VOLUME 7

IJLT | The INDIAN JOURNAL of LAW and TECHNOLOGY

2011

IJLT | The INDIAN JOURNAL of LAW and TECHNOLOGY

ISSN 0973-0362 Volume 7
2011

national law school of india university
bangalore

IJLT The INDIAN JOURNAL of LAW and TECHNOLOGY

VOLUME 7 2011

Published by
THE LAW AND TECHNOLOGY COMMITTEE
Student Bar Association, National Law School of India University,
Bangalore, India

Faculty Advisor
Ms. A. Nagarathna
Assistant Professor, National Law School of India University,
Bangalore, India

IJLT The INDIAN JOURNAL of LAW and TECHNOLOGY

VOLUME 7 2011

INFORMATION ABOUT THE JOURNAL

The Indian Journal of Law and Technology (ISSN 0973-0362) is an academic journal, edited and published annually by students of the National Law School of India University, Bangalore, India. All content carried by the Journal is peer-reviewed except for special comments, student articles and editorial notes. The Journal comprises:

- the Board of Advisory Editors, consisting of professionals and academicians pre-eminent in the field of law and technology, which provides strategic guidance to the Journal;
- the Article Review Board, a panel of external peer-reviewers;
- the Editorial Board, consisting of students of the National Law School of India University, which is responsible for selecting and editing all content as well as contributing occasional editorial notes;
- the Law and Technology Committee, again consisting of students of the National Law School of India University, which publishes the Journal and performs secretarial functions.

INFORMATION FOR CONTRIBUTORS

The Indian Journal of Law and Technology seeks to publish articles, book reviews, comments and essays on topics relating to the interface of law and technology, particularly those with a developing world perspective.

- **Mode of Submission**

Submissions can be in electronic form or in hard copy form. However, submissions in electronic form are strongly encouraged in order to expedite the submission review process.

Please address submissions in electronic form to the Chief Editor of the Indian Journal of Law and Technology at "editorialboard@ijlt.in".

Please address hard copies of manuscripts to:

The Chief Editor,
Indian Journal of Law and Technology,
National Law School of India University,
Nagarbhavi, Bangalore 560242, India.

To facilitate the review of submissions in hard copy form, authors are urged to also provide their submissions in electronic form. However, submissions in hard copy form cannot be returned to the authors through post or other means.

Regular Submission Review

The Journal shall communicate an acknowledgement to all authors shortly after the receipt of their submissions. The preliminary review of the submissions shall be completed within four weeks of receipt in usual circumstances. The submissions that are initially accepted shall be blind-refereed by the Article Review Board. The Journal shall make due efforts to complete the entire peer-review process within a reasonable time frame. The Journal shall notify the authors about the exact status of the peer-review process as required.

Expedited Submission Review

This option is available to those authors who have received an offer of publication from another journal for their submissions. The authors may request an expedited submission review. However, the decision to grant an expedited submission review shall remain at the discretion of the Editorial Board. Please note that requests for an expedited submission review can only be made in relation to submissions in electronic form. All such requests must be accompanied by the following details:

- Name(s) of the author(s) and contact details;
- Title of the submission;
- Details about the journal(s) which has/have offered to publish the submission;
- Whether the offer is conditional or unconditional and, if the offer is conditional, then what conditions are required to be met for final acceptance;
- The date(s) on which the offer(s) expire(s).

The Journal shall make due efforts to accommodate the existing offer(s) and applicable deadline(s). However, upon an offer of publication pursuant to the expedited submission review, the authors shall have to communicate their decision within five calendar days of the notification of the offer. If there is no response, then the Journal shall have the discretion to withdraw the offer.

- **Submission Requirements**
  - All manuscripts must be accompanied by:
    (1) a covering letter mentioning the name(s) of the author(s), the title of the submission and appropriate contact details.
    (2) the résumé(s)/curriculum vitae(s) of the author(s).
    (3) an abstract of not more than 200 words describing the submission.
  - All submissions in electronic form should be made in the Microsoft Word file format (.doc) or in the OpenDocument file format (.odt).
  - All text and citations must conform to a comprehensive and uniform system of citation. It is preferred that the system prescribed in THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 19th ed., 2010) or a more recent edition thereof be observed. The Journal employs footnotes as the method of citation.
  - No biographical information or references, including the name(s) of the author(s), affiliation(s) and acknowledgements should be included in the text of the submission, the file name or the document properties. All such information can be provided in the covering letter.
  - The Journal encourages the use of gender-neutral language in submissions.
  - The Journal shall be edited and published according to the orthographical and grammatical rules of Indian English that is based on British English. Therefore, submissions in American English shall be modified accordingly. The Journal encourages authors to use British English in their submissions in order to expedite the editing process.
  - The Journal strongly encourages authors to not exceed 30,000 words (inclusive of footnotes) in their submissions.
  - The authors are required to obtain written permission for the use of any copyrighted material in the submission and communicate the same to the Journal. The copyrighted material could include tables, charts, graphs, illustrations, photographs, etc. according to applicable laws.

DISCLAIMER

PERMISSIONS

The Chief Editor,
The Indian Journal of Law and Technology,
National Law School of India University,
P.O. Box 7201,
Nagarbhavi,
Bangalore 560242,
India.

SUBSCRIPTION INFORMATION

The following procedure should be followed in relation to subscription requests.

- Send a cheque or a demand draft in the name of the "Registrar, National Law School of India University". Send a covering letter accompanying the cheque or the demand draft stating requisite contact details including postal address, telephone number and e-mail address.
- Send an e-mail to "editorialboard@ijlt.in" and "library@nls.ac.in" confirming the subscription request and the subscription payment. The e-mail should also provide the contact details mentioned hereinabove.
- If the subscription payment is received then the subscription shall be confirmed through an e-mail. If no request for back-issues is made, then the subscription shall commence from the forthcoming issue.
- Contact the Managing Editor at "editorialboard@ijlt.in" for inquiries and updates.

