, ch. I, § 1. The illegal material was classified as a "general category of material that violates human dignity," and includes primarily "child pornography, extreme gratuitous violence and incitement to racial and other hatred, discrimination, and violence." To combat child pornography, for example, the EU established police hotlines for users to complain, special police units, a system of cooperation among the Member States, and several international operations took place.

193. *Id.*

194. *Id.* at 19, ch. II, § 2.2.2 ("... it is doubtful whether children of four have the same problems as adolescents of 15").

195. For the comparison of the new media to the old media, *see id.* at 7–11, ch. I, §§ 2–2.5.

196. *See id.* at 13, ch. II, §§ 1–1.1.

pean Commission and the European Parliament.[197] But this approach should not be mistaken for a liberal hands-off attitude. Rather, the underlying but clear direction was that self-regulation can be assisted by the State. The goal was set accordingly, to create a common framework for self-regulation,[198] and national frameworks within the Member States.[199] The idea was to foster a climate of confidence with the relevant industries.[200]

Self-regulation was to be achieved in cooperation with the industries. Some of the measures mentioned were drafting codes of conduct and identifying areas where there might be a need for common standards of labeling material.[201] In addition, it was suggested to raise awareness of users, especially of parents. Codes of conduct, as later EU documents elaborated, should inform users of any risks from the content, provide a warning page, visual signal, or a sound signal, have a descriptive labeling or classification of content, and apply a system to check the users' age, support parental control measures, and handle complaints.[202] In most EU countries there are now operative codes of conduct.[203]

These recommendations were followed up.[204] The most ambitious project undertaken was the multi-annual, 25-million-Euro *Safer Internet Action Plan*, which took place between 1999 and 2002.[205] The

197. *See* Council Recommendation, *supra* note 22, at 50–51 (detailing the various measures taken following the Green Paper).

198. *See* Green Paper, *supra* note 22, at 24–25, ch. III, § 3.1.

199. *See* Council Recommendation, *supra* note 22, at 50, Art. I (1).

200. *See id.*, recital 10, at 49.

201. *See* Green Paper, *supra* note 22, at 25, ch. III, § 3.2.

202. *See* Council Recommendation, *supra* note 22, at 52–55.

203. *See* Evaluation Report From the Commission to the Council and the European Parliament on the Application of Council Recommendation of 24 Sept. 1998 Concerning the Protection of Minors and Human Dignity, COM(01)106 final at 5–6, *available at* http://europa.eu.int/comm/avpolicy/regul/new_srv/ermin_en.pdf; *see also* Council Conclusions of 23 July 2001 on the Commission's Evaluation Report on the Application of the Recommendation Concerning the Protection of Minors and Human Dignity, 2001 O.J. (C 213) 10, 11, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/c_213/c_21320010731en00100011.pdf; Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Intermediate Evaluation of the Implementation of the Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks, COM(01)690 final at 2–7, *available at* http://europa.eu.int/eur-lex/en/com/cnc/2001/com2001_0690en01.pdf.

204. *See* Council Conclusions of 17 Dec. 1999 on the Protection of Minors in Light of the Development of Digital Audiovisual Services, Art. 9, 2000 O.J. (C 8) 8, 9, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/c_008/c_00820000112en00080009.pdf.

205. *See* Decision No. 276/1999/EC of the European Parliament and of the Council of 25 Jan. 1999 Adopting a Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks, Art. 1, 1999 O.J. (L

European Union supported dozens of projects designed to create the common and national framework for self-regulation, focusing on three avenues: (1) *Hotlines*: creating a European network of hotlines to report illegal material. The projects resulted in a group of fourteen countries (including some non-European countries, such as the US and Australia) that have hotlines grouped together into a cooperative system, known as INHOPE.[206] (2) *Rating and Filtering*: several projects examined technological solutions. The intermediate assessment was that self-labeling and filtering schemes were not a practical solution for Europeans, at least in the year 2000, and that third-party filtering software products require major improvements.[207] One of the problems identified was the English language focus of most current filtering technology.[208] (3) *Awareness*: various projects to inform users of the risks and chances online. Furthermore, associations of ISPs were established throughout the EU, including in a pan-European association.[209] The Action Plan has been considered by the EU to be a success, and it is considering extending it for two more years.[210]

