THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
VOLUME 7, 2011

RETHINKING ONLINE INTERMEDIARY LIABILITY: IN SEARCH OF THE 'BABY BEAR' APPROACH

Gavin Sutter *

ABSTRACT

This paper examines various national approaches to the regulation of online content. Its particular focus is on the treatment and liability of the intermediary service provider in the context of data provided by third parties. It does this through a survey of the issues involved in the provision of unacceptable content, basing on this even its assessment of why the intermediary should have an appropriate role in the first place. It then moves on to how content can be regulated at this point. The argument this paper makes is that a case-specific approach offers probably the optimum solution; being not too liberal, absolving intermediaries of all responsibility while not being overtly stringent either, thereby overburdening the intermediary. This analysis is contextualised in an exposition on the value of the legal right to the freedom of expression.

TABLE OF CONTENTS

* LL.B., LL.M. Lecturer in Media Law at the Centre for Commercial Law Studies, Queen Mary, University of London. This paper is based on a lecture first delivered at Consilience 2010, a law and technology conference organised by the National Law School of India University, Bangalore.

I. INTRODUCTION

Once upon a time, there was a young lady by the name of Goldilocks, who, as the author is sure the reader will recall from childhood, indulged in what may only be described as an unlawful invasion of the home of the Three Bears, wherein she stole their food, sat in their chairs, and slept (or attempted to sleep) in their beds. Various versions of the tale ascribe differing responses to the bears, who, upon returning home, discover her asleep in one of their beds. Whether these bears would have the right to violently expel the intruder from their own home might be the subject of a very different legal commentary. In this instance, however, it is the behaviour of young Goldilocks herself in which the author is interested. The story informs us that she availed herself of food, seating and finally bedding belonging to each of the Bears in turn. Father Bear's preferences were rather too Spartan for Goldilocks: his porridge too cold, his chair and his bed too hard; Mother Bear's proved to opposite: too hot, too soft. It was only when she moved on to the food and furniture belonging to Baby Bear that Goldilocks discovered options which were Just Right.[1] Various nation States have adopted differing approaches to the difficulty of regulating unacceptable content online, and in particular to the appropriate role(s) to be ascribed to the intermediary online service provider with respect to the control of data provided by third parties. Some States seem to favour a much harsher, more interventionist approach across the board, while others vary in their

[1] For further background to the origins of this folk tale, see *The Story of the Three Bears*, WIKIPEDIA, http://en.wikipedia.org/wiki/Goldilocks.

approach from strict to rather *laissez faire* depending upon the nature of the particular content in question. This paper will first consider the significant issues raised by the availability of unacceptable content (whatever that may be) in the online environment, moving on to discuss why, of all the potential 'targets', intermediary service providers might be considered appropriate parties to involve in regulation. This analysis will have to include not only consideration of what is practical from a utilitarian standpoint, but also what is considered to be 'fair', or at least *appropriate* when taking into account such issues as cost or acceptability within the context of a democratic society which espouses the value of freedom of speech and expression. If the online intermediary can reasonably be viewed as an appropriate point at which to regulate undesirable content, then it must further be considered *how* this is to be achieved. Several different models of regulation at the intermediary level exist. There is also a key policy decision to be made as to whether standard of liability to which the intermediary is held should vary with the nature of the content. In the US, for instance, very different approaches are in place with respect to defamatory content and that which infringes copyright, whereas under the European model an intermediary's liability for third party content is judged against a uniform approach irrespective of the particular nature of the material and why it is unlawful. The paper will ultimately conclude with an outline of what is, in the opinion of the author, the 'Baby Bear' approach to the role of the intermediary with regard to online, unlawful content. That is to say, an argument will be made that a specific approach is as close as is available to the "just right" solution, being neither too liberal, allowing intermediaries to abdicate all responsibility for the content which they make available, nor overly stringent, placing an inappropriate burden upon the intermediary. This will be placed in the context of the perceived value of 'freedom of expression', a right often enshrined in law.

II. DRAMATIS PERSONAE

When considering how best to regulate unacceptable online content, balancing desired regulation with freedom of expression, one must take into

---

2 *See, e.g.*, Section 2, OBSCENE PUBLICATIONS ACT, 1959, "Prohibition of publication of obscene matter". The test of Obscenity is set out in Section 1(1) of the 1959 Act thus:

"For the purposes of this Act an article shall be deemed to be obscene if its effect or (where the article comprises two or more distinct items) the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it." (emphasis author's).

account not only *whom* to regulate, but *why* one wishes to regulate in the first place, or what the aim of regulation and its enforcement is. Clearly, where content has been decreed by the State to be undesirable and therefore banned, it will be desired to punish any person who breaches such content regulation. There may also be other aims behind these laws. For example, UK obscenity law incorporates offences of distribution of content clearly based upon the notion that circulation of such content may be harmful to its audience.[2] In the online environment there will typically be several parties involved in making content available, and it may be that in certain circumstances parties other than the initial source should face some level of liability for their active or passive role in this distribution.

There are three key categories of persons who may be subjected to liability. First, and most obviously, there is the source of the undesirable content. This would be the person who posts a defamatory statement on their blog, or an individual who uploads child pornography, or infringing copies of works protected by copyright. Such a person may often be the main target of regulation as the party who has taken the primary active role in circulating undesirable content. Secondly, there is the recipient of the unlawful information: the end user. Where the nature of the material is such that even mere possession is unlawful, then the audience as well as the source of the material may face legal liability.[3] Thirdly, there is the internet intermediary. It need hardly be stated that without the involvement of an intermediary service provider the unlawful content cannot be distributed online to begin with. The involvement of the service provider may be very low level, such as, for instance, providing internet access which is then used by an individual to communicate unlawful content via email. It may also be that the service provider is more involved, such as where hosting services are provided to someone who proceeds to set up a website on the intermediary's servers, offering unlawful content. Within the category of service provider, the author also includes some of those who run a website such as a discussion forum to which third parties may upload information. The level of editorial responsibility assumed by those responsible for such sites varies greatly. Those who actively edit the material posted to their sites effectively take ownership thereof and would be considered the content provider. Many

---

3 *See, e.g.*, Section 63, CRIMINAL JUSTICE AND IMMIGRATION ACT, 2008 *quod subsequent* on the possession of extreme pornography.

operate by avoiding actively editing content posted, instead responding only to complaints about specific articles. The latter can be viewed as a service provider in a number of different liability schemes, as will be discussed below. The liability faced by the service provider will vary depending upon the potential for control over the content in question and awareness of its existence. As already noted above, some jurisdictions will also vary in approach according to the nature of the unlawful content in question.

Inevitably, choosing the appropriate targets for and modes of online content regulation is not purely a utilitarian decision, but also involves the application of value judgements. These include the concept of 'fairness'. In addition to the basic concept of what is 'just' or 'moral', this might also include a consideration of the economic cost of regulation. Placing certain responsibilities upon an intermediary service provider, for instance, may lead to considerable expenditure in terms of manpower, equipment, perhaps even 'opportunity cost'.[4] It is beyond the scope of this paper to deal in-depth with the question of financial cost of regulation. The author's primary focus here is freedom of expression. Freedom of speech or expression, as will be demonstrated, is a universally recognised value albeit that the appropriate limits thereof are far from being globally agreed upon. Any nation State which enshrines some level of freedom of expression in its laws must ensure that its approach to online content regulation must remain consistent with that value, hence concerns being raised over regulatory models which might 'chill' free speech.

III. UNACCEPTABLE CONTENT & ENFORCEMENT OF NATIONAL LAW

Before exploring further the policy issues of imposing legal liability upon the various parties discussed above, it is important to consider the nature of unacceptable content, and the viability of applying national laws to the online environment. Just what is 'unacceptable content'? Where lie the boundaries in relation to the type of material which may be freely expressed and distributed

---

4 "the loss of other alternatives when one alternative is chosen", *Opportunity Cost*, OXFORD DICTIONARIES, http://oxforddictionaries.com/definition/opportunity+cost (last visited Jul. 9, 2011). In other words, the time which employees of a service provider spend complying with such legal duties is time which they might otherwise have spent improving and developing their services in such a way that might have increased profitability. Such cost is notoriously impossible to estimate accurately.

by individuals or organisations? When one reviews 'freedom of speech' across the globe, it becomes clear that many different cultures and legal systems support the notion that all citizens under their jurisdiction should have some basic right to express themselves, free from interference by the organised State. This is, for example, enshrined in international laws such as Article 10 of the European Convention on Human Rights (incorporated into UK domestic legislation by virtue of the Human Rights Act 1998, in force as of 2002), and Article 19 of the Universal Declaration of Human Rights. On a national level, the First Amendment to the United States Constitution famously provides that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." Seemingly the broadest protection for free expression in any nation State, the First Amendment has been cited to protect the rights of bodies such as the Ku Klux Klan to express their views on race,[5] or NAMBLA (North American Man-Boy Love Association), whose constitutional right to promote their view that paedophilia is simply another sexual preference which should not be prosecuted by the State.[6] The constitutions of the Republic of Ireland and the People's Republic of China also explicitly guarantee the right to freedom of expression for their citizens. These typically extend to the right to express an opinion, the right to peaceable assembly, and so on. Article 41 of the Chinese constitution states "Citizens of the People's Republic of China have the right to criticize and make suggestions to any state organ or functionary..."

---

5 In Brandenburg v. Ohio, 395 U.S. 444 (1969), the US Supreme Court ruled that inflammatory speech by members of the Ku Klux Klan is protected speech under the First Amendment. Protection would only be lost where the speech in question was directed to inciting and likely to incite "imminent lawless action".

6 *See*, for instance, the debate surrounding Curley v. NAMBLA, a wrongful death lawsuit brought against NAMBLA by the parents of a young boy murdered by paedophiles. The suit was based on a claim that the murderers had visited the NAMBLA website and had thus been incited to solicit sex from the boy, and then murder him when he refused. The plaintiffs dropped the action in 2008, when a court ruled that the only witness to the supposed incitement of the murderers by NAMBLA that the plaintiffs were able to produce was not competent to testify. *See Curley Family Drops Case Against NAMBLA*, BOSTON GLOBE, (April 23, 2008), "http://www.boston.com/news/local/breaking_news/2008/04/curley_family_d.html. For the particulars of the original lawsuit, which was first launched in 2000, see *Amended Complaint And Jury Demand in Curleys v. NAMBLA*, THECPAC.COM, http://www.thecpac.com/Curleys-v-NAMBLA.html. Without sufficient proof of intent and likelihood of inciting "imminent lawless action", the First Amendment applies to NAMBLA's website, per Brandenbrg v. Ohio, 395 U.S. 444 (1969). *See supra* note 3.

'Censorship' is not a term of which States tend to be fond. It conjures up images of morally illegitimate controls upon an individual's right to express or access certain types of information, an Orwellian approach to control. If the average person – Greer LJ's "man on the Clapham omnibus"[7] – were to be asked what he thought of 'censorship', no doubt he would respond negatively towards the concept. Yet pose the question another way – 'Should individuals have the right to exchange pornographic images featuring children?', for instance, and the response will undoubtedly be very different. All key provisions on freedom of expression, including those to which reference is made above, are in some way limited or qualified. The European Convention on Human Rights clarifies that:

> The exercise of these freedoms, since they carry with them 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 the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.[8]

Clearly this will stretch to include a very wide range of material, including hate speech,[9] obscene materials,[10] defamatory material, or material which is in breach of privacy or is likely to prejudice the outcome of a trial.[11] Article 30 of

---

7 Hall v. Brooklands Auto-Racing Club, (1933) 1 K.B. 205.

8 *See* Article 10(2) of the European Convention on Human Rights.

9 *See, e.g.* , Section 17-29, UK PUBLIC ORDER ACT, 1986, and the RACIAL AND RELIGIOUS HATRED ACT, 2006, which set out the criminal offences of incitement to racial hatred and incitement to religious hatred. *See also* Section 74, CRIMINAL JUSTICE & IMMIGRATION ACT, 2008, on incitement to hatred on grounds of sexuality. These speech and expression-based offences clearly fall within the ambit of Article 10(2)'s legitimate grounds for the limitation of free speech. *See also* D.I. v. Germany, Case No. 26551/95, ECommHR, (26 June 1996), in which it was held that German laws forbidding Holocaust denial were a legitimate Article 10(2) restriction. This conclusion was reached on the basis that to deny the occurrence of that historical event was contrary to the principles of peace and justice in the Convention preamble, and advocated racial and religious discrimination. Further, per Article 17 the free expression right can be lost where the aim is using it is to deny or limit the availability of Convention rights to others.

10 The test of obscenity in English law is whether the article in question will have "a tendency to deprave and corrupt" a substantial proportion of its likely audience, and is thus clearly rooted in the concept of the protection of morals. (*See* Section 1, OBSCENE PUBLICATIONS ACT, 1959).

the Universal Declaration of Human Rights makes clear that none of the fundamental freedoms set forth in the Declaration may be construed in such a way as to permit anything "aimed at the destruction of any of the rights and freedoms set forth herein." Thus free expression is limited where that would, for instance, violate the right to a fair trial,[12] or the right to privacy.[13] Among free speech provisions at the level of the nation State, even the mighty First Amendment to the US Constitution has its limits. Obscene materials,[14] libel and slander, and activities amounting to "falsely shouting fire in a crowded theater [*sic*]"[15] all fall without the bounds of the protection afforded speech and expression by the First Amendment. There is also no First Amendment right to use profane language in a broadcast.[16] Similarly, *Bunreacht Na Héireann*, the constitution of the Republic of Ireland, places certain limitations upon free speech. Article 40(6)(1) makes clear that:

> The education of public opinion being, however, a matter of such grave import to the common good, the State shall endeavour to ensure that organs of public opinion, such as the radio, the press, the cinema, while preserving their rightful liberty of expression, including criticism of Government policy, shall not be used to undermine public order or morality or the authority of the State.

---

11 Thus the restrictions placed by the UK Contempt of Court Act 1981 upon media reports of a criminal case prior to the issue of a verdict by the court.

12 *See* Article 10 of the UN Universal Declaration of Human Rights.

13 *See* Article 12 of the UN Universal Declaration of Human Rights .

14 For the classic definition of what constitutes obscenity for the purposes of US law, *see* Miller v. California, 413 U.S. 15 (1973).

15 "The most stringent protection of free speech would not protect a man falsely shouting fire in a theater and causing a panic. [...] The question in every case is whether the words used are used in such circumstances and are of such a nature as to create a clear and present danger that they will bring about the substantive evils that Congress has a right to prevent." Per US Supreme Court J. Oliver Wendell Holmes Jr. in Schenck v. United States, 249 US 47 (1919), in which the Court upheld the Espionage Act of 1917, concluding that a defendant was not protected by the First Amendment when distributing a pamphlet opposing conscription of US citizens into the US Army upon the state's entry into the First World War in 1917. This ruling was later overturned by the Supreme Court in Brandenburg v. Ohio, 395 US 444 (1969), in which the court concluded that only inflammatory speech which would incite "imminent lawless action" (such as a riot, for example) would be in breach of the First Amendment, as opposed to merely advocating behaviour counter to the law. Nonetheless, Holmes' statement survives in popular discourse as a term understood to mean that the speaker has knowingly expressed him or herself in a manner which is beyond the bounds of expression protected by the First Amendment.