- **Annual Subscription Rates (postage included)**

Indian Subscribers

	One Year	Two Years	Three Years
Students	INR100	INR200	INR300
Others	INR200	INR400	INR600

International Subscribers

	One Year	Two Years	Three Years
Students	US$25	US$45	US$55
Others	US$35	US$60	US$80

Please visit the website of the Indian Journal of Law and Technology at "http://www.ijlt.in" to get additional information and to access the archives of previous volumes.

IJLT The INDIAN JOURNAL of LAW and TECHNOLOGY

VOLUME 7 2011

CONTENTS

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
Volume 7, 2011

LIMITATIONS AND EXCEPTIONS IN THE DIGITAL ERA

William Patry[*]

ABSTRACT

Ideological polarization has hijacked copyright debates, drowning out the question: how do we get our copyright laws to do what we want them to do? The term "limitations and exceptions" assumes that the ability to control all unauthorized uses is the norm. This special comment asserts that private rights should never trump public interest, and that our copyright laws must reflect this principle. Copyright law must be grounded in current technological and market conditions in order to accomplish its lofty objectives. Even as changes wrought by digital technology are at the core of most debates over copyright, there is a failure to grasp the profundity of these changes and the challenges they pose. We need dynamic laws in order to encourage creativity on the internet. Properly structured copyright laws would enable desirable behaviour in a world that technology is changing faster than ever before. It is argued that guiding principles such as fair use should be the bases for adjudication and not statutory straitjackets, as is already the case in legal regimes supporting the most advanced technology sectors, in India and the U.S.A. Though legislative and judicial understandings are not always at par in their level of progression, even judicial interpretation in light of broad principles as opposed to a closed list is a step in the right direction because we need transformative laws to regulate the transformative world we live in.

Copyright debates around the world have been hampered by polarizing ideological debates, losing sight of the only relevant question: how do we get our copyright laws to do what we want them to do? We should figure out how we want our copyright laws to work, stripped of rhetoric that tries to shape the end result before we have even begun.

---

[*] Senior Copyright Counsel, Google Inc. Parts of this article will appear in a forthcoming book, How to Fix Copyright (Oxford University Press, Fall 2011).

The term "limitations and exceptions" is just such a rhetorical device, although it seems innocuous enough at first glance. The term assumes a natural state of affairs where the ability to control all unauthorized uses is the norm: limitations and exceptions are limitations and exceptions *from* something after all, and that something is believed to be a world in which exclusive rights are the unfettered ability to exclude others from using the copyrighted work, no matter the social utility of the use.

Of course, all copyright systems allow some unauthorized uses, but the point is that the 'limitations and exceptions' rhetoric attempts to restrict such uses to the minimum and to place a heavy burden on the passage of new ones. Harvard Law School professor Joseph Singer noted this phenomenon in connection with property claims:

> [W]e imagine those limits to be exceptions to the general rule that owners can do whatever they want with their property. The burden is always on others (meaning non-owners or the state) to explain why the owner's rights should be limited, and in today's political climate that burden is heavy.[1]

If ownership means presumptive control by an owner, and if the existence of ownership rights is a good thing, then limitations on the rights of the owner must be justified by sufficiently strong presumptions of legitimacy.[2]

In copyright law, we see this approach in statements that limitations and exceptions will be allowed, only if "there is a public interest ... that justifies overriding the private rights of authors in their works in ... particular circumstances."[3] Private rights should never trump the public interest, and nor should a heavy burden be necessary to enact laws that further the public interest. Laws exist only to further the public interest.

While private rights thoughtfully crafted can be important and further public interest, there is no such thing as copyright rights privately created and privately enforced. Copyright is created by public officials in the government for public

---

1 Joseph Singer, ENTITLEMENT: THE PARADOXES OF PROPERTY 3 (2000).

2 *Id* at 4.

reasons and is enforced by public laws and by public judges. Copyright laws are created as an entire fabric consisting of certain entitlements given to copyright owners, and certain entitlements given to the public. There is no support for treating any one entitlement as more privileged or important than another.

Judge Pierre Leval of the U.S. Court of Appeals for the Second Circuit in Manhattan made this point in talking about the important role of transformative, unlicensed fair uses in furthering the goals of creativity: "Fair use should not be considered a bizarre, occasionally tolerated departure from the grand conception of the copyright monopoly. To the contrary, it is a necessary part of the overall design."[4] The Canadian Supreme Court took the same approach in *CCH Canadian Ltd.* v. *Law Society of Upper Canada*,[5] where Chief Justice McLachlin wrote:

> Before reviewing the scope of the fair dealing exception under the Copyright Act, it is important to clarify some general considerations about exceptions to copyright infringement. Procedurally, a defendant is required to prove that his or her dealing with a work has been fair; however, the fair dealing exception is perhaps more properly understood as an integral part of the Copyright Act than simply a defence. Any act falling within the fair dealing exception will not be an infringement of copyright. The fair dealing exception, like other exceptions in the Copyright Act, is a user's right. In order to maintain the proper balance between the rights of a copyright owner and users' interests, it must not be interpreted restrictively. As Professor Vaver, *supra*, has explained at p. 171: "User rights are not just loopholes. Both owner rights and user rights should therefore be given the fair and balanced reading that befits remedial legislation."[6]

---

3 Sam Ricketson, WIPO Study on Limitations and Exceptions of Copyright Related Rights in the Digital Environment, Standing Committee on Copyright and Related Rights, 9th Sess., Geneva, June 23 to June 27, 2003, SCCR/9/7 (Apr. 5, 2003). It should be noted that Professor Ricketson was referring principally to the civil law tradition. Professor Ricketson's view was challenged by a number of prominent European experts in a July 17, 2008 declaration. Max Planck Institute for Intellectual Property and Competition Law, *A Balanced Interpretation of the 'Three-Step' Test in Copyright Law*, *available at* http://www.ip.mpg.de/ww/en/pub/news/declaration_on_the_three_step_.cfm. (last visited Jul. 24, 2011).