The UK government follows the European preference for self-regulation of the Internet. While the government has proposed the creation of a new criminal offense of "sexual grooming" on the Internet, for which individuals can be prosecuted before any sexual act has taken place,[211] it also launched the Internet Taskforce on Child Protection in 2001 to review Internet content rating systems, develop a "kitemarking" scheme for chat rooms, and promote "safe surfing"

33) 1, 3, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/1999/l_033/l_03319990206en00010011.pdf; *see also* Safer Internet, http://www.saferinternet.org.

206. *See* http://www.inhope.org.

207. See the European Union's announcement, Commission Issues Reports on Parental Control Technologies Aimed at Enhancing Safety of Internet, IP/00/621 (Brussels, 15 June 2000), *available at* http://europa.eu.int/ISPO/docs/services/docs/2000/June/ip_00_621_en.pdf.

208. Accordingly, one of the projects funded by the E.U. Action Plan aims at developing a multi-lingual filtering tool. *See* http://www.net-protect.org/en/scope.htm.

209. *See* European Internet Services Providers Association, http://www.euroispa.org.

210. *See* Follow-up to the Multiannual Community Action Plan on Promoting Safer Use of the Internet by Combating Illegal and Harmful Content on Global Networks, COM(02)152 final at 3, *available at* http://europa.eu.int/eur-lex/en/com/pdf/2002/en_502PC0152.pdf. The proposal is to extend the action plan also to new technologies that have been developed in the meantime, such as mobile and broadband content, peer-to-peer file sharing systems, chat rooms, instant messaging and more.

211. In one area, calls were even being made to prevent children from using Internet chat rooms in public libraries, following concerns that two murdered girls had possibly been "groomed" through a chat room. *See Chatroom Ban in Bid to Cut Abuse*, KENT & SUSSEX COURIER, Aug. 30, 2002, at 5. The use of chat rooms in this way shows a new problem caused by the Internet, as such text would not always infringe the Obscene Publications Act. *See* Akdeniz & Srossen, *supra* note 38, at 223.

education and awareness for parents and children.[212] The UK government also recently launched a new campaign warning of the dangers to children from using chat rooms, publishing a code of practice for operators of chat rooms developed jointly by the government, Internet bodies, and child protection agencies.[213]

The Internet Watch Foundation ("IWF") was established in 1996 with the support of the UK government, although it is not a government agency. The IWF operates a hotline to which Internet users can report illegal material, which is then passed on to the police, and which leads to ISPs being issued a notice to take down the illegal material.[214] The fear exists that if this means removing newsgroups that contain some illegal material,[215] this could also remove much legal content along with it. The organization promotes the use of voluntary ratings systems and filtering systems among parents, teachers, and others responsible for children. The IWF also seeks to educate users about the dangers on the Internet, especially for children, and ways of dealing with such problems. The division of functions in this way is argued to reflect the division between illegal and harmful material, promoting merely educational and voluntary measures in relation to the latter.[216]

212. *See* Improving Child Protection on the Internet: A Partnership for Action, http://www.homeoffice.gov.uk/docs/childprotnet.pdf (Mar. 28, 2001).

213. *See* http://www.thinkuknow.co.uk. The Code of Practice suggests chat room operators should include a virtual panic buttons and safety messages for child users. *See* Stuart Millar, *Chat Room Danger Prompts New Safety Code*, GUARDIAN, Jan. 6, 2003, *available at* http://www.guardian.co.uk/uk_news/story/0,3604,869385,00.html.