16 Federal Communications Commission v. Pacifica Foundation, 438 U.S. 726 (1978).

Of interest here is the fact that the Article goes on to make clear that:

> The publication or utterance of blasphemous, seditious, or indecent matter is an offence which shall be punishable in accordance with law.

This might possibly include some material that the Strasbourg Court may interpret as being legitimate expression under Article 10 of the European Convention on Human Rights, a document to which the Republic of Ireland is a signatory State. The underlying value judgements implicit in such provisions should not go ignored. *Bunreacht Na Héireann* strongly bears the hallmarks of Eamon De Valera, the (then still technically) self-proclaimed President of the Republic of Ireland.[17] De Valera deputised the drafting to others, but he personally supervised their work, and woven throughout the 1937 provisions was a clear reflection of his own devout Roman Catholicism. The Constitution explicitly forbade the establishment of a State religion, and guaranteed the religious freedom of all citizens. Nonetheless, divorce (until 1997) and sale of contraceptives (until reforms begun in the 1970s), were prohibited by the 1937 Constitution. Other Roman Catholic values enshrined in the Constitution remain to the present, not least Ireland's traditionally strict censorship laws, which tend to reflect traditional Catholic morality. This is of note as the Irish Constitution provides us with a clear example of how localised values can effect the perception of where the limits of freedom of expression may reasonably be drawn. Local social and political culture is clearly at work in the Constitution of the People's Republic of China, which emphasises the need to limit free expression in order to protect the security of the State:

> "The State maintains public order and suppresses treasonable and other criminal activities that endanger State security; it penalizes actions that endanger public security and disrupt the socialist economy and other criminal activities,..."[18]

---

[17] Some confusion inevitably exists in the terminology, as while de Valera was among those who proclaimed the establishment of the Republic of Ireland as early as during the Easter Rising of 1916, the Republic of Ireland as a state fully independent of Britain was not recognised by Westminster until the passage of the Republic of Ireland Act, 1948. Nevertheless, it can be stated in summary that the Irish Free State created by the Anglo Irish Treaty signed on 6th December 1921 was a *de facto* Republic for all practical, day to day purposes. Following several terms in government as Taoiseach, he was eventually elected President in 1959, serving in that capacity until his retirement from public office in 1973.

[18] Article 28 of the Constitution of the People's Republic of China.

> "No organization or individual may, on any ground, infringe upon the freedom and privacy of citizens' correspondence except in cases where, to meet the needs of State security or of investigation into criminal offences, public security or procuratorial organs are permitted to censor correspondence in accordance with procedures prescribed by law."[19]

It is clear that the Chinese State authorities feel that forms of political dissent which oppose the State and its system of government are inappropriate and should be prevented: see, for instance, the closure of Tiananmen Square on the occasion of the twentieth anniversary of the 1989 pro-democracy protests, which were forcibly broken up by the Chinese military. In the USA, or even the UK, for instance, where political culture is very different, this would not be considered to be a reasonable limitation upon citizens.

Thus, there exists a very wide range of what the author has termed 'unacceptable material'. This may include, for example, political speech. This might incorporate laws restricting holocaust denial, as are in place in France and Germany.[20] China, among others, as we have seen restricts political speech which would criticize the State, or pose a threat to "national security". Sexual expression is commonly restricted. Some States, such as Saudi Arabia, forbid pornography altogether; others, such as the UK permit a certain level of pornographic material, with only certain extreme forms being illegal to distribute or even, in relation to limited categories of material, to possess. Child pornography, or perhaps more properly 'child sexual abuse images',[21] are illegal in every nation State of which the author is aware. The freedom of speech or expression which has the effect of defaming a living individual is generally

---

19 Article 40 of the Constitution of the People's Republic of China.

20 Such provisions have been declared by the Strasbourg court to be a legitimate Article 10(2) restriction upon the free expression right – *See supra* note 4.

21 The UK based Internet Watch Foundation has this to say on the matter of labelling paedophile material:

> "Please note that 'child pornography', 'child porn' and 'kiddie porn' are not acceptable terms. The use of such language acts to legitimise images which are not pornography, rather, they are permanent records of children being sexually abused and as such should be referred to as child sexual abuse images".

See Disclaimer/Note used by Internet Watch Foundation on its Website, IWF.ORG.UK, http://www.iwf.org.uk/public/page.103.htm (last visited May 21, 2010).

restricted. Certain forms of commercial speech are also subject to limitations, for example the regulation of advertisements, or the restriction of certain products such as Viagra, or Valium, is common. All of these are considered by those States which impose such regulation to be legitimate limitations upon free speech and expression which is not therefore an unfettered right. Problems arise when applying such regulation to the internet. Computer technology and the internet as we know it today, most particularly the World Wide Web with its hypertext linking as devised by Sir Tim Berners Lee at the turn of the 1990s, presents many challenges to regulation. Matters technical can often be addressed by straightforward adaptation or even amendment to a pre-existing legal provision. Thus, the UK Defamation Act 1996 placed upon a statutory footing the old English common law defence of innocent dissemination, ensuring in the process that the defence covered internet service providers.[22] When the Crown Prosecution Service encountered difficulties with defendants charged with offences relating to child pornography exploiting a lacuna in English law which meant that an image of an adult, digitally altered to appear to be a child to a degree that it was indistinguishable from a real image of an actual child, was not an offence,[23] this was simply addressed by the creation of the concept of 'pseudo-photographs'.[24] The real difficulty lies not in creating a law which will apply to online technology, but rather in *enforcement* of any such law. The internet is a global entity which neither recognises nor respects national boundaries; material made available online by uploading it in one jurisdiction is automatically available globally, whether legal there or not. In the early 1990s, a popular school of thought insisted that the web was a 'new' space, its own jurisdiction, which should – and, indeed, *would* – be subject to no national laws.[25] This has come to be known as 'the Cyberspace Fallacy'.[26] The reality is that cyberspace, the internet, is the most overregulated space there is, with each and every State

---

22 For the application of Section 1 to an ISP, see Godfrey v. Demon, [1999] E.M.L.R. 542.

23 Prosecutors believed that many of the images claimed to be merely digitally altered pictures of adults were in fact genuine images of children, but proving this to be so presented a major difficulty, leading to the belief that many defendants were able to escape charges of which they were actually guilty.

24 *See* Section 1, PROTECTION OF CHILDREN ACT, 1978 as amended by the CRIMINAL JUSTICE AND PUBLIC ORDER ACT, 1994.

25 *See, e.g.* , John Perry Barlow, A *Declaration of the Independence of Cyberspace*, EFF.ORG, https://projects.eff.org/~barlow/Declaration-Final.html (last visited May 21, 2010).

26 *See, e.g.*, C. Reed, INTERNET LAW ¶ 7.1.1 (Cambridge University Press, 2nd edn. 2004).

clamouring to apply its laws and cultural standards in that context. This is, inevitably, further complicated by the fact that so often these competing laws are wholly contradictory. For instance, in mid 2000, Yahoo Inc became embroiled in legal action in France over material hosted on their servers in California. French law has express provisions forbidding the trade in Holocaust denial material and certain Nazi-related items and paraphernalia. Such material was advertised for sale on Yahoo Inc.'s auction website. The material was uploaded and hosted in the USA, where it was not unlawful, but, due to the nature of the internet, available to be viewed within France, where it was. The French court ordered Yahoo to take steps to block this content from availability to internet users in France.[27] Yahoo petitioned a US court, and were granted a guarantee that the French decision would not be enforceable in the US as such restrictions upon speech would be in violation of the First Amendment.[28] Thus, stalemate. There followed two decisions from the US Court of Appeal for the Ninth Circuit. In the first, overruling the first instance judgement, delivered in August 2004, the Court found that as the French court had sought only to deal with transactions taking place within France and had not sought to enforce the judgement within the USA, Yahoo could properly be subject to French jurisdiction over the issue.[29] In the following February, however, the Ninth Circuit Court of Appeals announced that this judgement was no longer to be regarded as a precedent to be followed, and reopened the case. The decision which followed found that, on the basis of a number of technicalities, US courts could indeed exercise jurisdiction over the incident.[30] The first instance granting of an order stating that the French ruling would not be applicable in the US was still overturned on the basis that no attempt had been made to do any such thing. Nonetheless, this was clearly a political decision which lays down a marker to the effect that the US courts will resist the enforcement of foreign judgements over US based web content. It does not seem unreasonable to surmise that the

---

27 La Ligue Contre le Racisme et l'Antisemitisme v. Yahoo! Inc Tribunal de Grande Instance de Paris, May 2000 (France).

28 Yahoo! Inc v. La Ligue Contre le Racisme et l'Antisemitisme US District Court Northern District of California, San Jose Division Case No: C-00-21275 JF November 2001 (USA).

29 Yahoo! Inc v. La Ligue Contre le Racisme et l'Antisemitisme, 379 F3d 1120 (9th Ct, August 23, 2004).

30 Yahoo v. La Ligue Contre le Racisme et l'Antisemitisme, 399 F3d 1010 (9th Ct, February 10, 2005).

Supreme Court's subsequent decision to decline to hear the case represents a tacit approval of this position.

Such problems occur also in relation to child pornography. It would seem, *prima facie*, that this is a universally reviled form of content, and indeed there appears to be not one single example of a nation State which permits the trade in images of children being sexually abused. Nonetheless, even here we have a problem. On a very fundamental level, there is no agreement as to exactly what constitutes a 'child'. Despite some vast differences in the age of consent, it is now fairly common in many countries that for the purposes of pornographic images, the person depicted must be aged eighteen or over. In the UK, a person of the age of sixteen or over can consent to sexual activity, though for the purposes of the distribution of indecent photographs, an individual is considered a child up to the age of eighteen.[31] Under Articles 176 and 177 of the Japanese Penal Code, the national age of consent in Japan is just thirteen, but under the Law for Punishing Acts Related to Child Prostitution and Child Pornography, and for Protecting Children 1999, a 'child', for the purposes of the offences relating to the distribution of child pornography,[32] is "a person under the age of eighteen years".[33] Since July 3, 1995, all producers of pornographic content in the USA have been required to guarantee that the performers appearing in their work are all aged eighteen or over.[34] Countries in which no concept of an age of consent exists, such as Oman, tend also to be those in which pornography will be illegal both under obscenity laws, and by default as in Oman sexual intercourse cannot lawfully take place outside of marriage.[35] As ever, the devil is in the details. While there may be some agreement internationally about the age at which minors become adult in relation to the pornography industry, the concept of what exactly constitutes an image of a child remains far from consistent across international boundaries. In the UK, for instance, 'child

---

31 *See* Section 1, PROTECTION OF CHILDREN ACT, 1978, as amended by the SEXUAL OFFENCES ACT, 2003.

32 Article 7, LAW FOR PUNISHING ACTS RELATED TO CHILD PROSTITUTION AND CHILD PORNOGRAPHY, AND FOR PROTECTING CHILDREN, 1998.

33 Article 2, LAW FOR PUNISHING ACTS RELATED TO CHILD PROSTITUTION AND CHILD PORNOGRAPHY, AND FOR PROTECTING CHILDREN, 1998.

34 18 U.S.C. 2257.

35 *See Legislation of INTERPOL Member States on Sexual Offences Against Children*, INTERPOL.INT, http://www.interpol.int/Public/Children/SexualAbuse/NationalLaws/.

pornography' includes not only images of actual sexual abuse of children, but also, as noted above, digitised images which appear to be realistic depictions of actual children.[36] It is an offence not only to distribute such material or to possess with intent to distribute, but even merely to possess for an individual's own private use. In 2009, the UK took this one step further with the creation of several possession offences relating to certain types of images of children which are not the sort of adapted images that the provisions relating to 'pseudo-photographs' entail, but are in fact wholly fabricated.[37] The scope of the new offence includes material which depicts sexual acts "with or in the presence of a child", and which include interaction with either other humans or "an animal (whether dead, alive or imaginary)".[38] There is no requirement that these be realistic images, though it can reasonably be presumed that prosecutions will be more likely to be pursued against CGI type material, or even some types of Japanese *Hentai*,[39] rather than very basic stick-figure drawings. Such laws are by no means global. The Japanese Law for Punishing Acts Related to Child Prostitution and Child Pornography, and for Protecting Children as passed in 1998 referred only to offences relating to distribution and possession with intent to distribute;[40] this law was, however, updated in 2003 to include a mere possession offence. By 2010, however, Japanese law still places no restrictions upon simulated or cartoon pornography involving minors. The USA has adopted a position somewhere in the middle. Since 1978, the Washington Supreme Court has backed the constitutionality of a ban on child pornography. While it is speech within the meaning of the First Amendment, the court has ruled, it may be banned as not only are children inevitably abused during its production, but it also provides a permanent record of that abuse which causes ongoing psychological harm to the victims.[41] This decision applied only to 'real'

---

36 *See* Treatment of 'pseudo-photographs' in Section 1, PROTECTION OF CHILDREN ACT, 1978, as amended by the CRIMINAL JUSTICE AND PUBLIC ORDER ACT, 1994.

37 Section 62, CORONERS & JUSTICE ACT, 2009.

38 Section 62, CORONERS & JUSTICE ACT, 2009.

39 'Hentai' is a form of Japanese Manga comic, or anime film, which concentrates upon the depiction of sexual activity. Often this can feature characters who appear to be minors, for instance young females in school uniforms or similar. The subgenre of hentai which focuses upon sexual activity involving minors is known as 'lolicon'.

40 Article 7, LAW FOR PUNISHING ACTS RELATED TO CHILD PROSTITUTION AND CHILD PORNOGRAPHY, AND FOR PROTECTING CHILDREN, 1998.

41 New York v. Ferber, 458 U.S. 761 (1978); Osborne v. Ohio, 495 U.S. 103 (1990) extended this logic to permit the criminalisation of simple possession of child pornography.

child pornography, however. The Child Pornography Prevention Act attempted to introduce into US law the concept of pseudo images of child pornography, and required that they be treated as equivalent to actual images. This was, however, struck down by the courts. In 1999, a Ninth Circuit Court ruled that these provisions violated the First Amendment on the basis that no actual children were harmed in their production, and that:

> "Any victimisation of children that may arise from paedophiles' sexual responses to pornography apparently depicting children engaged in explicit sexual activity is not a sufficiently compelling justification for the CPPA's speech restrictions."[42]

In 2002 the Washington Supreme Court reached the same conclusion.[43] Congress responded with the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today ('PROTECT') Act 2003, which criminalised such images if, and only if, they would qualify as being obscene (and therefore fall without the ambit of First Amendment speech) without there being a child depicted in the image.