4 Pierre N. Leval, *Toward a Fair Use Standard*, 103 HARV. L. REV. 1105, 1110 (1990).

5 *CCH Canadian Ltd.* v. *Law Society of Upper Canada*, [2004] 1 S.C.R. 339.

6 *Id* at ¶ 48.

If we had only authorized creativity, we would live in a very sterile world: few government figures and few copyright owners are fond of others satirizing them. Few businesses are willing to let competitors thrive rather than try to eliminate them through any means possible, including through misuse of the copyright laws.

At one level asking what we want copyright to do and how to do that in practice sounds silly, since we all know what we want copyright laws to accomplish: to promote creativity and innovation, provide the public access to work and create jobs, to name the major objectives usually cited. These are lofty goals and we should all endorse them as they represent positive contributions to society. However, their loftiness disguises significant flaws: we rarely, if ever, take the time before drafting particular copyright laws to see whether they are capable of accomplishing what we want them to do, and we rarely check after we have passed those laws to see if they lived up to their promise. Instead, we simply pass new laws. Want more works? Extend the term of copyright. Want to stop people from copying? Add more penalties. We don't sit down before and examine whether a term of protection of life of the author plus 70 years will really cause a single work to be created beyond what a term of life of the author, plus 50 years, would not. We do not sit down before and examine whether putting someone in prison for 10 years will cause them not to copy, whereas 5 years in prison would not make them stop. Our laws need to be based on evidence, not rhetoric or ideology.

Part of grounding our laws in evidence is grounding them in current technological and market conditions. Much of the Indian copyright law is 50 years old, although there were amendments in 1994 and 1999.[7] Many of the foundational elements in all of the world's copyright laws are centuries old, and have proven to be highly resistant to adaptation. The biggest failure of adaptation has been in the failure to realize the profound changes wrought by digital technology, even as those challenges are at the core of most current debates over copyright.

---

[7] Indian Copyright Act, 1957, amended by the Copyright (Amendment) Act, 1994 and the Copyright (Amendment) Act, 1999. The Copyright (Amendment) Bill, 2010 has not yet been passed by the Rajya Sabha.

Unlike the analog world of scarcity where the costs of production and distribution of hard copy led to control over copyrighted works by a few, we now live in a world of digital abundance. Laws made for the world of analog scarcity cannot effectively regulate a world of digital abundance. It makes no sense to retain laws written to regulate the turn of the 18th century London book trade, for 21st century global markets. The differences begin with the change in the role of consumers. The passive role formerly assigned to consumers in the analog world no longer holds: at the production level, authors and performers have the opportunity to create a finished product and reach audiences directly, outside of the control of the traditional gatekeepers. Millions of other people around the world can act as their own creators, producers and distributors (via websites and social networks). We live in a world of unparalleled democratic creativity.

Copyright is meant to encourage creativity. You cannnot encourage creativity, though, if you have to first ask permission before you make any reference to another's work, or if you have to first pay lawyers to decide whether you need to ask permission. Internet search engines provide one example of how copyright laws have to adapt to permit conduct we should all agree is desirable. The ability to search for lawfully made images, video, music, and textual content involves making a copy of that content. Search engines crawl the web constantly and make copies of the entire web (unless individual sites are password protected or blocked through the use of simple, readily available software code such as robots.txt.). These pages are then analyzed and ranked; links are provided to a user in response to a query. Search engines often provide a snippet from relevant websites so that users can decide which sites to access, including thumbnails of images. These snippets are similar to library card catalogues and should be exempt under fair use, fair dealing, code-based exemption provisions, or doctrines such as implied consent. The back-end copying of the web – necessary for indexing – must be exempt too in order for consumers to be able to see the snippets in response to their queries. Without that back-end copying, search – which relies on indexing – is impossible.

When you view a webpage, your browser needs to make a local copy of the page on your computer. In order to transfer data across the Internet, data "packets" are sent between Internet service providers' routers. In effect, this

means that the router makes and sends a copy of the "packet" to the next router in the chain, and so on until it reaches its recipient. Email servers must make copies of messages in order to transfer them from sender to recipient. Video streaming sites must temporarily store (cache) and buffer copies or portions of the audiovisual works being streamed in order to present an uninterrupted viewing experience.

These are all socially desirable uses, that not only do not harm the market for copyrighted works, but increase their market by connecting potential purchasers to rights holders. It does not matter whether one calls such uses fair uses, fair dealing, or anything else: what matters is that we indentify the behavior we wish to encourage and then enact laws that enable that behavior. Everything else is a distraction: whether the reproduction right, the making available right, the performance right or any other right, is "implicated," should be a non – issue. Whether this technology or that technology is used, should be irrelevant. Law is an end to a means, not an objective in itself, and copyright laws are similarly situated. They are not an end in themselves, but rather a means to socially desirable behavior. Focusing on behavior, not rights, not entitlements, and not technologies will go a long way toward making our copyright laws effective. Adopting dynamic legal doctrines like fair use, that can quickly respond to changes in behavior, rather than waiting for governments to legislate permitted innovation, is also critical. Static legal rules cannot further dynamic, creative and technological markets.