214. In 2001, the hotline processed 11,357 reports, "leading to notices to UK ISPs to take down 3332 web sites and newsgroup articles containing images of child abuse and 2949 reports to police for investigation." *See* Internet Watch Foundation, 2001 Annual Review (2002), http://www.iwf.org.uk/about/annual_report/ar2002/css/ar2002_2.htm [hereinafter IWF 2001 Annual Review]. The Hotline has been criticized in previous years on the basis that the figures

> tell us little as the actual amount of child pornography on the Internet is unknown. It is, therefore, difficult to judge how successful the UK hotline has been. Another downside is that the efforts of the organisation are concentrated on the newsgroups carried by the UK ISPs. 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.

Cyber-Rights and Cyber-Liberties (UK), *Who Watches the Watchmen Part II: Accountability & Effective Self-Regulation in the Information Age*, http://www.cyber-rights.org/watchmen-ii.htm (Sept. 1998) [hereinafter *Who Watches the Watchmen*].

215. The IWF recommends to ISPs not to host newsgroups that regularly contain child pornography or newsgroups that appear to advertise pedophile content or activity. *See* Internet Watch Foundation, *IWF Tightens Net on Child Abuse*, http://www.iwf.org.uk/news/press/detail_press.epl?INFO_ID=106 (Feb. 13, 2002); Internet Watch Foundation, *National Crime Squad Raids Confirm Newsgroup Strategy*, http://www.iwf.org.uk/news/press/detail_press.epl?INFO_ID=102 (Nov. 28, 2001).

216. Sutter, *supra* note 141, at 370–71.

While the IWF is an independent body, it works closely with the government and in the 2001–02 financial year, it received state funds.[217] It also liaises with other regulators, such as the Broadcasting Standards Commission and the British Board of Film Classification, and with industry, such as the Internet Service Providers Association and the London Internet Exchange. In addition to this, the organization has frequent exchanges with children's charities, and has attempted to work internationally with groups on similar projects. Concern was initially expressed about the lack of involvement from civil liberties groups,[218] though later the Board was reconstituted to gain more balance. While the IWF has been seeking a broader base of subscribers, most of its funding has come from ISPs,[219] and it is still very much linked to the industry.

The IWF has been criticized on the grounds that it operates as a regulatory body providing a public function involved in the development of government policy, but with the status of a private body.[220] This function will remain in the hands of the IWF even after the establishment of a new communications regulator.[221] This is indeed one of the constitutional difficulties with a legal regime of private-ordering—the private bodies are, depending on the extent of horizontal effect, beyond the reach of constitutional law.[222] Consequently, it has been argued that the body has avoided many of its public responsibilities, such as providing open information on why certain policies such as filtering are to be preferred, without proper public consultation or the normal channels of accountability.[223] In advising whether material is illegal, the IWF can be argued to be performing a quasi-

217. *See* IWF 2001 Annual Review, *supra* note 213.

218. Akdeniz & Strossen, *supra* note 38, at 224–25.

219. *See* IWF 2001 Annual Review, *supra* note 213. However, it has also received grants from the European Commission.

220. *Who Watches the Watchmen*, *supra* note 214. For similar criticisms, see Cyber-Rights and Cyber-Liberties (UK), *Memorandum for the Internet Content Summit 1999*, http://www.cyber-rights.org/reports/summit99.htm (Sept. 1999).

221. The initial remit of the new Office of Communications ("OFCOM"), established in the Office of Communications Act of 2002, does not include regulation of the Internet. Instead, OFCOM will support and promote the existing mechanisms of tackling illegal materials, in particular working with the IWF. *See* Department of Trade and Industry, *Communications White Paper*, ¶ 6.10, *available at* http://www.communicationswhitepaper.gov.uk/pdf/ch6.pdf (last visited Nov. 25, 2003).

222. Even if the IWF was deemed to be a public authority for the purposes of Section 6 of the Human Rights Act, a constitutional challenge would be harder to sustain given that the IWF's role is largely advisory rather than providing a direct restraint.