With respect to simple possession of actual child pornography offences, the UK, Japan and the US all criminalise such activity, but this too is not universal. Of the 94 Interpol countries which had laws specifically addressing child pornography[44] by 2008, only 58 made it an offence merely to possess without intention to distribute.[45]

Clearly, then, even in an area of criminal law relating to a form of content seemingly universally regarded as 'unacceptable', it is possible for national laws to vary greatly, to the point where online content uploaded within one jurisdiction might be perfectly legal, yet, due to being internationally available the same content will almost inevitably be available in a jurisdiction where it is

---

42 Free Speech Coalition v. Reno, 198 F. 3d. 1083, 1102 (CA9 1999).

43 Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002).

44 This figure does not include those countries which outlaw child pornography under more general obscenity provisions, only those which have specific child pornography laws.

45 *See* International Centre for Missing and Exploited Children, *Child Pornography: Model Legislation & Global Review* (5th Edn. 2008), http://www.missingkids.com/en_US/documents/CP_Legislation_Report.pdf.

wholly illegal. So what happens when a State discovers that unlawful material has been distributed into its jurisdiction via the internet and wishes to trace and prosecute the source? It is entirely possible that the State in which the culprit is based will refuse to extradite him or her on the basis that no crime has been committed as far as that State is concerned. Thus, the business of enforcement becomes a difficult one indeed. This is, of course, assuming that the source of the unacceptable material can in fact be traced. For those really determined, it is technically possible to make it at least very difficult, if not outright impossible, to trace them as the source of the material uploaded. Software and instructions on how to do this are readily available: a simple Google search run by the author took only 0.27 seconds to return well over 400,000 results for "hiding ip address". Such tools are always marketed as for the purposes of protecting individual privacy, though of course they cannot detect whether that privacy is being abused for criminal purposes.

In relation to civil law, the situation may be somewhat simpler. For example, the UK is a signatory State to the Brussels Regulation 2002, which provides that where claimant and defendant are located in two different EU Member States, the claimant has a choice of jurisdiction in which to bring an action. Either he may sue the defendant in the jurisdiction in which the latter is domiciled in respect of all damage occasioned, or alternatively in each individual jurisdiction in which there has been damage but then only for the damage caused within that jurisdiction. The English courts have most notably applied this to libel, permitting an English student to sue a French newspaper within England in respect of the small number of copies of the defamatory article which were circulated in England.[46] Where the defamatory publication originates without the UK, English law similarly makes provision for identifying whether a case may be brought in the English courts: this will fall to be decided under the traditional rules of Private International Law. First, there must be a publication within the jurisdiction. Online publication, consistent with the very oldest cases on publication[47] is construed as having taken place at the

---

46 Shevill v. Press Alliance, SA [1995] ECR 1-415; note that this case was decided under the Brussels Convention of 1996, now superseded by the Brussels Regulation 2002. This change would have no significant practical impact upon the outcome of a case with the same facts today as the relevant provisions here are repeated unchanged in the Regulation.

47 *See, e.g.*, Jones v. Davers, (1596) Cro Eliz 496, Price v. Jenkings, (1601) Cro Eliz 865, in which letters written in French were held not to have been published by delivery to a third party who understood no French and therefore did not gain any knowledge of the defamatory allegations contained therein.

point in time and location at which the defamatory article becomes available to a third party in an intelligible form. In other words, it has only been published once it has been downloaded to an individual's browser and is capable of being read.[48] As the court in *Jameel* v. *Dow Jones*[49] was at pains to point out, while English defamation law has no *de minimus* requirement for publication beyond that it must be to at least one third party, the courts will not allow a case to be heard where publication is so limited as that for the case to be allowed to go ahead would constitute an abuse of process. In Jameel the case was thrown out on this specific ground, as on the facts it was established that of the five persons who could be shown to have viewed the article in question, only two were considered 'live' publications, the others being Jameel and his lawyers. In addition to the publication issue, the courts have also been clear that there must be a 'sufficient connection' between the claimant and the jurisdiction.[50] This 'sufficient connection' has been found, for example, where a Russian businessman showed that he had both personal and business connections in the UK going back some years, and had spent a fair degree of time in England over that period.[51]

So, it would seem that at least in relation to defamation, and certain other areas of civil law, it is simply a matter of determining the appropriate jurisdiction and the case may proceed. However, here again the State will run into potential enforcement problems. If the Defendant has no assets in the country against which any judgement may be enforced, and none in any friendly jurisdiction which might agree to enforce the court's decision, it might well be that nothing can be done.[52] This is a particularly significant issue for the courts in London,

---

48 Harrods v. Dow Jones, [2003] E.W.H.C. 1162; the court here took notice of this line of reasoning in the prior Australian case of Gutnick v. Dow Jones, [2002] H.C.A. 56.

49 Jameel v. Dow Jones [2005] E.W.C.A. Civ. 75.

50 *See, e.g.* , Berezovsky v. Michaels, [2000] 1 W.L.R. 1004; Don King v. Lennox Lewis, [2004] E.W.C.A. Civ. 1329.

51 Berezovsky v. Michaels, [2000] 1 W.L.R. 1004.

52 At least short of arresting and trying defendants who happen to set foot in the jurisdiction, or in another jurisdiction from which they may be extradited. Timothy Koogle, an ex CEO of Yahoo Inc voluntarily travelled to France to face criminal charges in a Paris court in relation to the *LICRA* v. *Yahoo* case discussed above. Koogle, who might, the author is tempted to speculate, have been less willing to comply with a request to appear before the French court had he been in danger of being imprisoned as opposed to facing a relatively small fine, was in February 2003 found not guilty on grounds of lacking the requisite *mens rea* for the crime, *French court acquits Yahoo! of criminal charges for Nazi sales*, OUT-LAW.COM, http://www.out-law.com/page-3319 (last visited May 21, 2010).

England having developed a well-deserved reputation as being much more libel claimant friendly than many other jurisdictions, especially the USA, leading to a fair level of what has been termed 'libel tourism'. In *Mahfouz* v. *Ehrenfeld*,[53] Eady J. gave judgement for the claimant, whom the Defendant author had accused in her book *Funding Evil* of being involved in funding international terrorism. Eady J. permitted the case to be heard in England, despite the fact that the book had never been officially published in England, on the basis of twenty-three copies having been bought by persons resident in England from a popular online retailer, and the fact that the first chapter of the book had been freely available on the ABC News website. The defence did not help their case by initially indicating that they would enter a plea of justification, then later in refusing to do so. In fact, Ehrenfeld had chosen not to defend the action at all, instead counter-suing in the US, where she effectively asked the courts to rule that the English decision would not be enforced in the US as it violated her First Amendment rights. The New York Court of Appeals ruled that that State's long arm rules would not apply to Bin Mahfouz, he having transacted no business in the State of New York. However, were he to take a case to enforce the English decision within New York State, the ongoing relationship between local legal representation and Mahfouz would be sufficient to give the State personal jurisdiction over him. His case would then have to be established on its merits under the much more Defendant-friendly local libel laws, and would be prone to fail.[54] Since this decision, the State of New York legislature has passed into law the Libel Terrorism Protection Act 2008, which purports to grant a New York court jurisdiction over any person who obtains a foreign libel judgement against a New York author or publisher, and limits enforceability to only those judgements that meet US standards of freedom of speech. That, however ridiculous it may be in the eyes of the author, this State legislation employs such an emotive term as "terrorism" in the post-9/11 world (and in New York, of all places), might be interpreted as a clear statement of the revulsion with which English libel laws are viewed by the elected representative of New York State. Or, perhaps more charitably, it might be considered to be demonstrative of the value placed by those persons on the First Amendment

---

[53] Mahfouz v. Ehrenfeld [2005] E.W.H.C. 1156 (Q.B.).

[54] Ehrenfeld v. Mahfouz, N.Y. Court of Appeals (decided Dec. 20, 2007), NYCOURTS.GOV, http://www.nycourts.gov/ctapps/decisions/dec07/174opn07.pdf (last visited May 21, 2010).

right that a potential violation of the same would be equated to terrorism. An equivalent legislative provision was passed at the federal level as the SPEECH (Securing the Protection of our Enduring and Established Constitutional Heritage) Act 2010. The practical effect of this legislation cannot be more than negligible at best, bearing in mind that the US courts were highly unlikely in any case to enforce a foreign libel judgment that would violate the First Amendment. The only reasonable conclusion to be drawn from the passage of this Act, it is submitted, is that it was intended as a message to US-based libel tourists who thought they might take a case for online libel in a more claimant-friendly jurisdiction and then attempt to enforce it in the US.

IV. ALTERNATIVE POINT OF REGULATION: THE END USER

Often, then, going after the source of unlawful content may well be impractical at best; at worst, an extreme case might result in intergovernmental disputes and economic sanctions. One response to this situation has been to instead focus upon the end user, the audience for unlawful content. Thus, in the UK, increasing use has been made of already extant possession offences in relation to child pornography, while the courts have also proffered creative interpretations of the law on *making* such images of children so as to include the simple act of printing out pictures, or even merely downloading the material in the UK.[55] Other forms of unacceptable content in respect of which new possession offences have been created in the UK include "extreme pornography", images which can "reasonably be assumed to have been produced solely or principally for the purpose of sexual arousal" and which fall into one or more of three distinct, narrow categories - serious, non-consensual violence in a sexual context, bestiality, and necrophilia.[56] Such offences reflect the concern (as yet unproven to a conclusive degree) that such extreme material can have a causative effect, in other words, that the audience will be incited to mimic the behaviours depicted. The problem with this as a solution is twofold. First, it only makes sense with a comparatively narrow range of unacceptable content. It is easy to imagine it working logically in respect of possession of certain obscene materials,

---

55 R. v. Bowden, [2001] 88 (Q.B.).

56 Sections 63-66, CRIMINAL JUSTICE AND IMMIGRATION ACT 2008.

politically unacceptable material (which may be Holocaust denial or counter-government information, depending upon the State in question), however it would be patently absurd in relation to, say, defamatory publications. In case of a libel published online, the very nature of the unlawfulness is that the average reader or viewer can be presumed to have no awareness that the statement presented to them is false. Contrast this to someone who knowingly downloads extreme pornography, and the gulf between the two situations is readily apparent. This is clearly not a solution that could be applied across the board. The second, and perhaps more significant, problem is the sheer volume of cases which, it seems, may result. In February 2006, for instance, it was widely reported that in the UK alone there were 35,000 hits looking for pages identified by the IWF as containing images of child pornography *per day*. This claim was widely and uncritically reported with varying degrees of sensationalism by a whole range of news outlets, from the venerable BBC,[57] to *The Independant*,[58] *The Times*,[59] and, of course, *The Daily Mail*[60] and *The Sun*.[61] There were, of course, those on the fringes of the media who expressed doubt about the veracity of such figures, pointing out that the reports of these figures in the press made no allowance for the fact that each individual 'hit' on a webpage relates only to a single piece of information on that page: a content-heavy page such as one mainly displaying photographs could account for up to one hundred hits on a single access or attempted access. The tone of the reports in *The Sun* et al., said these critics, tended to suggest that each of these hits came from a unique user, rather than a smaller number of users looking at rather more content as is more likely to have been the case.[62] The real figure may actually be much smaller, as even BT itself

---

57 *BT sounds child web porn warning*, BBC ONLINE (February 7, 2006), http://news.bbc.co.uk/1/hi/uk/4687904.stm.

58 *35,000 attempts to access child porn blocked every day*, THE INDEPENDENT (February 7, 2006), http://www.independent.co.uk/news/uk/crime/35000-attempts-to-access-child-porn-blocked-every-day-465859.html.

59 *BT Concern as Child porn traffic spirals*, THE TIMES (February 7, 2006), http://business.timesonline.co.uk/tol/business/industry_sectors/telecoms/article728029.ece.

60 *35,000 attempts every day to access child porn sites*, THE DAILY MAIL (February 7, 2006), http://www.dailymail.co.uk/news/article-376408/35-000-attempts-day-access-child-porn-sites.html.

61 *Web child porn outrage*, THE SUN (February 7, 2006), http://www.thesun.co.uk/sol/homepage/news/article37067.ece.

62 *See, e.g.* , Kieran McCarthy's blog, KIERENMCCARTHY.CO.UK, http://kierenmccarthy.co.uk/2006/02/07/twisting-the-facts-to-fit-the-story-child-porn-nonsense/ (last visited May 21, 2010); Doubts were also expressed by The Register, *See* Tim Richardson, *ISPA seeks analysis of BT's 'Cleanfeed' stats*, THE REGISTER, (July 21, 2004),http://www.theregister.co.uk/2004/07/21/ispa_bt_cleanfeed/ (last visited May 21, 2010).

acknowledged in an official statement, which said that the reported figures could give "no indication of the intent behind an access attempt so any claim to identify the number of people from the number of blocked visits is pure speculation."[63] Nonetheless, it would not take an *enormous* number of cases to present a significant difficulty for the court system to process. It may also be considered that going after the end user, rather than a party in a position to control the distribution of unacceptable content, is merely targeting a hydra head: unless the distribution of the content in question can be stemmed, the State will never be able to successfully eradicate it. The other problem with a regulatory approach focussed solely upon the end user is that, of course, by the time a prosecutable offence has been committed, the material has already reached an audience. This could be argued to be rather too late for the State if the primary concern, the reason why the particular content is unacceptable to begin with, is the perceived harm that it may do to the viewer (in the case of sexually explicit material) or other parties (for example, persons whose identity is to be protected by law or even where public knowledge of the material is considered damaging to the government, such as State secrets).

V. BRINGING IN THE MIDDLE MAN

So, it would seem that by process of elimination we arrive at the conclusion that the intermediary needs to play a role in order to efficiently act against unacceptable and unlawful internet content. This is not to say that, where prosecution might be possible, the State should decline to target the source of unacceptable content, nor (if appropriate) the end user. It certainly does, however begin to seem that from a purely utilitarian, efficiency-based point of view, the logical approach is to take advantage of an intermediary who is in the position to have some level of control over whether certain content is made available. Of course, legitimate concerns may be raised that the intermediary should not be made unfairly liable for content originating from third parties, nor be unfairly burdened with the economic costs of enforcing regulation over third party content on their servers. There exists a general, international consensus that intermediaries should not be strictly liable for third party material which is made available via their services.[64] In Europe, as well as beyond, the

---

63 *Supra* note 62.