If our goal is to encourage creativity, we must adapt copyright laws to the actual ways people create now, and to the actual markets now for that creativity. Technology, and the market changes brought by technology, are creating new paths, and require new business models. Dr. Francis Gurry, Director General of the World Intellectual Property Organization, has argued that successful copyright policy has to be based on neutrality to technology and to business models, and should not "preserve business models established under obsolete or moribund technologies."[8]

---

[8] Dr. Francis Gurry, The Future of Copyright, Speech Delivered at the WIPO Blue Sky Conference on Future Directions in Copyright Law, Sydney, Australia (Feb. 25, 2011) *available at* http://www.wipo.int/about-wipo/en/dgo/speeches/dg_blueskyconf_11.html (last visited Jul. 18, 2011).

Yet, ordinary people, using the Internet and digital applications in ordinary ways, are unwittingly engaging in massive copying on a daily basis simply because of the way those technologies function. For good reason, the Internet has been called a giant copying machine, copying, of necessity, every step we take.[9] Copyright laws that make such ordinary, everyday things, acts of infringement, make no sense.

At the same time, and paradoxically, we are fast approaching an era when there will be copyright laws *without* copying. The increasing streaming of works to consumers rather than selling physical media like DVDs or CDs, as well as accessing works stored in the cloud (on someone else's computer servers) rather than owning your own copy, represent significant changes to consumer habits, and open up the possibility for a true global distribution of culture, since streaming and cloud computing are not dependent upon physical stores or national boundaries. They also represent a way for copyright owners to significantly reduce costs of production and distribution and to reach much larger audiences.

In order to make possible the broad, social goals of copyright, we need laws that give courts guiding principles to decide disputes, rather than statutory straitjackets. Straitjackets consist of narrow lists, drawn up by government officials, of which types of (unlicensed) creativity are permitted. The idea that government officials can effectively formulate and execute a creativity – centralized command system in which all permitted uses can be carefully spelled out in advance, is to believe that the Soviet planned economies were a rousing success.

A top – down copyright regime in which creative acts are limited to those few acts the government has by regulation permitted, inhibits, rather than maximizes, cultural democracy. This regrettable approach is, however, the approach currently taken in many countries of the world. Raising the specter of an allegedly dangerous approach, the ominous "U.S. – style fair use", defends the straitjacket, government – approved approach to creativity.

The fair use privilege was originally created in the 18th century by English common law judges, but now has its most well – known home in Section 107

---

9 *See* "Better Than Free," THE TECHNIUM (Jan. 31, 2008), http://www.kk.org/thetechnium/archives/2008/01/better_than_fre.php (last visited Jul. 18, 2011).

of the U.S. Copyright Act.[10] Section 52(1) of the Indian Copyright Act has a similar, although somewhat more limited provision. Israel's fair use provision is the closest to that found in the U.S.

Fair use consists of principles, not rules, and its goal is to ensure that creativity flourishes in the face of overly exuberant exclusive rights. Fair use is not a blank ticket for all unauthorized uses, though; it is instead, a tool to further socially beneficial behavior. Sometimes this means that a plaintiff bringing an infringement claim against an unauthorized user wins and gets to stop that use because fair use is rejected. Sometimes this means that the unauthorized user wins and gets to continue his or her use without permission and without payment because fair use is found. The public always wins.

Fair use determinations are always made on a case – by – case basis because creativity does not come in cookie – cutter forms; creativity is messy and unless the law takes that messiness into account, the law will stifle creativity. Over the centuries, four factors have come to be seen as important to the fair use analysis, but not exclusively so and not all four are always important in every case. The first fair use factor is the nature and purpose of defendant's use. This factor examines how and why the copyrighted work was used. This inquiry helpfully goes beyond the mere fact that a use is unauthorized, and instead drills down into the reasons for the use. The second factor examines the nature of the copyrighted work. Is the plaintiff's work a factual work and of a kind it is typical to quote from or adapt? This factor is relatively unimportant because it is common for factual works to quote from other factual works and for non-factual works (like musical works) to copy from other non-factual works. It is uncommon for a song to copy scientific descriptions from a journal article, but it is common for one musical composition to copy from another musical composition. The third factor looks at how much of the copyrighted work was copied. Did the defendant take only enough of the work to suit his or her legitimate purpose, or did the defendant pig out and take as much as he or she wanted out of laziness?

---

10 The general distinction between an exemption and a privilege is that with an exemption if you fall into a class of people covered by the exemption you are entitled to its benefits. With privileges, there is no class-based entitlement; rather, each person must prove their entitlement on an ad hoc basis. The distinction does not hold in all cases, though.

The fourth fair use factor is concerned with the effect of defendant's work on plaintiff's market for its work. This factor attempts to evaluate whether the use is of a type we wish copyright owners to control. Parody, satire, book reviews, and many educational uses fall outside of areas we want copyright owners to control. Verbatim copying that acts as a substitute for the original is the type of use we want copyright owners to be able to stop, if they choose.

Fair use, with its ability to flexibly adapt to changes in technologies and markets, has permitted innovative companies to offer products and services that would not have been possible in other countries. It is not accidental that U.S. and India (which has a fair use regime as well) are home to the world's most advanced Internet technologies and skilled tech sector employees. Those who speak of encouraging innovation and job creation but insist on "strong" intellectual property laws miss this obvious reality: it is not strong intellectual property laws that have made possible these innovative services, but the opposite: fair use and other legal doctrines (such as implied license) that have been flexibly applied in order to allow technological sector companies to operate effectively.

Critics of the fair use doctrine point to the alleged "open-ended" nature of fair use and assert that it lacks certainty. The term open-ended is used here as a derogatory synonym, as without boundaries or without any guidance; the term open-ended is used to conjure up fears that one simply never knows what a U.S. court might do. Those who take this position do not point to any particular decisions of U.S. courts as going "off the deep-end", as having come to a decision that was reached only because U.S. courts allegedly have unfettered rights to do whatever they want. Instead, the claims are theoretical: "a U.S. court *could* go crazy", a claim that could apply to all courts.