223. Cyber-Rights and Cyber-Liberties (UK), *Who Watches the Watchmen: Internet Content Rating Systems, and Privatised Censorship*, http://www.cyber-rights.org/watchmen.htm (Nov. 1997). However, steps have been taken to improve the situation.

judicial function that draws the boundary between illegal and harmful content. A further concern is that, by encouraging systems that go beyond the realm of the illegal material, and seeking to restrict harmful content through the promotion of filters and ratings, the body will step into the realms of censoring legitimate speech in the name of protecting children. Critics have argued that it would be preferable to have political action by a democratically elected and accountable government rather than "random censorship by law enforcement authorities or by self regulatory bodies."[224] A defense can be made that much of the IWF's work concerns child pornography, a subject about which there is an overall consensus and little in the way of legal ambiguity.[225] Furthermore the IWF enjoys the support of the industry in that it helps shield ISPs from potential liability by pointing out the illegal material that should be removed, without the ISPs having to provide resources to monitor and handle complaints.[226]

CONCLUSION

Digital technology crosses borders, and brings with it promises for empowerment and democratization, but in the short history of the Internet, it is also clear that pornography is global. In this Article, we looked at the European approach to the harms caused to children by the easy availability of such material online.

While the problem is not unique to Europe, thus far, European countries have opted for a very different approach than that opted for in the US. While the US attempted, and failed, the direct public-ordering approach—the 1996 CDA and its replacement, COPA—Europe chose a mixed approach of indirect public-ordering and private-ordering. Broadly speaking, this approach better fits Etzioni's analysis than the US approach.

There might be many political, sociological, and other explanations for this difference in approach. By way of conclusion, we wish to propose that the legal environment might be one such explanation: freedom of speech is recognized in Europe and protected, but its structure enables balancing it with other public interests. In light of this approach, the puzzle is even greater: European versions of the US CDA or COPA are far more likely to survive scrutiny in Europe

224. Akdeniz & Strossen, *supra* note 38, at 224.
225. *See* Edwards, *supra* note 14, at 296.
226. *Id.*

than in the US. Nevertheless, this path was not taken. We want to speculate that the reason for the different approaches can be found here: The strong protection that the First Amendment provides in the US does not leave much room for other interests, or balancing rights and interests, and the constitutional clash between freedom of speech and the interest in protecting children from harmful material is inevitable.

In Europe, the initial point is different. It is one of compromise and balancing. This renders the clash between the rival interests and rights less charged, at least on a legal-constitutional level. Once the rival interests are on a par, normatively speaking, there is a more relaxed atmosphere to devise a delicate balance. Private-ordering, which minimizes governmental interference, is such a solution.

However, this is not to say that the issue of protecting children on-line is less important in Europe than it is in the US. The newspapers are full of stories of the dangers to children that lurk on the Internet. In spite of the more relaxed legal environment, the European approach has taken note of the difficulties in US public-ordering and attempts to avoid such conflicts or embarrassments. Imposing direct public-ordering may threaten to create an issue that will polarize competing interest groups and lobbies, and thereby undermine the more balanced approach to expression rights that has been described. Furthermore, the difficulties in defining and enforcing direct public controls provide another deterrent. Regulating with the cooperation of the Internet industry is more likely to be practicably administered and less divisive.

This form of regulation does not come without difficulties. It is unlikely to prevent children from accessing all material deemed harmful. Furthermore, it has the potential to act as censorship, but in a more subtle form. The actions of those deciding what types of material is harmful is less likely to fall foul of the schemes of constitutional protection. The less charged environment in Europe may also permit this type of approach. While fewer groups demand outright prohibition of harmful material, fewer groups also cry foul when such private organizations attempt to act as censors. The approach in Europe may be less divisive and high profile than the legislative attempts in the US, but it nevertheless carries costs.

Justice Louis Brandeis once noted, "[i]t is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and eco-

nomic experiments without risk to the rest of the country."[227] Nowadays, culture, economy, and politics are more global than ever before, the technology of the Internet is borderless, but principles of political morality are still universal, even if their concrete application is local. Europe and the United States can each serve as a laboratory to each other.

227. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932).