64 *See, generally*, C. Reed, INTERNET LAW (Cambridge University Press, 2nd edn. 2004).

focus seems to have been primarily upon this matter of ensuring that liability does not unfairly accrue. The author would suggest, however, that it is high time that this should be balanced by an equal focus upon when it is indeed legitimate to hold intermediaries to account for the content distribution that they facilitate, and to consider how they might be involved in the process of enforcing restriction upon unacceptable content.

A. Regulating at the intermediary service provider level: 'Just Right'?

So, then, can we say that the regulation of unacceptable content online is simply a matter of recruiting the intermediary and consider the Baby Bear approach, the ideal means of regulating online content, identified? Alas, no. There still remains a whole spectrum of options of varying levels of State intervention, from full-on State control of the intermediaries, requiring them to censor at that level, to a much more *laissez-faire* approach emphasising industry self-regulation. The exact approach to be taken by the State, harsh interventionism, or something much softer, remains to be determined. Further, a State must also decide whether to impose differing liability regimes designed to best reflect individual categories of content, or a uniform approach which does not concern itself with the specific type of unlawful material, but instead focuses upon the intermediary's relationship to that content and whether there existed a sufficient level of awareness for liability for its distribution to arise. Many States, vary in approach, taking a more interventionist line in relation to some unlawful material than others. This can, and often does, reflect murkier political reality. In the US, for instance, a much more liberal regime is in place with regards to intermediaries distributing libellous content uploaded by third parties than provided in relation to copyright works. Rather inevitably, this reflects the lobbying power of the entertainment industry in the US, bearing in mind especially how liberal content laws can otherwise be there, typically rooted in a First Amendment justification. The European position regarding intermediary liability for third party content specifically provides one common approach common to all flavours of unlawful material, the only variance being that in relation to civil cases for damages, the standard of awareness for liability is lower, including both actual *and* constructive knowledge.[65] This, of course, recognises the differing burdens of proof applied in criminal (beyond all reasonable doubt) and civil (balance of probabilities) actions.

---

[65] *See* Article 14, Electronic Commerce Directive (Directive 2000/31/EC).

B. Father Bear: the Strict Paternalist

The People's Republic of China is commonly accused by Western nations of having adopted the most stringent level of online censorship. As has already been discussed, while the Chinese Constitution promotes freedom of expression, it also requires that there be certain restrictions thereon, most particularly in relation to political criticism of the State and its model of government. To this end, a wide range of strategies have been adopted, all of which entail the intermediary performing an editorial role, in effect acting as an agent of the State to remove the availability of unacceptable material whether arising from within or without China. Section 5 of the Computer Information Network and Internet Security, Protection and Management Regulations 1997 states:

"No unit or individual may use the Internet to create, replicate, retrieve, or transmit the following kinds of information:

1. Inciting to resist or breaking the Constitution or laws or the implementation of administrative regulations;
2. Inciting to overthrow the government or the socialist system;
3. Inciting division of the country, harming national unification;
4. Inciting hatred or discrimination among nationalities or harming the unity of the nationalities;
5. Making falsehoods or distorting the truth, spreading rumours, destroying the order of society;
6. Promoting feudal superstitions, sexually suggestive material, gambling, violence, murder;
7. Terrorism or inciting others to criminal activity; openly insulting other people or distorting the truth to slander people;
8. Injuring the reputation of state organs;
9. Other activities against the Constitution, laws or administrative regulations."[66]

---

[66] *See* Jason P. Abbott, THE POLITICAL ECONOMY OF THE INTERNET IN ASIA AND THE PACIFIC DIGITAL DIVIDES, ECONOMIC COMPETITIVENESS, AND SECURITY CHALLENGES (New York 2004).

This list includes a range of varieties of 'unacceptable content', although it is the political censorship that has received most attention from the international community. The PRC State Council Order Number 292 of September 2000 introduced further restrictions, forbidding websites based within China from hyperlinking to news websites based outside the State, or carrying news articles provided by outside stories, without official approval. Article 4 introduced a compulsory licensing regime for those operating "commercial internet information services", with mandatory registration for their non-commercial counterparts. Also of particular significance in this Order is Article 11, which states that "content providers are responsible for ensuring the legality of any information disseminated through their services." Further requirements include that providers must retain copies of all usage records for sixty days, and provide these to relevant officials upon request. Article 15 again reiterates the categories of material which are forbidden for providers to "produce, reproduce, release, or disseminate": this includes information which "endangers national security...is detrimental to the honour of the State...undermines social stability, the State's policy towards religion [and] other information prohibited by the law or administrative regulations."

Such laws clearly facilitate a strict, 'Father Bear' model of control over internet content originating within mainland China. Controversy has arisen when Western commercial interests have sought to exploit the huge and growing Chinese market in internet services. With the rapid growth of China's economy and its emergence in recent decades as a world economic superpower has come also a rapidly growing Chinese market for all sorts of Western-style products and services, including online services: by December 2009, it has been estimated, the number of Chinese citizens online reached 384 million.[67] Too good a business opportunity to pass up as this has appeared to business interests, many have discovered that it comes at the cost of bad publicity at home. Some big players in the IT industry sought to represent their Chinese ventures as purely a trade issue, wholly unrelated to questions of free expression. Said Bill Gates, then still Microsoft CEO, during a 1994 press photo call with the Chinese President:

---

[67] *China's Internet titans leave West behind*, CNN.COM, (January 23, 2010) http://edition.cnn.com/2010/BUSINESS/01/22/china.internet.companies/ (last visited May 12, 2010).

"[I]t's a little strange to tie free trade to human rights issues, it is basically getting down to interference in internal affairs."[68]

Other businessmen argued that they could do more to effect change in Chinese policy with regards to free expression by engaging the market and operating within the State than remaining outside; that they would also lose out on a potentially very large profit by doing so was typically less emphasised in their statements on the matter. Google took such a position when its entry into the Chinese market with Google.cn in 2006 faced heavy criticism due to the perceived capitulation of Google (whose main Google.com site was already available in China, albeit that search returns were often censored) to a content control regime far removed from American conceptions of freedom of speech.[69]

Other major Western online brands which have also begun operating in China and subject to this content regime during the past decade include Yahoo, AOL, Skype, and MySpace. Yahoo, in particular, faced controversy when the company complied with orders from Chinese courts to identify individuals who had used Yahoo services such as email and blogs to breach laws forbidding criticism of the State.[70] In early 2010, Google's relationship with the Chinese State came to a shuddering halt. In January of that year, Google announced that the company's communications infrastructure had been subject to "a highly sophisticated and targeted attack on our corporate infrastructure originating from China".[71] The primary target of the attack, according to Google, appeared to be Gmail accounts held by Chinese human rights activists. Google's official response stopped short of accusing the Chinese government of being behind this activity, but the allegation of State involvement was nonetheless implicit

---

68 G. Walton, *China's Golden Shield: Corporations and the development of Surveillance Technology in the People's Republic of China*, Canadian Rights and Democracy (2001), DD-RD.CA http://www.dd rd.ca/site/_PDF/publications/globalization/CGS_ENG.PDF (last visited May 12, 2010).

69 *Google censors itself for China*, BBC NEWS ONLINE, (January 25, 2010), http://news.bbc.co.uk/1/hi/technology/4645596.stm (last visited May 12, 2010).

70 *See, e.g.*, , *Dissident jailed 'after Yahoo handed evidence to police*,TIMES ONLINE, (February 10, 2006), http://www.timesonline.co.uk/tol/news/world/asia/article729210.ece (last visited May 12, 2010); and *Chinese couple sue Yahoo! In US over torture case*, THE INDEPENDENT,(April 20, 2007) http://www.independent.co.uk/news/world/americas/chinese-couple-sue-yahoo-in-us-over-torture-case-445436.html (last visited May 12, 2010).

71 *A New Approach to China*,(January 12, 2010), GOOGLEBLOG.BLOGSPOT.COM, http://googleblog.blogspot.com/2010/01/new-approach-to-china.html (last visited May 17, 2010).

in Google's decision to "review the feasibility of [their] business operations in China." Discussions were to be entered into as to whether the People's Republic of China would permit Google to continue to operate within the State absent the censorship of content that had hitherto been facilitated by Google.cn.[72] No such agreement proved forthcoming, and on March 22, 2010 Google officially closed down its mainland Chinese operation, with all traffic to Google.cn being redirected to the (uncensored) Google.com.hk site in the Special Administrative Region of Hong Kong.[73] An official response from China was extremely critical of Google's behaviour:

> "Google has violated its written promise it made when entering the Chinese market by stopping filtering its searching service and blaming China in insinuation for alleged hacker attacks.
>
> This is totally wrong. We're uncompromisingly opposed to the politicisation of commercial issues, and express our discontent and indignation to Google for its unreasonable accusations and conducts."[74]

On 30th March 2010, all Google search facilities were blocked in Mainland China.[75] They were made available once more in mid July of the same year, but in a severely restricted form, with only searches for products, music and translation services escaping the block.[76] The restrictive controls over the availability of the Google.cn services operate via the most significant part of China's internet content control strategy, known as the Golden Shield Project. In essence, Golden Shield, run by China's Ministry of Public Security, is a massive-scale firewall which attempts to prevent unacceptable forms of online content from penetrating the Chinese communications network. The project was begun in

---

72 *Supra* note 71.

73 *A New Approach to China: an update*, GOOGLEBLOG.BLOGSPOT.COM, (March 22, 2010), http://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html (last visited May 17, 2010).

74 *China condemns decision by Google to lift censorship*, BBC NEWS ONLINE, (March 23, 2010), http://news.bbc.co.uk/1/hi/world/asia-pacific/8582233.stm (last visited May 17, 2010).

75 *Google blames Chinese censors for outage*, LOS ANGELES TIMES, (March 31, 2010), http://articles.latimes.com/2010/mar/31/business/la-fi-china-google31-2010mar31 (last visited May 12, 2011).

76 *Google China search returns, but site in limited in features*, TECHWORLD, (July 12, 2010), http://news.techworld.com/networking/3230184/google-china-search-returns-but-site-is-limited-in-features/ (last visited May 12, 2011).

1998, and during its first several years $700 million dollars were spent upon networking and network monitoring facilities in order to realise its aims.[77] The Golden Shield operates by blocking and filtering content at the level of gateways on the telecommunications network. IP addresses linked to sites carrying unacceptable content will be blocked; where the website in question is based on a shared server, all websites on that server will be blocked. The system also incorporates DNS[78] filtering and blocking, URL[79] filtering (both for specific addresses and keywords within URLs), and keyword-based packet filtering.[80] Websites specifically forbidden in China and thus routinely blocked by the system have included Western news outlets, websites associated with dissident Chinese groups and pro-democracy movements, and groups such as Amnesty International[81] and Reporters Without Borders.[82] The list of specifically banned websites is somewhat fluid and can be difficult to determine from an outsider's point of view, as the status of sites can change at short notice, or certain parts of an organisation's web presence may be forbidden while others remain accessible. For instance, at one point much of the BBC's online content was inaccessible in China.[83] In recent years, Wikipedia[84] has oscillated between being forbidden entirely, available in Chinese only, and available also in English but with certain topics (Falun Gong, or the Tiananmen Square protests in 1989, for instance) being blocked. Typically, hotels and cybercafés patronised by tourists, journalists and other Westerners are subject to a relaxation of these rules. For the average Chinese citizen, however, Golden Shield would seem to represent a heavy-

---

77 *The Great Firewall: China's Misguided – and Futile – Attempt to Control What Happens Online*, 15.11 WIRED, . (October 23, 2007) http://www.wired.com/politics/security/magazine/15-11/ff_chinafirewall?currentPage=all (last visited May 17, 2010).

78 Domain Name System, *The hierarchical method by which Internet addresses are constructed*, GOOGLE.CO.UK, http://www.google.co.uk/search?aq=f&sourceid=chrome&ie=UTF8&q=What+does+DNS+mean#hl=en&q=Dns&tbs=dfn:1&tbo=u&sa=X&ei=PMfOTdm1O8St8QP5iYHcDQ&ved=0CBsQkQ4&fp=d6224a1ed3c88408 (last visited May 12, 2011).

79 Uniform Resource Locator, more commonly referred to as a 'website address'.

80 For a detailed explanation on how the internet operates, see C. Reed, INTERNET LAW Chap 1 (Cambridge University Press, 2nd edn. 2004).

81 AMNESTY INTERNATIONAL, http://www.amnesty.org.

82 REPORTERS WITHOUT BORDERS, http://www.rsf.org.

83 *China 'blocks' BBC Website*, BBC NEWS ONLINE, (October 12, 1998), http://news.bbc.co.uk/1/hi/world/asia-pacific/191707.stm (last visited May 17, 2010).

84 WIKIPEDIA, http://en.wikipedia.org (last visited May 17, 2010)

handed, Father Bear restriction upon online content by using technology and filtering content at the service provision level to restrict the availability of material officially considered to be undesirable.

To some degree, the effectiveness of such a strategy is questionable. Filtering based on a list of proscribed websites will always involve a great degree of playing 'catch-up'; web content can easily be mirrored or copied elsewhere, migrated to new servers with new IP addresses and URLs. A website already reviewed and categorised as 'acceptable' can also change entirely in character from one day to the next. Keyword-based blocking is a blunt tool at best, unable as it is to detect context, although where the prevention of access to certain types of material is considered to be an overriding interest, this may be of lesser concern. Those who are determined to get around the bar on certain content can do so via various technical evasion mechanisms, such as proxy servers or the use of virtual private network connections, leading some critics to conclude that such systems can be easily circumvented in order to receive unacceptable content, though it might still be possible for the system to record that such material had been accessed, and by whom.[85] Those without sufficient technical knowledge to disguise their online activity may well find themselves under arrest: In 2003, the Golden Shield's first year fully operational, Amnesty International noted a 60% rise in "the number of people detained or sentenced for internet-related offences" as compared to the previous year.[86]

C. Father Bear in the West

While the effectiveness of the Golden Shield approach may be debated, by far the most common criticism of the Chinese system by Western commentators is tied to negative perceptions of authoritarianism; phrases such as "big brother" abound, along with many emotive arguments about this being an intrusive and unacceptable level of censorship. It might at first appear that such an approach would be considered a mismatch for our democratic political culture, one which by and large emphasises a great degree of individual choice over government control. It would seem, however, that at least the ISP industry in the UK finds the use of such technologies to control unacceptable content to be a perfectly

---

85 *See, e.g.*., Clayton R, Murdoch SJ & Watson RNM, *Ignoring the Great Firewall of China*, (University of Cambridge), CL.CAM.AC.UK, http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf (last visited May 17, 2010).

acceptable way of doing things. Indeed, on analysis the main objection to the Chinese approach seems to arise more from objection to Chinese concepts of unacceptable political content than to the use of filtering technology at the service provider level *per se*. British Telecom operates what is known as 'Cleanfeed', a content blocking system which is used to prevent access to online content identified by the Internet Watch Foundation[87] as featuring child pornography, or "images of child sexual abuse". This system is used by most of the larger UK ISPs. Supporters of Cleanfeed claim that since going live in mid 2004, Cleanfeed has been used to stem a relentless tide of attempts to view online child pornography. In October 2009, in response to a question in the House of Commons, Alan Campbell MP, then Parliamentary Under-Secretary of State responsible for crime reduction, stated that:

> "The Government is very clear that the use of blocking to prevent access to these images is something that internet service providers should do, and is pleased with the support from providers, which has led to 98.6 per cent of UK consumer broadband lines being covered by blocking of sites identified by the Internet Watch Foundation as containing [child pornography]... It remains our hope that the target of 100 per cent of consumer-facing ISPs operating a blocking list will be achieved on a voluntary basis and we keep progress on the 100 per cent target under review."[88]

It is also of interest to note that the Internet Watch Foundation itself has openly stated:

> "Blocking is designed to protect people from inadvertent access to potentially illegal images of child sexual abuse. No known technology is capable of effectively denying determined criminals who are actively seeking such material..."[89]

---

86 Amnesty International, *People's Republic of China: Controls tighten as internet activism grows*, (2004), AMNESTY.ORG, http://www.amnesty.org/en/library/asset/ASA17/001/2004/en/9dc9d9e2-d64d-11dd-ab95-a13b602c0642/asa170012004en.pdf (last visited May 17, 2010).