Describing the fair use regime as open – ended in the sense of "anything goes" is inaccurate. As an initial matter, the description ignores that the essentials of copyright infringement actions in all countries – even those vehemently opposed to fair use are equally open – ended. Whether something is unprotectable fact or protectable expression is open-ended in this same sense. Whether one movie or novel infringes another is based on whether the two works are substantially similar, also an open – ended inquiry. Whether the two works are substantially similar in expression depends on how much copyrighted expression

was taken. How much copyrighted expression was taken involves both quantitative and qualitative assessments. Whether an artist's honor or reputation has been harmed by an unauthorized use is as open-ended an inquiry as exists in copyright law, yet European policy makers and copyright owners passionately argue in favor of such inquiries. Fair use inquiries are of exactly the same nature and usually involve the same questions as those open-ended inquiries that routinely take place under European copyright laws. The third fair use factor examines how much of the copyrighted work was taken. This is the exact same inquiry undertaken in the basic infringement analysis. The fourth fair use factor examines the impact of the use on the market for the copyright owner's work. This is the same inquiry undertaken at the damages phase of an infringement analysis. The first fair use factor examines the purpose of the use, which is also relevant for defenses such as parody or satire. The second fair use factor examines the nature of the copyrighted work, which is also relevant in the infringement analysis for determining what protectable expression is and what is not. The differences between the basic infringement analysis and fair use analysis, where they exist at all, are a matter of degree and not kind.

Nor are judges free to do whatever they wish in making fair use determinations. The fair use analysis in Section 107 of the U.S. Copyright Act merely recognizes in the statute the common law fair use doctrine. Section 52(1) of the Indian Copyright Act is to the same effect (even though the statute refers to fair dealing, the Indian courts have used the terms fair dealing and fair use interchangeably, unlike U.K. courts). The common law doctrine of fair use has developed over two centuries of case law, over the course of which it has given rise to a coherent set of principles, found in a number of other national statutes. In practice, U.S. and Indian courts, like all common law courts, are governed by precedent. Hierarchically, decisions of the U.S. Supreme Court govern all lower courts, and decisions of the circuit courts of appeal govern all decisions of trial courts within that circuit. The U.S. Supreme Court has heard a number of fair use cases. I am unaware of a single complaint about how the *results* reached in those cases would be incompatible with international law.[11] The same holds true for decisions of the lower courts.

---

[11] Professor Ruth Okedjii has argued that the indeterminacy and breadth of fair use are inconsistent with the Berne Convention and the TRIPS Agreement *in* Ruth Okediji, *Toward an International Fair Use Doctrine* 39 COLUM. J. TRANSNAT'L L. 75, 117 (2000). However, I do not share this view nor does the reputed Berne scholar Professor Sam Ricketson.

Criticizing a legal doctrine because in some dispute in the future, some court *might* reach a result that some *might* disagree with, misapprehends the rule of law, and is equally a problem in countries that have closed lists, i.e., enumerated lists of permitted uses. Uses not on the list are infringing. Closed lists are defended in part by claiming they provide certainty. The claim of certainty, however, is a myth. Having a closed list is no guarantee that a correct decision will be reached in construing whether a particular use qualifies or not. There is no guarantee that a court in Australia, Canada, or the U.K. interpreting fair dealing statutes will not adopt an interpretation that is too restrictive or too liberal from the standpoint of the legislators who enacted them.

There are a number of other problems with closed lists of permitted uses. First is the inherent problem of legal indeterminancy: lists of enumerated uses require words to specify which uses are permitted. It is very difficult to select words that have the necessary precision so that courts need not interpret and reinterpret them; and potential litigants can easily determine their meaning *before* engaging in desired conduct. Here is an example of a permitted use from a closed list that is ambiguous: "research." Does "research" encompass both commercial and non-commercial research? Does it permit the copying of entire works or only parts, and if the latter, how do you know how much you can copy? Does the exemption apply when the copyright owner has established a market for the work(s) in question, or only when there is no such market? Does the existence of a potential license constitute such a market, and regardless of the terms of the license? Can a party who is entitled to the research privilege hire a third party to do the copying for them? These are only a few of the ambiguities.

The answers to those ambiguities cannot be answered merely by pointing to the presence or absence of "research" on a closed, exhaustive list of privileges. The answers will be given according to other principles, principles not found in the list, but which rather animate all copyright laws: is the use in the broad, social interest? The alleged sharp divide between the approach found closed lists and fair use does not exist when it comes to the type of inquiry judges are required to undertake.

There is, however, a very sharp divide between the flexibility found in fair use and the top-down approach imposed by European Union directives. That

divide greatly inhibits creativity and innovation in the European Union and therefore gives U.S. companies a distinct advantage. As British Prime Minister David Cameron observed in November 2010, while referring to U.S. law and calling for a review of English copyright law: "Over there, they have what are called 'fair-use' provisions, which some people believe gives companies more breathing space to create new products and service... I want to encourage the sort of creative innovation that exists in America"[12] (he could have added India and Israel as well). The irony of course is that fair use was a British invention.

Closed lists must be regularly updated on the penalty of crushing technological or market innovations: no legislature, no matter how careful or insightful, can think of all current uses, much less think of uses, technologies, or markets that are not yet in existence. In the past, technologies and therefore business models, changed slowly. This is no longer the case. The rapid pace of technological innovation brought about by the Internet and digital tools has radically collapsed the time lines for businesses to adapt and therefore for laws that seek to regulate business issues arising on the Internet. Static laws that attempt to establish for all time the rules governing technological and market innovation will impede that innovation. This does not mean the Internet should be without regulation, but it does mean that the nature of the Internet must be taken into account when framing regulations for it.

A principal attribute of the Internet is its unplanned, distributed nature, with distributed here meaning multiple autonomous computers and software interacting without a central command. The lack of a central plan and command has made the spectacular growth of the Internet possible, and it is what makes the creativity on the Internet so exciting too: creativity is now something we all can engage in, without regard to borders and without having to go through gatekeepers. Creativity is no longer a central command activity; it is dynamic. Being dynamic, if we want to encourage the new creativity, we need dynamic, flexible laws.

The flexibility of fair use is particularly suited for inherently dynamic situations. Closed lists are particularly suited for static situations. We should

---

12 "UK Copyright Laws to be Reviewed, Announces Cameron", BBC, http://www.bbc.co.uk/news/uk-politics-11695416 (last visited Jul. 18, 2011).

not choose between these two approaches since they address very different fact situations. We need fair use because there are many situations that are dynamic. You cannot legislate detailed rules to decide dynamic situations; you can only set forth guiding principles. Fair use is precisely such a set of principles, principles that have been tested in the forge of thousands of court cases and opinions. Fair use works in dynamic situations because dynamic situations require dynamic legal principles.

Culture is usually dynamic; we may have established, canonical works, but at one time they were not canonical: they were the new works on the block. All new works either build on works of the past or are understood in context with the present and the past in a dynamic relationship. If we want to further culture, we need dynamic laws. Dynamic laws tailored to the dynamic nature of creativity do not mean an absence of guidelines. First of all, there are some fairly static situations, situations with identifiable fact patterns. For example, where a consumer buys a lawfully made hard copy of a book, the consumer should be able to subsequently give away or sell that copy. Or, where a newspaper is reviewing a book, the reviewer should be able to quote from the book to explain points made in the review. In such situations, concrete exemptions, whether contained on a list or otherwise, are desirable. Where we can identify recurring problems, we should provide specific guidance.

But static fact patterns are not the norm in copyright because of the dynamic nature of creativity, technology and markets. At the same time that copyright is touted as leading to innovation – which is inherently dynamic – the uses necessary to allow such innovation are foreclosed by static, closed lists of permitted uses. It is not at all coincidental that vested rights holders interests favour closed lists while innovative Internet companies favour fair use. As Dr. Francis Gurry cautioned, "Copyright should be about promoting cultural dynamism, not preserving or promoting vested business interests."[13]

The current provisions in Section 52(1) of the Indian Copyright Act provide a list of statutory defenses. As in the U.S., which has a fair use defense in Section 107, followed by a series of exemptions and statutory licenses in Sections 108

---

13 Gurry, *supra* note 8.

through 122, there are also numerous exemptions in the remainder of Section 52 and in Section 52A. Indian legislators have proposed amendments that seem positive. In particular, the proposal for a consolidated fair dealing provision, extending it to "any work", rather than, as present, only to literary, dramatic, musical or artistic works, is indeed welcome, as is the liberalizing of the news reporting defense. At the same time, the Indian statute and proposals lack, in my opinion, the more flexible approach found in U.S. fair use and permitted by the Berne three-step test. In this respect, Indian courts appear to be ahead of U.S. courts, citing Judge Leval's article on transformative uses.[14] For example, in *Chancellors, Masters and Scholars of Oxford University* v. *Narendera Publishing House*,[15] the High Court of Delhi wrote:

> 32. Copyright law is premised on the promotion of creativity through sufficient protection. On the other hand, various exemptions and doctrines in copyright law, whether statutorily embedded or judicially innovated, recognize the equally compelling need to promote creative activity and ensure that the privileges granted by copyright do not stifle dissemination of information. Two doctrines that could immediately be summoned are the idea-expression dichotomy and the doctrine of fair use or fair dealing. Public interest in the free flow of information is ensured through the idea-expression dichotomy, which ensures that no copyright is granted in ideas, facts or information. This creates a public pool of information and idea from which everyone can draw. At the same time, as Judge Leval observes, all creativity is in part derivative, in that, no creativity is completely original; each advance stands on building blocks fashioned by prior thinkers (Bernard Shaw expressed it by saying that Shakespeare was a tall man, but he (Shaw) was taller as he stood on Shakespeare's shoulders). Judge Leval further observed that most important areas of intellectual creativity like philosophy, literature and sciences are referential, and require continuous re-examination of existing theses.
>
> 33. The doctrine of fair use then, legitimizes the reproduction of a copyrightable work. Coupled with a limited copyright term, it

---

14 Leval, *supra* note 4.

15 *Chancellors, Masters and Scholars of Oxford University* v. *Narendera Publishing House* 2008 (106) D.R.J. 482.

> guarantees not only a public pool of ideas and information, but also a vibrant public domain in expression, from which an individual can draw as well as replenish. Fair use provisions, then must be interpreted so as to strike a balance between the exclusive rights granted to the copyright holder, and the often competing interest of enriching the public domain. Section 52 therefore cannot be interpreted to stifle creativity, and the same time must discourage blatant plagiarism. It, therefore, must receive a liberal construction in harmony with the objectives of copyright law. Section 52 of the Act only details the broad heads, use under which would not amount to infringement. Resort, must, therefore be made to the principles enunciated by the courts to identify fair use.

The judgment in *Narendera Publishing* is not an outlier, and in common law tradition, is built on previous Indian High Court decisions, including *Syndicate of the Press of the University of Cambridge* v. *B.D. Bhandari*,[16] *Civic Chandran* v. *Ammini Amma*,[17] and *Blackwood & Sons* v. *A N Parasuraman*.[18] These cases illustrate that it is not the name given to a provision, but rather its purpose and application.