87 INTERNET WATCH FOUNDATION, http://www.iwf.org.uk.

88 Hansard, 21 October 2009, PUBLICATIONS.PARLIAMENT.UK, : http://www.publications.parliament.uk/pa/cm200809/cmhansrd/cm091021/text/91021w0024.htm#09102144000018.

89 *See IWF Facilitation of the Blocking Initiative*, IWF.ORG.UK. http://www.iwf.org.uk/public/page.148.437.htm.

If this is merely a tool the chief effect of which is to protect people from themselves, and which cannot be relied upon to actually thwart or at least deter those actively interested in the content designated to be blocked, then the validity of such an approach as a means of enforcing certain laws pertaining to unacceptable content might be called into question. A further criticism that has been levied at this is the lack of accountability in the decision-making body. The 'blacklist' of material to be blocked is drawn up by the Internet Watch Foundation, and it is the IWF which decides whether material drawn to its attention should be blocked. This effectively means that a private body is in the position of determining whether material should be accessible to internet users without the material being first declared by a court to be unlawful. It may be posited that this critique is almost as alarmist as the claims made about Cleanfeed's effectiveness: the February 2006 news reports cited above in regards to supposed attempts to access child pornography within the UK were based on statistics released about Cleanfeed's operations.[90] Individual cases where the boundary between 'art' and 'child sexual abuse images', between innocent and unacceptable material, can and do arise. In 2007, following a tip off from a member of the public, police seized a photograph, which was on display in an art gallery as part of an installation by artist Nan Goldin. The photograph in question depicted two very young girls, one of whom was naked and facing the camera, legs splayed. That the work in question was owned by a celebrity, Elton John, ensured the story garnered much media coverage.[91] In this and several other similar incidents, the photograph was later returned and no charges brought. In December 2008, a thirty-two year old album cover caused a stir when a picture of the album caused several Wikipedia pages to be temporarily added to the IWF blacklist. The picture in question depicted a naked, prepubescent girl striking an open-legged pose, her crotch obscured by an overlayed image of a cracked-glass effect; the album's title: *Virgin Killer*.[92] Following negotiations with the Wiki Foundation, the IWF issued a statement

---

90 *See Alternative point of regulation: The End User*, part IV of this article, at 53.

91 *Sir Elton John owns photo seized from exhibition by child porn police*, TIMES ONLINE, (Sept. 27, 2007), http://entertainment.timesonline.co.uk/tol/arts_and_entertainment/visual_arts/article2537080.ece (last visited May 17, 2010).

92 *Scorpions Censored*, BBC 6 Music News, (Dec. 8, 2008), http://www.bbc.co.uk/6music/news/20081208_scorpians.shtml (last visited May 17 2010).

that "in light of the length of time the image has existed and its wide availability, the decision has been taken to remove this webpage from our list."[93] The image was reinstated by Wikipedia,[94] and no prosecution has been brought. It is, however, tempting to dismiss this handful of cases as the exceptions that prove the rule: surely, for the most part, it will be obvious whether material found online is contrary to law on sexualised depictions of children? Any content regulation law is apt to provide hard cases where material is 'near the knuckle' but not quite illegal. Nevertheless, there remains, at least an academic concern with respect to material that, however distasteful it may be, is technically lawful. At present, the IWF blacklist is limited to child sexual abuse images, however, the remit of material in which the organisation takes an active interest and will, pursuant to a complaint from a member of the public, investigate, notifying both the relevant service provider host and the police, is broader, including criminally obscene material, a broad category indeed.[95] Here there is probably more scope for mistakes to be made. Should the IWF in future expand its blacklist to incorporate such material, there may be stronger concerns raised with regards to the accountability of an extra-legal body effectively censoring online content which has not been pronounced unlawful by the proper authorities, i.e. the courts as accountable, public bodies.[96]

A number of other concerns are raised by the operation of the BT Cleanfeed system, as based on the IWF blacklist. Richard Clayton, formerly of Demon Internet, now based at the University of Cambridge, has argued that the Cleanfeed system can be reverse-engineered in order to effectively function as an index of child pornography websites for those who wish to view such content.[97] Of course, this claim is disputed by BT, who contend that it is not

---

93 *IWF statement regarding Wikipedia webpage*, IWF.ORG.UK http://www.iwf.org.uk/media/news.archive-2008.251.htm (last visited May 17, 2010).

94 *See Virgin Killer*, WIKIPEDIA, http://en.wikipedia.org/wiki/Virgin_Killer#cite_ref-bbc_6_music_2-0 (last visited May 17, 2010).

95 *IWF Role and Remit*, IWF.ORG.UK, http://www.iwf.org.uk/public/page.35.htm (last visited May 17, 2010).

96 *See also* McIntyre TJ & Scott C, *Internet Filtering: Rhetoric, Legitimacy, Accountability and Responsibility* in REGULATING TECHNOLOGIES (Brownsword R & Yeung K (eds.), Hart Publishing, Oxford 2008).

97 *See* Clayton R, *Failures in a Hybrid Content Blocking System* (2005), CL.CAM.AC.UK http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf (last visited May 17, 2010).

quite so simple a matter as Clayton suggests. Again, though, BT did admit that the system serves more to prevent accidental access, such as via following a link in a spam email, than to deter hardened paedophiles who tend to be more technologically adept than the average web user.[98] The system is also prone to the same problem of 'overblocking' as the Golden Shield Project, with one questionable site leading to many more on a shared server being blocked. Identifying 'overblocking' as a problem is, of course, something of a value judgment. Undoubtedly there are those who would consider incidental restriction of legitimate material to be acceptable 'collateral damage' in the fight against unacceptable online content. Nevertheless, the author would submit that in countries which subscribe to a Western conception of 'freedom of expression', this is unsuitable. The US First Amendment tradition outlined above would clearly never condone such an approach, while the jurisprudence of the European Court of Human Rights on the Article 10 right, while it maintains the default position of favouring freedom of expression in cases where there is any doubt as to whether an Article 10(2) restriction should be put in place, is unlikely ever to support a system that places significant restrictions on legitimate speech. A further issue which has been raised is the 'spill over' effect upon neighbouring jurisdictions. Typically, a large service provider will operate a common set-up across, for example, both the UK and Ireland, thus 'exporting' Cleanfeed regulation to a jurisdiction in which it has not been officially established and which may have differing laws. Were Cleanfeed-type systems to be applied to a broader range of content, this could have the potential for a large quantity of material that is perfectly legal in the neighbouring jurisdiction nevertheless being censored out from availability. A foreshadowing of this occurred in the 1990s, when Rupert Murdoch's Sky organisation established a South East Asian arm. As per normal commercial practice, this straddled several different jurisdictions in the region, however, in order to ensure access to the lucrative Chinese market, all were subjected to the much more restrictive Chinese standard of content regulation.

These various issues and concerns relating to blocking systems in use by internet service providers have long been something left to national policy, but

---

[98] *Back door to the blacklist* THE GUARDIAN (May 26, 2005), http://www.guardian.co.uk/technology/2005/may/26/onlinesupplement (last visited May 17, 2010).

this may be set to change. In March 2009, the European Commission published a proposal for a new Framework Decision[99] which would commit Member States to "take the necessary measures to...obtain the blocking of access by internet users to internet pages containing or disseminating child pornography..."[100] Such a policy is also promoted by the CIRCAMP (Cospol Internet Related Child Abusive Material Project), which involves partners from sixteen countries.[101] The likelihood of a European legal instrument requiring mandatory imposition of filtering is increased by the European Commission's own assessment that filtering systems which have no basis in legislation, being operated by service providers on a purely voluntary level, do not qualify as "prescribed by law" and are thus apparently in infringement of Article 10 of the European Convention on Human Rights.[102] The author would also submit that a further Article 10-based assessment would have to be made of any proposed introduction of mandatory blocking by service providers. The free expression interest would require to be weighed against the interest in controlling the material. It is highly foreseeable, of course, that any argument based on an objective analysis of the likely utility of such measures in preventing the distribution of child pornography will be wholly swept aside by emotive arguments: this is exactly the type of situation where doubting opinions are often interpreted as support for whatever evil the proposed legal change is designed to combat. The Strasbourg court will always prioritise the control of child pornography over free expression in the

---

99 *Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA*, (March 25, 2009), EUR-LEX.EUROPA.EUhttp://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0135:FIN:EN:PDF (last visited May 18, 2010).

100 Article 18, *Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA*, (March 25, 2009), EUR-LEX.EUROPA.EUhttp://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0135:FIN:EN:PDF (last visited May 18, 2010).

101 For details of CIRCAMP *see* http://circamp.eu/ (last visited May 18, 2010); for further academic analysis of both CIRCAMP and EC policy leading to the proposed Framework Decision see McIntyre TJ, *EU Developments in Internet Filtering of Child Pornography*, BILETA Conference (2010), http://www.bileta.ac.uk.

102 *See* European Commission, *Accompanying document to the Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA*, 30 (March 25, 2009), EUR-LEX.EUROPA.EU http://eur-lex.europa.eu/LexUriServ.do?uri=SEC:2009:0355:FIN:EN:PDF (last visited May 18, 2010); *See also* Sunday Times v. UK, (1979) 2 E.H.R.R. 245.

broad sense. Whether the mandatory use of a system which, hypothetically, led to chronic overblocking of innocent material without corresponding results leading to the limitation of distribution of child pornography, is Article 10 compliant might be a less clear-cut argument in theory, although it would probably have to be a very severely disproportionate limit upon free expression in order to overrule the emotive arguments in favour.

A further, Father Bear type legal requirement which obliges service providers to effectively act as agents for the State in enforcing content regulation laws is the UK's Digital Economy Act 2010. In the face of much opposition, this controversial statute was rushed through Parliament during the final days of the Brown government. Critics raised a great many objections to this Act, not least to the provisions requiring service providers to police copyright infringement by their subscribers. The Act places a range of obligations upon service providers, including to notify subscribers when a complaint of infringement has been released, to provide details to the relevant rightsholder of all instances of infringement, and ultimately to maintain the capacity to suspend internet access by habitual infringers for a period.[103] Provision is also made for a right of appeal to be granted to subscribers who are to be so cut off, although this did nothing to quell opposition to the Act, before or after its passage. The details of how it was envisaged that these aims would be realised remain unclear, as the Act predominantly empowered various offices and positions to put in place the necessary practical workings. Compliance with the Act is to be overseen by OFCOM,[104] and intermediaries who do not meet requirements are liable to be fined up to UK £250,000.[105]

Opposition to the Digital Economy Act came not only from privacy campaigners[106] and fringe political parties,[107] but also from the Liberal Democrats,

---

103 *See* Sections 3 - 18, UK DIGITAL ECONOMY ACT, 2010.

104 Sections 11-12, DIGITAL ECONOMY ACT, 2010 inserting, respectively, new sections 124I 'Code by OFCOM about obligations to limit internet access' and 124J 'Content of code about obligations to limit internet access' into the Communications Act, 2003.

105 Section 14, DIGITAL ECONOMY ACT, 2010 inserting new section 124L 'Enforcement of obligations' into the Communications Act, 2003.

106 *See, e.g.*, OPENRIGHTSGROUP, http://www.openrightsgroup.org/ (last visited May 18, 2010).

107 *E.g.* Pirate Party, http://www.pirateparty.org.uk (last visited May 18, 2010), or Green Party, http://www.greenparty.org.uk (last visited 18th May 2010); the Greens, as of May 2010, now have their first MP and a voice within Parliament.

the only mainstream political party to oppose the passage of the Act.[108] The 2010 UK General Election produced a hung Parliament, with no one party having an overall majority. Negotiations led to the Conservatives, the largest party in Parliament after the election, forming a coalition government with the Liberal Democrats. Notably, however, OFCOM announced shortly after the election that only larger fixed-line service providers, those with more than 400,000 subscribers, will face obligations under these provisions in the Digital Economy Act. This has, predictably, led to suggestions that smaller intermediaries, as well as mobile broadband providers, will become 'piracy havens'.[109] Opponents from within the intermediary community, headed by BT and TalkTalk sought judicial review of the Act's passage on grounds that it received 'insufficient scrutiny before being rushed through into law', and that it is in key respects incompatible with the Electronic Commerce Directive, the E-Privacy Directive and Article 10 of the European Convention on Human Rights.[110] This challenge, broadly speaking, failed, Parker J. finding the Act to be acceptable within the framework of European rights.[111] The one area in which the High Court upheld the service providers' challenge is, however, far from insignificant. The Authorisation Directive[112] requires that any administrative charges imposed upon a service provider shall:

> "cover only the administrative costs which will be incurred in the management, control and enforcement of the general authorisation scheme and of rights of use and of specific obligations..., which may include costs for international cooperation, harmonisation and standardisation, market analysis, monitoring compliance and other market control, as well as regulatory work involving preparation and enforcement of secondary legislation and administrative decisions, such as decisions on access and interconnection".[113]

---

108 LIBERAL DEMOCRATS, http://libdems.org.uk/home.aspx (last visited May 18, 2010).

109 *Ofcom creates piracy havens at small ISPs* THE REGISTER (May 18, 2010), http://www.theregister.co.uk/2010/05/18/small_iss_dea/.

110 *BT and TalkTalk in legal challenge to Digital Economy Act*, BT PRESS RELEASE, (July 8, 2010) http://www.btplc.com/news/Articles/ShowArticle.cfm?ArticleID=98284B3F-B538-4A54-A44F-6B496AF1F11F.

111 R (BT Telecommunications PLC & Anor) v. Secretary of State for Business, Innovation and Skills, [2011] E.W.H.C. 1021 (Admin.), BAILII.ORG http://www.bailii.org/ew/cases/EWHC/Admin/2011/1021.html, (last visited May 12, 2011).

112 Directive 2002/02/EC.

113 Article 12(a), Directive 2002/02/EC.

The draft Online Infringement of Copyright (Initial Obligations) (Sharing of Costs) Order 2011[114] included "qualifying costs" which Parker J. held amounted to administrative charges which service providers would be obliged to pay to OFCOM in order for the latter and the appeals body to operate the functions delegated to them by the Act. Such charges are clearly prohibited by the Authorisation Directive, and thus are unlawful. As the Order in its draft form envisages that the service provider would pay 25% of the total cost of dealing with each copyright infringement report,[115] this is a positive gain for the service providers who otherwise would have been facing a significant bill each time one of their subscribers was investigated over a claimed infringement of copyright. The other obligations still stand, although developments elsewhere in Europe may call them into question.

France finally passed its three strikes law in October 2009, following an amendment to satisfy the Constitutional Council providing the opportunity for judicial review prior to a subscriber being cut off for up to twelve months.[116] As originally passed by Sarkozy's government, there would have been no court hearing on the infringements, instead punitive action would have been taken based solely upon a presumption of guilt, violating the right to be presumed innocent until declared otherwise in a court of law. New Zealand's equivalent, one of the first to be introduced, was never enforced and in fact swiftly reversed by the government.[117] The draft international Anti-Counterfeiting Trade Agreement, which has been under discussion for several years among some thirty parties including the European Union and the USA, originally included plans for a number of controversial provisions including the obligatory hand over of subscriber information by service providers without a warrant, and a version of the 'three strikes' rule. Various leaked drafts of the Agreement included such strong provisions, although the position may have changed: the April

---

114 LEGISLATION.GOV.UK, http://www.legislation.gov.uk/ukdsi/2011/9780111505779/schedule/paragraph/1 (last visited May 12, 2011).

115 *See* Draft Online Infringement of Copyright (Initial Obligations) (Sharing of Costs) Order 2011. Clause 1(6)(b).

116 *France Approves Wide Crackdown on Net Piracy*, THE NEW YORK TIMES, (October 22, 2009), http://www.nytimes.com/2009/10/23/technology/23net.html?_r=1 (last visited May 18, 2010).

117 *3 strikes' strikes out in NZ as government yanks law*, ARS TECHNICA, (March 23, 2009), http://arstechnica.com/tech-policy/news/2009/03/3-strikes-strikes-out-in-nz-as-government-yanks-law.ars (last visited May 18, 2010).

2010 draft officially released to the public omits these provisions. Instead the section on service providers emphasises the need to provide "limitations and defences" for service providers in respect of third party liability, along with a pledge "to prevent infringement and remedies which constitute a deterrent to further infringement...Those measures, procedures and remedies shall also be fair and proportionate."[118] That such draconian measures as 'three strikes' are proposed in the copyright field is largely reflective of the influence of the powerful entertainment industry lobby: it is wholly typical for these debates to be primarily viewed by government as a rightsholder issue rather than, say, a matter of what is best for the consumer.

An obstacle for the rollout of 'three strikes' type laws is the growing perception of internet access as a fundamental human right. A global survey, commissioned by the BBC and carried out across twenty-six countries and involving over 27,000 adult participants, found that almost eighty percent of those surveyed believed access to the internet to be a fundamental human right.[119] This view has also been presented by the influential US Secretary of State, Hilary Clinton,[120] and the French Constitutional Council in its ruling on the initial, unamended French version of 'three strikes'.[121] The fact that the French law passed one sufficient provision that had been made to allow a right of appeal and require a court order prior to a suspension effectively emasculated the law, as rightsholders are not now simply able to demand that a user be identified and cut off, but must instead go to court in respect of infringement.[122]

---

118 *See* Section 4, Anti Counterfeiting Trade Agreement Public Predecisional/Deliberative Draft April 2010 : Special Measure Related to Technological Enforcement of Intellectual Property in the Digital Environment, TRADE.EC.EUROPA.EU, http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146029.pdf (last visited May 18, 2010).

119 *Internet access is a 'fundamental right*, BBC NEWS ONLINE, (March 8, 2010), http://news.bbc.co.uk/1/hi/technology/8548190.stm (last visited May 18, 2010); For detailed survey results, *see Four in Five Regard Internet Access as a Fundamental Right: Global Poll*, NEWS.BBC.CO.UK, http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/08_03_10_BBC_internet_poll.pdf (last visited May 18, 2010).

120 *Remarks on Internet Freedom*, (January 21, 2010), STATE.GOV http://www.state.gov/secretary/rm/2010/01/135519.htm (last visited May 18, 2010)..

121 *Internet access is a fundamental human right, rules French court*, DAILY MAIL ONLINE, (June 12, 2009), http://www.dailymail.co.uk/news/worldnews/article-1192359/Internet-access-fundamental-human-right-rules-French-court.html (last visited May 18, 2010).

122 *Top French court rips heart out of Sarkozy legislation*, THE TIMES ONLINE, (June 11, 2009), http://technology.timesonline.co.uk/tol/news/tech_and_web/article6478542.ece (last visited May 18, 2010).

In the Belgian case of *Scarlet* v. *SABAM*, the Société Belge des auteurs, compositeurs et éditeurs (SABAM), a royalty collection body representing copyright holders, persuaded a court to issue an injunction against the Defendant ISP ordering it to monitor its servers for any sign of unlawful file-sharing which infringed the rights of SABAM members, to identify the culprits, and to filter out and block these activities. This injunction was perpetual, and all costs of compliance with its terms fell to be borne by the service provider. Unsurprisingly, the service provider appealed against the order. The Brussels Court of Appeal referred the matter to the European Court of Justice, specifically on the question of whether such an injunction could be issued compliant with Article 8(3) of the Copyright in the Information Society Directive[123] and Article 11 of the Intellectual Property Enforcement Directive,[124] both of which require member States to make provision for injunctive relief to protect copyright holders from online infringement. Under the Directives, such injunctions may be granted not only against the infringing parties, but also their service providers. In turn, these provisions must be enacted in a manner compliant with both the Article 8 (privacy) and Article 10 (freedom of expression) rights as set out in the European Convention on Human Rights.

At the time of writing, the European Court has yet to reach a ruling on the matter, but Attorney General Cruz Villalon has provided the court with an opinion on the matter.[125] The Attorney General notes that the injunction in question is an extraordinary measure, and one which is rather arbitrary when considering how difficult it is to foresee and the serious cost to the service provider of compliance. While the service provider has been ordered to completely block

---

123 Directive 2001/39/EC. Article 8(3) states: 'Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.'

124 Directive 2004/48. Article 11 states: 'Member States shall ensure that, where a judicial decision is taken finding an infringement of an intellectual property right, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement. Where provided for by national law, non-compliance with an injunction shall, where appropriate, be subject to a recurring penalty payment, with a view to ensuring compliance. Member States shall also ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right, without prejudice to Article 8(3) of Directive 2001/29/EC.'

125 *See* CURIA.EUROPA.EU, http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=rechercher&numaff=C-70/10.

the unlawful activity, the Attorney General notes that this is not something which has been achieved before. It would indeed be a significant technological step were a service provider to manage to block an identified category of material with a one hundred per cent success rate. Further, the Attorney General has identified significant problems in terms of human rights compliance in that there is no guarantee given that the terms of the injunction will respect the privacy of individual subscribers, nor has any right of appeal been provided for a subscriber who unexpectedly finds his or her internet service terminated. Should, as seems likely, the court follow this advice, it is likely to require some degree of rethinking in Westminster as to the Digital Economy Act, albeit that the provisions of the latter are somewhat less draconian, for example, provision is made for a basic right of appeal and an appropriate forum in which such an application might be reviewed. The key problem with this legislation from a human rights perspective, one which was particularly raised by the Joint Committee on Human Rights, is that the degree of detail which has been left to secondary legislation makes it "impossible [to] assess fully whether [the Act] will operate in a compatible manner in practice".[126] Jeremy Hunt, the Culture Secretary of the coalition government returned by the general election of May 2010, in February 2011 ordered OFCOM to review the Act, accepting that "it is not clear whether the site blocking provisions in the Act could work in practice." The government also initiated a dialogue with the service provider community in order to explore whether it might be possible to bypass the Act with a system of voluntary blocking by service providers. It remains to be seen how the situation will be resolved, as the conclusion of the British judicial review of the Digital Economy Act is contradictory to the likely outcome of the SABAM case in the European Court, assuming (as is very likely) the Attorney General's advice is followed.

Should the notion of a fundamental right to internet access, even one that is not inalienable, as per the French example, gain the full support of global lawmakers, this is one Father Bear approach to incorporating service providers into the State mechanism for enforcing internet content regulation that is likely to be very limited in effect.

---

126 House of Lords, House of Commons Joint Committee on Human Rights *Legislative Scrutiny: Digital Economy Bill Fifth Report of Session 2009-2010* ¶ 1.39.

D. Mother Bear Regulation: the Soft Touch

Father Bear, strong-arm regulation, then, is an imperfect solution. State conscription of service providers to regulate by blocking and filtering is problematic, raising all sorts of questions, not least that of how it will be funded – by the service providers (who will, inevitably, pass on the cost to the subscriber in the form of higher fees)? Or by the State (which will, inevitably, pass on the cost to the taxpayer)? In most Western States, it is likely that service providers will be very resistant to any such compulsory government-run scheme. That said, voluntary blocking is no less problematic, raising questions of accountability, over-blocking, and potentially even, within Europe, a breach of Article 10. So is a softer, more liberal policy – a Mother Bear type approach – the answer? In relation to civil liability (with the specific exception of intellectual property), US Federal law provides an extremely broad immunity for unlawful content uploaded by third parties. This immunity is to be found in the Communications Decency Act of 1996. The CDA was much vilified at the time due to other provisions which created new offences in relation to online pornography and its availability to minors, and which were ultimately found unconstitutional and struck out by the US Supreme Court in the landmark case of *ACLU* v. *Reno*.[127] The so-called 'Good Samaritan' provision in Section 230, however, remained. This section grants a broad and unconditional immunity from liability in respect of third party provided content. It was designed in order to free service providers from fear of liability should they make any effort to edit material on their servers, and intended to thereby encourage them to censor out unacceptable material. In practice, the application of the immunity is no doubt very far from those intentions. The leading case on Section 230 is *Zeran* v. *AOL*.[128] In this case, Section 230 prevented a service provider from being liable for a defamatory posting which it hosted, despite the fact that it had actual knowledge of the posting. A string of cases have followed *Zeran*, the immunity seemingly widening over time. In *Blumenthal* v. *Drudge*,[129] the service provider escaped liability for

---

127 ACLU v. Reno 521 U.S. 844 (1997), LAW.CORNELL.EDU, http://www.law.cornell.edu/supct/html/96-511.ZS.html (last visited May 19, 2010); for further discussion of the Communications Decency Act in this respect *see* G. Sutter, *'Nothing New Under the Sun': Old Fears and New Media* 8(3)INT'L J. OF L.& INFO. TECH. , 338-378 (2000).

128 Zeran v. AOL 129 F. 3d. 327 4th Cir. (1997).

129 992 F Supp 44, 51-52.

a defamation posted by a gossip columnist – this in spite of the fact that the intermediary maintained active editorial control over the column. Again, in *Ben Ezra, Wenstein & Co* v. *America Online*,[130] a service provider was able to avoid liability in relation to erroneous stock values attributed to the plaintiff's company as the information had been provided by a third party. *Schneider* v. *Amazon.com*[131] saw Section 230 being applied to the operator of a website to which third parties were able to post material – in this case, the action arose out of postings to Amazon.com's user reviews which allegedly defamed the plaintiff author. Amazon.com, despite not being a traditional internet service provider as such (c/f America Online, for example), were ruled to be entitled to the Section 230 defence.

A further significant step came in the Ninth Circuit Court of Appeal's decision in *Batzel* v. *Smith, Cremers & Museum Society Network*.[132] This ruling made the defence available to a non-commercial entity for the first time. The plaintiff, Batzel, was a lawyer who collected art. Smith, employed by Batzel as a labourer working at her house, overheard a conversation in which Batzel said she was related to Gestapo leader Heinrich Himmler. Smith drew the wild conclusion that Batzel's collection of European art must therefore have been stolen by the Nazis and inherited by her, and sent an email outlining this to Cremers, the editor of the Museum Society Network. Cremers was involved with running the organisation's email list which was designed to publish information about stolen paintings. Cremers did not tell Smith that he would publish the content of the email, but did so with only minor edits, sending it to some 1,000 MSN list subscribers. Batzel discovered this and instigated defamation proceedings. Overruling the decision of the lower court, the Court of Appeal decided that the minor amendments made by Cremers were not sufficient to make it a separate piece of expression: it remained fundamentally Smith's content. The case was sent back to the lower court in order to decide whether Cremer had a reasonable belief that Smith's email laws intended for publication,

---

130 Ben Ezra, Wenstein & Co v. America Online (D.N.M. 1999).

131 Schneider v. Amazon.com Case No. 46791-3-I, 31 P.3d 37 Washington Court of Appeal (September 17, 2001).

132 Batzel v. Smith, Cremers & Museum Society Network 333 F.3d 1018 9th Circuit (2003).

in which case the Section 230 defence would be available. In *Barrett* v. *Fonorow*[133] the Illinois Court of Appeal cited Batzel and its wide definition of what comes under ambit of Section 230 – Section 230 applied to people running a website which contained defamatory remarks just as it did to a service provider offering traditional internet access and/or hosting facilities.

Two cases in later years posed a challenge to the status quo in relation to Section 230. In *Barrett* v. *Rosenthal*,[134] a Californian Court of Appeal sought to fundamentally alter the accepted position on the application of the immunity, finding that *Zeran* and all those cases following it had misinterpreted the provision. This decision claimed that all Section 230 actually sought to do was to immunise service providers from strict, publisher liability for third party content, but that traditional distributor, awareness-based liability would still arise. This decision was later reversed by the Supreme Court of the State of California, which found *Zeran* and subsequent decisions to be sound.

In *Fair Housing Council of San Fernando Valley* v. *Roommates.com*,[135] the court was asked to consider the liability position of a website which provided a searchable database designed to allow users to advertise for a 'roommate' to share rented living quarters. The Defendants drafted and posted questionnaires designed to build user profiles to the website. These questionnaires included questions about roommate preferences, including a question about the preferred sexual orientation of potential roommates. The Defendants, if liable in respect of the profiles thus posted to their website, would face liability under the Fair Housing Act as this required members to answer questions that potentially enabled other members to discriminate against them, and these questionnaires were distributed via the website. The court of first instance ruled that the Defendants enjoyed the protection of Section 230. Due to the way in which the website was set up, the flow of information was controlled in such a way that answers to questionnaires were used to determine whether an individual should be notified of rooms available, or be allowed to view a particular profile. For instance, a person who was listed as having children would not be shown

---

133 Barrett v. Fonorow 799 N.E. 2d 916, 279 Ill Dec. 113.

134 Barrett v. Rosenthal (2003) 112 Cal.App.4th 749, 757-758, 5 Cal.Rptr.3d 416 and Supreme Court of California Opinion No. S122953 (November 20, 2006).