The Parliament could further these developments by amending Section 52(1) by adding the following provision

(iv) other uses, including transformative uses, that do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the rights holder.

This provision would be consistent with India's international obligations, India's own case law, and the efforts of forward thinking judges like Judge Leval and Chief Justice McLachlin. We live in a transformative world and need transformative laws.

---

16 *Syndicate of the Press of the University of Cambridge* v. *B.D. Bhandari*, M.I.P.R. 2009 (2) 60.

17 *Civic Chandran* v. *Ammini Amma*, 1996 (16) P.T.C. 670 (Kerala High Court).

18 *Blackwood & Sons* v. *A N Parasuraman*, A.I.R. 1959 Mad 4.

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
VOLUME 7, 2011

BIAS IN SEARCH RESULTS?: DIAGNOSIS AND RESPONSE

Benjamin Edelman *

ABSTRACT

The author explores allegations of search engine bias, including understanding a search engine's incentives to bias results, identifying possible forms of bias, and evaluating methods of verifying whether bias in fact occurs. He then considers possible legal and policy responses, and assesses search engines' likely defences. He concludes that regulatory intervention is justified in light of the importance of search engines in referring users to all manner of other sites, and in light of striking market concentration among search engines.

TABLE OF CONTENTS

---

* The author is an Assistant Professor at Harvard Business School. His consulting clients include various companies with interests adverse to Google; selected clients are detailed at www.benedelman.org/bio. His research and publications are indexed at www.benedelman.org.

I. INTRODUCTION

The essence of a search engine is the selection of a series of links responsive to a user's request. However, the web offers billions of pages, and even an obscure query often uses words mentioned in hundreds or thousands of pages. Meanwhile, pages compete for top positions where they can enjoy the most clicks and, for commercial sites, the most purchases. To decide which links to feature, it is widely understood that search engines build an index of page contents and use proprietary algorithms to match user requests to pages from the index. On the most charitable view, a well-designed fully-automated index and search algorithm select those search results that are most relevant to a user's request. But a growing undercurrent questions whether search results are in fact chosen optimally and evenhandedly. Might a search engine sometimes elect to favor links to its own sites and its partners' sites? Or disfavour sites in some way adverse to the search engine's interests, perhaps current or prospective competitors? How would users know if search results suffered from any of these biases?

This paper proceeds in four parts. First, I identify the incentives that might push a search engine to favour and disfavour certain results. Second, I propose mechanisms to identify bias. Third, I sketch possible claims and defenses, assessing the ability of litigation and regulation to shape search results. Finally, I present possible remedies to blunt alleged bias while minimizing the intrusiveness of regulatory intervention.

Let me pause at the outset to note that my analysis focuses largely on Google. I choose this focus for two reasons. First, while Google widely claims that its algorithmic results are "algorithmically-generated",[1] "objective",[2] and "never

---

1 *Technology Overview*, GOOGLE, http://www.google.com/corporate/tech.html.

2 *Our Philosophy*, GOOGLE, http://www.google.com/intl/en/corporate/tenthings.html.

manipulated"[3]; other search engines make such claims rarely or never. Second, Google's dominant market share (presently estimated at 66% of U.S. core searches, and 95%+ in many European countries) means that any bias at Google has a much larger impact than bias at another search engine. In short, Google alone has the power to make or break a site – and Google alone has promised not to abuse that power.

II. THE MARKET FOR WEB SEARCH AND THE THREAT OF BIAS

Web search is notable in part for the value of the leads it can provide to users. Whereas news sites reach users as they follow world events and social networking sites reach users communicating with friends, web search reaches users as they seek information and, often, plan purchases. Web sites therefore place a particularly high value on referrals from search.

For more than a decade, leading search engines have combined both paid and unpaid results. Paid results, typically at screen top and right, are allocated through a bidding process, and advertisers are typically charged for each click from search results through to an advertiser's destination. Unpaid results, typically appearing at the left side of a search results screen, are understood to come from search engine's indexing of all manner of sites.

In both paid and unpaid results, search engines retain substantial discretion to select which listings to present and in which order. Various critics have alleged that search engines use this discretion improperly.[4] Indeed, Google co-founders Sergey Brin and Larry Page argued in 1998 that "advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers", which led them to conclude that it is "crucial" for a search engine to be "transparent".[5] Despite the co-founders' early concern about search bias, Google has more recently faced all manner of allegations of impropriety in search results. Consider three recent complaints:

---

3 *Id.*

4 Among the earliest to flag this concern were L. Introna and H. Nissenbaum, *Shaping the Web: Why the Politics of Search Engines Matters*, 16(3) THE INFORMATION SOCIETY, 1-17 (2000).

5 Sergey Brin and Larry Page. *The Anatomy of a Large-Scale Hypertextual Web Search Engine*, http://www7.scu.edu.au/1921/com1921.html.

- In a search for "network neutrality", Google allegedly grants more favorable positions to sites that favour network neutrality than to sites presenting an opposing view.[6] Separately, Google's management and public policy staff have spoken in favour of network neutrality.[7] By promoting listings consistent with Google's corporate position, Google allegedly builds support for the policy it favors.
- In searches for restaurant reviews (e.g. "best burrito boston"), Google's newly-introduced Places service claims substantial (allegedly, excessive) on-screen space and multiple listings. In contrast, sites that specialize in storing and analyzing restaurant reviews – Yelp and Chowhound, among others – find their links less prominent. By sending users to Google's own local search service rather than competitors, Google builds traffic to its own offering, to competitors' dismay.[8]
- In searches for industrial supplies, users rarely receive algorithmic links to the business-to-business "vertical search" site TradeComet. Furthermore, Google allegedly refuses to sell advertisements to TradeComet on the same terms Google offers to others. By denying traffic to a would-be competitor (offering an alternative search engine and alternative ad platform), Google protects its established search engine and advertising system.[9]

Each of these allegations is, to date, substantially unproven – at least as to Google's intentions, and arguably as to at least a portion of the underlying acts.