135 Fair Housing Council of San Fernando Valley v. Roommates.com CV-03-09386-PA 9th Cir.;(May 15, 2007).

the listing of someone who did not wish to let to anyone with children. The Court of Appeal ruled that this involvement in the distribution of the material was sufficient involvement in the creation of the online content that the material was no longer wholly third-party content, and thus the site was not entitled to enjoy the Section 230 immunity. The Plaintiffs were therefore entitled to bring a case for violation of the Fair Housing Act, which prevents discrimination in residential property lettings. Section 230 protection *was* however available in relation to an open-ended question which allowed users to post a paragraph describing what they were looking for in a roommate; most potentially discriminatory responses were found here. Users were permitted to formulate their own responses, with no set 'tick-box' type answers given. The Defendants' involvement in this voluntarily-supplied content was not sufficient to make them a content provider: no specific answers were suggested, and they did not prompt any of the discriminatory comments made. Further, these comments were not used in order to restrict or channel access to profiles by other members. Contrary to some commentator's views, this decision does not represent a limit on the extent of the Section 230 immunity, but rather a distinction on the facts of the case between what is and is not third party content in relation to the availability of the immunity. Those running such websites in future will have to be careful as to how they solicit and treat information if they wish it to remain third party content. Clearly, Section 230 has evolved into a very broad immunity indeed;[136] it might be argued that it is equally clear that it has failed on a fundamental level. Absent the Communications Decency Act's provision which rendered it an offence to provide internet services to an individual engaged in supplying pornography to a minor, there is no impetus for a US-based service provider to adopt an active role in editing their servers.[137] Further, as the case-law indicates, providing that a defamatory posting can be shown to be third

---

136 It should also be noted that the application of Section 230 is not limited to liability for defamatory content alone. It has been successfully used in order to evade liability for hosting unlawful third part content in a whole range of situations, including a sexual assault upon a minor arising from a Myspace profile which falsely identified a thirteen year old girl as an adult (Doe v. Myspace 528 F.3d 413 5th Cir. (2008)), financial loss occasioned by clicking on fraudulent advertisements on Google (Goddard v. Google, *Inc.* 640 F. Supp. 2d 1193 (N.D. Cal.) (Jul. 30, 2009)), and fraudulent advertisements on an online ticket reseller website (Milgram v. Orbitz Worldwide, LLC ESX-C-142-09 (N.J. Super. Ct. Aug. 26, 2010), SCRIBD.COM http://www.scribd.com/doc/37008339/Milgram-v-Orbitz.

137 Indeed, the awareness-based regime in force in relation to third party copyright infringement under the Digital Milliennium Copyright Act 1998 (see below) would further discourage this.

party content, made available at the request of a third party, the service provider can escape liability no matter how aware of the unlawful material. Rather than freeing the service provider to take an active voluntary role in web regulation, this provision in fact facilitates an abdication of any responsibility for defamatory material online. This is very far removed from the original intention of the Section 230 immunity, which after all was drafted in a context of which it was shorn by the Supreme Court, and so inevitably exists in a position wholly unintended by those by whom it was formulated. It is submitted that this is an unsatisfactory solution from an objective point of view: surely it is reasonable that the knowing distribution of unlawful material occasion legal liability?

E. Awareness-based Liability: a third way?

So, both direct State regulation via recruiting intermediary service providers as an effective agent of the State (Father Bear) and softer regulation leaving them free to do as they will in the hope that this will spur a great sense of social responsibility leading to effective self-regulation (Mother Bear) are less than ideal modes of regulating online content at the level of service provider. Is there a viable middle ground, a 'third way' option that might fit the 'just right' Baby Bear role? It has long been posited by academics that there exists a broad international consensus that a service provider should not face liability in respect of unlawful content provided by a third party and of which the service provider is unaware.[138] Might an awareness-based liability standard then be a realistic option for the control of online content in the absence of being able to trace and punish the source of the material?

The EU Directive on Electronic Commerce[139] provided a framework for EU Member States to enact into domestic legislation which incorporated an awareness-based liability regime for service providers in respect of third party provided content. Across several articles in Section 4 - "Liability of Intermediary Service Providers" - the Directive provides a sliding scale of liability. Essentially, the greater the potential for control that a service provider might be reasonably expected to have over the material in question, the higher the standard the

---

138 *See, e.g.*, Reed C., INTERNET LAW ¶ 4.2.4 (Cambridge University Press, 2nd edn. 2004).

139 EU Directive on Electronic Commerce 2000/31/EC.

service provider must reach in order to be entitled to claim the immunity. Article 12 applies where a service provider is functioning as a "mere conduit", merely providing access to the internet with no storage of material for longer than is strictly necessary to forward a transmission, and no control over when, from whom and to whom a communication is sent, nor its content. Where this is the case, the service provider is granted a complete immunity from any liability for the content (though note that a member State's courts may require that an identified person's communications be monitored in order to prevent or terminate an infringement). The immunity under Article 13, which deals with caching, is qualified. Here the service provider may only avail itself of the defence if it has not been in receipt of "actual notice" of the unlawful content in question. The distinction between caching and hosting in the Directive is significant, given that while caching involves some degree of storage and therefore the service provider can reasonably be expected to have a greater potential to control material which has been temporarily cached, it clearly would be unrealistic to the point of being unjust to expect that this extend to the same level of awareness as might reasonably be expected in relation to material that is hosted long-term. Caching is defined in the Directive as:

> "... automatic, intermediate and temporary storage ... performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request ..."

Note that for the purposes of the Directive, caching is specified to be a *temporary* activity. This is significant as a *technical* understanding of caching does not entail a time-limited treatment of the material. For instance, caching on a technical level is typically understood to mean:

> "the service of copying the pages of a Web site to geographically dispersed servers, and when a page is requested, dynamically identifying and serving page content from the closest server to the user, enabling faster delivery."[140]

Per Article 14, "illegal activity or information" which is actually hosted by an ISP, having been placed on its servers by a third party, will not give rise to liability on the part of the service provider unless or until that service provider

---

[140] WHATIS.TECHTARGET.COM, http://whatis.techtarget.com/definition/0,,sid9_gci214325,00.html.

has sufficient awareness of the unlawful nature of the material and fails to remove or to disable it. Reflecting the burden of proof in the respective courts, the requisite level of awareness for content which breaches criminal law is actual knowledge, whereas in relation to content which is contrary to civil law (such as libel), constructive knowledge is sufficient. Once the relevant level of awareness is present, the service provider is required to remove the material as quickly as is reasonably practicable or face liability.

Tailing off this section of the Directive, Article 15 clearly provides that no Member State is to oblige service providers within its jurisdiction to routinely edit the material which they make available online, although there is no bar upon an individual service provider deciding to assume such editorial responsibility for itself. This would, of course, be highly inadvisable as the service provider would thereby open itself up to a great risk of primary liability.

In theory, this awareness-based system seems a fair and balanced answer to the question of how best fairly to apportion legal liability to service providers. Just as it would be manifestly unfair to penalise a service provider in respect of information over which they had no control, or even information hosted on their servers at the request of a third party and of which they could not possibly have been aware (for instance, an off-topic, defamatory posting on a third party-run bulletin board dedicated to discussion of 1940s clothing), then so too it would seem that a service provider who knowingly continues to allow their system to perpetuate the distribution of unlawful content of which they are aware should indeed face liability. Yet in practice this raises pronounced difficulties.

Case-law across several Member States has shown that the Directive has not provided for the level of harmonisation intended, in particular in relation to eBay. eBay, the global market leader in online auction service provision, has faced lawsuits across a number of European jurisdictions regarding the sale of counterfeit products via its website. A number of cases have been brought against eBay, each involving trademark holders demanding that eBay be held responsible for policing and preventing the sale of counterfeit items which infringe those marks by eBay members. As one might expect, eBay's response has been to argue that it is for the owner of the mark to trawl for infringements and report

them to eBay, who will then remove them once on notice. Given the nature of the website, it may not always be possible for eBay to detect whether a particular item in a particular auction is counterfeit. That the time and expense involved in finding those sellers who are trying to pass off counterfeit goods should be incurred by the trademark owner who stands to benefit from the mark seems wholly reasonable. Not all courts have agreed, however. Significantly, the Directive provides that each of the qualified immunities granted may be subject at the national level to a court injunction ordering the service provider to enforce a specific injunction. See, for instance, Article 14(3):

> "The limitations of the liability of intermediary service providers established in this directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it."

In the German case of *Rolex* v. *Ebay/ Ricardo (Internet Auction I)*,[141] the Federal Court of Justice was asked by the claimant to find eBay liable for the sale by a subscriber of counterfeit Rolex-branded wristwatches, in breach of the claimant's registered trademark. Further, the claimant also wished to oblige eBay to prevent future such abuse of its mark. The Court ruled that under the German domestic equivalent of Article 14, eBay could not be held liable in respect of the auctions for counterfeit goods as it was entitled to rely upon the notice-based, qualified immunity provided. But eBay was not to be excused liability completely. Article 14(3) rendered this further a matter for domestic German law. Under Section 1004 of the German Civil Code, the rightsholder retains a right of permanent injunctive relief against any person who has caused the property to be interfered with, insofar as the burden thus imposed is reasonable. In this case, the court held, not only must eBay take down the specific auctions complained of, but also monitor and remove any and all future auctions for infringing goods providing that it was economically reasonable for them so to do. On the facts it was found reasonable to expect eBay to police its auctions for counterfeit Rolexes via, for example, installing software which would

---

[141] Rolex v. Ebay/ Ricardo (Internet Auction I) BGH 11.03.2004, I ZR 304/01, JurPC Web-Dok.

detect such auctions. In the English case of *L'Oreal* v. *eBay*[142] Arnold J. was so minded to find that, under European and English law, "eBay...are under no legal duty or obligation to prevent infringement of third parties' registered trademarks."[143] He further considered that eBay should not be liable to prevent future infringements simply on the basis that such had previously happened and might do again.[144] The decision of the English court stands to be further impacted by the reasoning of the European Court of Justice, to which the case has been referred for clarification on a range of issues.[145] In substantially similar circumstances, a French court simply declined to recognise eBay as being entitled to the protection of Article 14, ruling that eBay's level of interaction with its users, services provided such as dispute resolution, and so on rendered its activities far beyond mere passive hosting.[146]

Other difficulties with the European approach also arise. When the draft legislation bringing it into UK domestic law was put out to public consultation, a major complaint raised by the internet industry was the lack of any definition of 'actual notice', as this could be crucial regarding liability for hosted, third party material in contravention of criminal law. This led to the introduction into the final Electronic Commerce (EC Directive) Regulations 2002 of Regulation 22, which amounts to a non-exhaustive list of factors which a court may consider when deciding whether an intermediary has received, via any means of contact that it has made available in compliance with Regulation 6(1)(c), actual notice of unlawful third party material present on its servers. Regulation 6(1) makes it obligatory for intermediaries to provide certain information to the end user 'in a form... which is easily, directly and permanently accessible.' Regulation 6(1)(c) refers to contact details which facilitate rapid and direct communication with the intermediary, such as email addresses,

---

142 L'Oreal v. eBay [2009] E.W.H.C. 1094 (Ch.), JUDICIARY.GOV.UK, *available at* http://www.judiciary.gov.uk/docs/judgments_guidance/l'oreal-ebay.pdf (last visited 19 May 2010) [hereinafter *L'Oreal*].

143 *L'Oreal*, *supra* note 142, at 375.

144 *L'Oreal*, *supra* note 142, at 381.

145 *See also* A Rühmkorf, eBay on the European Playing Field: A Comparative Case Analysis of *L'Oréal v eBay*, 6:3 *SCRIPTed* 685, (2009), LAW.ED.AC.UK,http://www.law.ed.ac.uk/ahrc/script-ed/vol6-3/ruhmkorf.asp (last visited May 19, 2010).

146 S.A. Louis Vuitton Malletier v. eBay, Inc., Tribunal de Commerce de Paris, Premiere Chambre B (Paris Commercial Court), Case No. 200677799 (June 30, 2008).

telephone numbers, and other contact details. This obligation is easily fulfilled by placing such contact details in a prominent place on an organisations homepage, or now more commonly linked to via an obvious 'contact us' hot link which is available on all pages and leads directly to a page of contact details. A dedicated (and frequently checked) email address for complaints of any sort is the most usual (and probably most useful) option here. Regulation 22 also lists several other factors which a court may consider:

> "the extent to which any notice includes –
>
> i) the full name and address of the sender of the notice;
>
> ii) details of the location of the information in question; and
>
> ii) details of the unlawful nature of the activity or information in question."

Although Regulation 22 offers some clarification of 'actual notice' many intermediaries remain sceptical, arguing that the position is still too uncertain in the absence of a clear court decision on the issue.

It also remains of concern to many that there is no clear delineation of the time frame within which action is expected to be taken following receipt of notice. The Regulations repeat the Directive's requirement that intermediaries act 'expeditiously', but this is not expanded upon any further. Some guidance as to what might be a reasonable timeframe can be found in the UK Terrorism Act 2006; in relation to the presence of material which encourages terrorism and the dissemination of terrorist publications, a service provider notified of such material is expected to remove it within "2 working days".[147] This time limit is only law in that very specific context, though a court might consider it reasonable to apply the same time limit by analogy in interpreting the "acting expeditiously" requirement in the Directive / Regulations. The UK Defamation Bill 2010, a private member's bill introduced in the House of Lords by Liberal Democrat peer Lord Lester, would have allowed a very generous fourteen days[148] within the context of a statutory 'notice and take down' approach. The

---

147 Section 3, TERRORISM ACT, 2006.

148 Clause 9(4)(a).

government-sponsored draft Defamation Bill attached to a public consultation, ongoing at time of writing, does not include any such provision. It is anticipated that if something along these lines is included in the final Act (currently projected to be delivered for Royal Assent by 2013, at the earliest), it is rather more likely to tend towards a shorter grace period as required in respect of terrorist related information. Where the standard of liability for third party material applies equally to all forms of unlawful material, there is a compelling argument for a common legal standard of what constitutes 'acting expeditiously', as opposed to piecemeal identification of different time limits for differing content.

On a far more fundamental level, going to the core of the awareness-based liability regime outlined in the Electronic Commerce Directive, there is the fact that a service provider on notice of unlawful content is in a position of being asked to make a legal decision. When a complaint of unlawful material has been received, the service provider will have to decide whether to agree with the complaint and remove the material, or reject it and run the risk of liability. The experience of the service provider in the English case of *Godfrey* v. *Demon*[149] is a cautionary tale indeed. Demon, in receipt of actual notice of the presence on a discussion group which it hosted but did not actively monitor of a posting which allegedly defamed the claimant, failed to act to remove it. In a preliminary hearing designed to determine whether the defendant service provider could have recourse to the awareness-based defence in Section 1 of the UK Defamation Act 1996 to the distribution of third party defamatory material, the court held that as soon as Demon received actual notice they were aware and the defence became unavailable; liability for publication of the alleged defamation arose from that point. The service provider chose at that point to settle the case for some GBP 500,000 (which included costs). Although decided under the Defamation Act 1996, the elements of the defence are sufficiently similar to the regime in the Electronic Commerce Directive that the courts can be presumed to make an identical decision under Article 14 / Regulation 19 in respect of any unlawful third party material which a service provider may be found to host. In many cases, it may well be clear whether particular material is unlawful: images of bestiality, for instance, or very clear

[149] Godfrey v. Demon [1999] 4 All E.R. 342.

cases of intellectual property violation – the use of Mickey Mouse in advertisements for a local fast food shop, for instance. However, in very many other instances it will be extremely difficult for a service provider to be sure; especially so with allegedly defamatory material. Demon's settlement payout eventually led to the company being sold; it will be a rare service provider which is willing to take the risk of continuing to carry material which, it is alleged, is unlawful when the alternative might be to face such a settlement or, worse, a heavy defeat in court. Should a service provider take the defensive position of summarily deleting all material about which a complaint has been received, much perfectly lawful content might be deleted, meaning that another party – the content provider – is treated unfairly. This raises also questions of freedom of expression being stifled. Critics of this regime suggest that there is a grave danger of a 'privatised censorship' effect: what if, runs this argument, an individual produces a website which exposes exploitative practices by a large company which relies upon third world sweatshop labour to produce its goods? That company would only have to threaten legal action against the service provider which, unwilling to take the risk of liability, would simply delete the 'defamatory' content which was actually perfectly true. This raises not only the question of fairness to the service provider, but also accountability in the making of such decisions. The great problem with defamation is, of course, that whereas it might be reasonably easy to tell whether a series of photographs could be child pornography or might be obscene, without further knowledge which will often be unavailable to the service provider, there is no way of determining whether material is defamatory. The author's anecdotal conversations with various persons in the UK industry suggest that service providers actually do make some effort to establish the legality of content prior to deletion. Nevertheless, concern about potential liability remains high. There seems no obvious or easy answer to this difficult situation.

In the US, there exists such a statutory awareness-based liability regime, exclusively in relation to copyright infringement. The Digital Millennium Copyright Act 1998 introduced a new Section 512 into the US Copyright Act, providing a series of qualified immunities for internet intermediaries in respect of infringing copies provided by third parties. These immunities, for providers of 'transitory digital network communications', caching and hosting services, although much narrower in terms of the unlawful information to which

they apply, mirror those in the Electronic Commerce Directive sufficiently as to not require further repetition here. An important distinction, between the US and European approaches is the so-called 're-posting provision' contained in Section 512(g) of the Digital Millennium Copyright Act. Under this subsection, an intermediary will face 'no liability for taking down generally' towards any aggrieved party where material has been removed in good faith pursuant to a notice of infringement. An exception to this general rule applies in respect of:

> "...material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice."

In order to take advantage of the immunity in respect of such third party provided material, the intermediary must take reasonable steps to ensure that the subscriber is promptly notified that the material has been removed and comply fully with the steps laid out in section 512(g). Effectively, this subsection provides a right of appeal for the subscriber whose material has been taken down pursuant to a complaint that it infringes copyright. If the subscriber, once notified, follows the correct procedure, the material can be reinstated by the intermediary who is then able to sidestep any further involvement in the dispute. The subscriber, in making the application for re-posting, agrees to meet the full cost of any action taken by another party for breach of copyright where it is found that the subscriber has indeed infringed that right. Such an approach would be an attractive addition to the Electronic Commerce Regulations in the eyes of those who fear that intermediaries will increasingly remove material at any complaint rather than risk liability, potentially removing much which is not unlawful in the process. It is possible that some variation of this approach respecting 'freedom of expression' in a broad sense could be adopted in Europe. This could be applied in respect of intellectual property, but also more widely. It would be a simple matter to apply this to defamation, for instance. This would be a move very likely to be welcomed by service providers, particularly in the UK where the vast majority of the case-law in this area to date has revolved around allegedly defamatory content. Removing the service provider from the picture and thus discouraging any potential for material to be taken down as soon as a complaint is received could address the perceived threat to freedom of

expression. Where the content provider wishes to dispute the claim of defamation in court, this would also be in tune with the general reluctance of the English courts to issue pre-trial injunctions in libel cases save in circumstances where it is so blindingly obvious that the article in question is defamatory that a reasonable defence cannot possibly be mounted.[150]

Obviously, there are some types of criminal material where this approach would be simply unsuitable. Perhaps it might work for, say, Holocaust denial material, but in respect of material which allegedly incites racial or religious hatred, would that really be something that should be risked? Morally, at least, would not a service provider which chose to maintain such material on its servers ahead of a trial be partly culpable if someone were to be the victim of an attack motivated by such material? Any service provider which chose not to delete material which was alleged to be child pornography, or obscene, would at best have a public relations nightmare on its hands when the media inevitably got wind of the story. It is submitted that while a re-posting provision would be a useful device in respect of civil liability, it is wholly unsuited to situations involving material which raises questions of criminal liability.

VI. LIABILITY REGIMES: ONE SIZE FITS ALL?

There is one further dimension to intermediary liability regimes. As is obvious from the above discussion, some States opt for a 'one size fits all' approach, while others prefer to vary the liability model according to the type of content. An example of the latter is the US, which provides a complete immunity for intermediaries from most kinds of civil liability, while in relation to other types of content, most notably copyright under the provisions of the Digital Millennium Copyright Act, an awareness-based regime is in place. In favour of this approach it might be argued that the control of differing types of content may be better served by differing schemes. Even the EU 'one size fits all' regime in the Electronic Commerce Directive must differentiate in practice between the standard of awareness required on the part of service providers in relation to third party content which is unlawful in civil and criminal law. Alternatively, a case might be made for taking a stronger line on the availability of material

[150] *See* D. Goldberg, G. Sutter & I. Walden MEDIA LAW, 423-424 (OUP, 2009).

which breaches privacy, for example, than libel; whereas a reputation can be restored, privacy cannot. Even under the 'one size fits all' regime in the UK, in practice there is a difference in treatment of, say, child pornography with the extra-legal IWF and Cleanfeed initiatives, and libellous material, which has been the basis for the vast majority of litigation involving UK intermediaries.[151]

The distinct problem with such a variable approach is that it is jumbled, and essentially a pick and mix. Differing approaches may overlap and contradict each other. For instance, while the Communications Decency Act's Section 230 does indeed provide a wide immunity from civil liability for ISPs, should a service provider adopt the role of editor over third party content uploaded to its servers, it would run a significantly increased risk of liability for copyright infringement. A court may consider that such editorial activity raises the likelihood of a service provider having sufficient constructive knowledge that it ought to have known of the existence on its servers of, say, a peer to peer website on which infringing copies of protected works are being exchanged.

Writing from a US perspective, Lemley suggests:

> "An ideal safe harbor would take the middle ground approach of the DMCA, but would avoid some of its pitfalls. It would be general rather than specific in its application to Internet intermediaries. It would give plaintiffs the information they needed to find tortfeasors, and would give them a mechanism for quickly and cheaply removing objectionable content from the Web, but it would also discourage intermediaries from automatically siding with the plaintiff, and would give them real immunity against the specter [*sic*] of damages liability."[152]

Lemley's ideal is precisely what the author would posit as, if not the *best* solution to the problematic question of intermediary liability law, certainly the *least worst*. A 'one size fits all' model means that the service provider is presented with a clear set of rules and is more likely to be able to identify the distinct liability issues *post-haste* than a system under which the nature of content must

---

151 See discussion above.

152 Mark A. Lemley, *Rationalizing Internet Safe Harbors*,6 J. TELECOMM. & HIGH. TECH. L.101, (2007); Stanford Public Law Working Paper No. 979836, SSRN.COM, http://ssrn.com/abstract=979836 (last visited Feb. 13, 2011).

first be identified, categorised and only then can they begin to identify the potential liabilities. A single, clear and streamlined system is easier for the service provider to deal with on a utilitarian level. On a more ephemeral level, it may be argued that it is simply 'right' or 'just' that a service provider's liability should be set at the same standard whatever the nature of the unlawful material. After all, the role of the service provider in each case is the same; a service provider which negligently or deliberately allows unlawful material to continue to be available on its servers commits the same fault irrespective of the nature of the content in question. Of course, the penalty for doing so may vary according to the type of content, and of necessity the burden of proof will vary between matters of civil law (e.g. defamation) and matters of criminal law (e.g. child pornography). Nonetheless, a single, streamlined system is easier for intermediaries to grasp and must therefore have a greater chance of success. Of course, as noted in the above discussion, the current European model, as enacted in the UK, requires further modification in order to discourage a situation where intermediaries become over-cautious and simply take down material upon request. The adoption of a 're-posting provision' as per the Digital Millennium Copyright Act into the European system would help to address this, even if it applied only to limited types of content. It would be particularly useful in the UK context in relation to defamatory material as well as alleged infringements of intellectual property. The line should, perhaps, as discussed above be drawn at content which (allegedly) breaches criminal law.

VII. THE BABY BEAR – REALISABLE AIM OR MYTHICAL BEAST?

And so, we return full circle to the opening question: how best to regulate unacceptable content in the online environment? It is clear that simply trying to trace all unlawful material to the source is often practically impossible, whether because the source is untraceable, or has committed no crime at the point of domicile and therefore cannot be extradited. The cultural subjectivity of so much of what any individual jurisdiction regards as 'unacceptable content' is such that this will be a problem ever with us, and global 'minimum standards' are unlikely to be reached to any great degree. Pursuing the end user may be viable in some circumstances; see, for instance, the English law on possession of extreme pornography. In reality, however, this will often simply be no more than cutting off hydra heads, never dealing fully with the problem of unacceptable material being distributed. Thus, we logically arrive at the notion

of controlling material at the level of distribution. Inevitably this involves bringing in the intermediary service provider. There are several approaches to this. First, there is the strict, Father Bear type approach, in which the service provider is in effect made an agent of the State, with obligations to prevent, to block and to filter certain forms of content. This approach is of only limited effect. Blocking software is inevitably subject to a range of technical limitations, not least the lack of capacity to judge the context in which keywords appear as well as the limitations placed in content which does not contain the blocked material but shares a server with material which does. The result is overblocking, with much that does not fall within the category of 'unacceptable material' being blocked. Some States might consider this to be an acceptable sacrifice as against preventing the spread of unacceptable content, but this will pose a problem in States where a high value is placed upon freedom of expression and any regulation which fetters that must clearly be necessary and proportionate in order to prevent what is regarded as a more significant danger. This has been the sticking point in the US in relation to various attempts to oblige the use of blocking and filtering in public libraries, for example, and would be likely to cause a problem were systems such as Cleanfeed in the UK to be expanded to a much broader range of unacceptable content than is currently the case. Already, voluntary systems like Cleanfeed are potentially non-compliant with Article 10, as discussed above, due to lack of clarity and accountability problems. In either case, blocking and filtering systems also raise questions with respect to funding, a matter not to be dismissed lightly.

If such 'Father Bear' approaches are not the answer, what is? It is clear from the experience of the US under the Communications Decency Act, Section 230, that deregulation designed to enable service providers to take an active, editorial role without fear of liability seems to have had the opposite result, in many cases service providers having abandoned any pretence at taking responsibility for the defamatory content made available by third parties on their software, even where specifically aware of identified instances of the same.[153] This 'Mother Bear' approach is clearly too soft.

---

[153] Of course, as discussed above, the complete absence of liability is not the only disincentive to police their servers, as adopting the editorial role could leave the service provider open to liability elsewhere in law, for example, under the provisions of the Digital Millennium Copyright Act.

So what *is* the 'Baby Bear' "just right" option? Is there, in fact, such a thing as "just right", or in reality must we simply settle for what is "least worst"? The awareness-based, 'one-size fits all' model of liability as forms the backbone of intermediary regulation with respect to third party provided content in Europe is rooted in the fundamentally fair notion that a service provider should not be held liable in respect of material over which it has no control, or of which it could not possibly have been expected to have been aware. It is submitted that in principle this is a fine standard: it would seem wholly appropriate for an intermediary service provider which has knowingly been distributing unlawful material to face liability at law for the same – or even, in relation to certain types of material which breaches civil law standards, to do so where a court could be satisfied that the service provider could reasonably have been expected to be aware of the unlawful content. In this respect, the author would contend that much of the discourse in this field over the past few years has in error focussed upon how intermediary liability may be limited; instead, the focus should, it is submitted, be upon whether and in what circumstances it is just and equitable for the intermediary to bear liability. There are, as discussed, several difficulties with the European approach in practice, not least that it will often effectively place the intermediary service provider in the difficult position of deciding whether material is or is not unlawful, with grave liability risks if a wrong call is made. Adopting a US-style re-posting provision in respect of material which has the potential to incur civil liability would assist in this respect, though it is submitted that such an approach, which effectively means that the material can remain available online unless or until declared unlawful by a court, is likely to be unsuitable in respect of illegal content such as obscene materials or child sexual abuse images. It seems likely that some level of State-sanctioned, statute-based blocking system will be put in use in various EU jurisdictions in future. This raises many problems indeed as discussed above, although at least some of these might be pre-empted by moving to an approach of basing the blacklist upon material which has indeed been ruled by a court to be unlawful, or at the very least relying upon the judgement of a specialist law enforcement department rather than putting the IWF in the position of making decisions about illegality. It is, of course, recognised that at least as long as the material covered by such a blocking approach limits its remit to child pornography, it will normally be reasonably obvious whether or not the material is likely to be in breach of the law.

So the Baby Bear approach to legislation, the "just right" approach for our State-as-Goldilocks to adopt as the best means for controlling unacceptable content in the online environment is really more a case of that which is the 'least worst' option. In practice, this is likely to be a mixed bag of both strong, Father Bear regulation and something less invasive, if not quite the soft, Mother Bear approach. Of course, it is also highly unlikely that for so long as the sheer variety of human cultural mores remains at once diverse as it is today and instantaneously globally available across all national boundaries, there will be adopted any one universal approach: 'Baby Bear' will be as different in character around the world as that which constitutes unacceptable material. *Plus ca change, plus la meme chose*!