---

6 Frank Pasquale, *Federal Search Commission? Access, Fairness, and Accountability in the Law of Search*, 93 Cornell Law Review 1185(2007). In my tests on January 17, 2011, searching for "network neutrality" at Google, five of Google's nine first-page algorithmic search results took positions strongly in favor of network neutrality (pages at savetheinternet.com, publicknowledge.org, googlepublicpolicy.blogspot.com, freepress.net, and commoncause.org), and four took mixed positions (wikipedia.org, wisegeek.com, nytimes.com, and timwu.org). Google's results also included two videos, both of which presented arguments in favor of network neutrality. No result took a position firmly against network neutrality.

7 Richard Whitt, *What Do We Mean by 'Net Neutrality'?*, Google Public Policy Blog, (June 16, 2007), http://googlepublicpolicy.blogspot.com/2007/06/what-do-we-mean-by-net-neutrality.html. ("Without nondiscrimination safeguards that preserve an environment of network neutrality, the Internet could be shaped in ways that only serve the interests of broadband carriers, rather than U.S. consumers and Web entrepreneurs.").

8 Amir Efrati, *Rivals Say Google Plays Favorites*, Wall Street Journal, December 12, 2010. (Quoting Yelp CEO Jeremy Stoppelman complaining that Google "is trying to leverage its distribution power" over search results.)

9 TradeComet.Com LLC v. Google, Inc., S.D.NY Case No 1:2009cv01400 (2009).

(Indeed, only the third is currently the subject of litigation.) Yet each allegation tells a cogent story – not just identifying practices consistent with initial attempts at verification, but also identifying how such behavior serves Google's interests.

Furthermore, each of these allegations typifies a broader class of concerns. Network neutrality is just one of scores of issues about which Google, both as a company and through its leaders' well-known opinions, holds a distinctive corporate view. (Consider climate change, Internet filtering in China, and US presidential politics.) Just as Google Places enjoys prominent space within Google's results, so too does Google grant abundant space to Google Maps,[10] Google Product Search,[11] and YouTube[12]; in addition, Google sometimes gives its own services distinctive benefits no one else can enjoy, such as guaranteed top-of-page placement for Health and Finance[13] and the exclusive ability to show images in paid search advertisements.[14] And TradeComet's allegations follow complaints from Foundem,[15] My Triggers,[16] and Search King[17] – each alleging that their algorithmic links became less prominent and/or that their advertising prices increased dramatically, a concern subsequently echoed by better-known sites such as Expedia and Kayak.[18]

---

10 *Traffic Report: How Google Is Squeezing Out Competitors and Muscling Into New Markets* INSIDE GOOGLE (June 2, 2010), http://www.consumerwatchdog.org/resources/TrafficStudy-Google.pdf.

11 Philip Segal, comment on Danny Sullivan, *Study: Google 'Favors' Itself Only 19% Of The Time*, SEARCH ENGINE LAND, (January 19, 2011), http://searchengineland.com/survey-google-favors-itself-only-19-of-the-time-61675.

12 Frank Reed, *Is Google Bowing to Pressure to Show More Competitive Offerings?*, MARKETING PILGRIM, http://www.marketingpilgrim.com/2011/01/is-google-bowing-to-pressure-to-show-more-competitive-offerings.html.

13 Benjamin Edelman, *Hard-Coding Bias in Google 'Algorithmic' Search Results* (November 15, 2010), http://www.benedelman.org/hardcoding/.

14 Benjamin Edelman, *Tying Google Affiliate Network* (September 28, 2010), http://www.benedelman.org/news/092810-1.html.

15 *Foundem's Google Story*, SEARCHNEUTRALITY.ORG (August 18, 2009), http://www.searchneutrality.org/foundem-google-story.

16 Answer and Counterclaim of Defendant Mytriggers.com, Inc., *Google, Inc., v. myTriggers.com, Inc.*, Case No. 09 CVH-10-14836 (Oh.).

17 Search King v. Google Technology, Inc. Case No. Civ-02-1457-M (W.D. Okla., 2003).

18 *Online Travel and Technology Companies Launch FairSearch.org Coalition, Urge Justice Department to Challenge Google-ITA Deal*, FAIR SEARCH (October 26, 2010), http://www.fairsearch.org/wp-content/uploads/2010/10/FairSearch.org-Coalition-Urges-DOJ-To-Challenge-Google-ITA-Deal_10-26-10.pdf.

III. IDENTIFYING BIAS

While the preceding section presents a series of allegations of bias, each allegation leaves room for doubt. Perhaps a Google search for "network neutrality" links to sites favoring that policy because such sites are more numerous or better designed (in a way that Google's crawlers assess more favorably), or perhaps sites presenting a contrary view tend to use other terms. Perhaps Google's search listings are in some important sense more useful without TradeComet's links. More generally, any notion of "bias" requires a notion of a baseline, yet it is less than obvious where to look for a basis of comparison.

A. Comparing Results Across Search Engines

In principle, a comparison between search engines could offer insight into bias. Each difference might result from innovation (one search engine finding ways to improve on the others' approach), ordinary innocuous diversity (search engines randomly linking to differing sites), or bias. But where a difference reflects a targeted removal of a site or class of sites, and where the removed sites seem to be favourably received by users (as evidenced in site usage, click patterns, visit duration upon arriving at a site, and more), there is greater cause to suspect the removal is for ulterior motives. So too if one search engine links to its own services more often than other search engines link to its services. Ben Lockwood and I recently ran such comparisons, finding that Google links to its services more often than other search engines do so.[19] An enlarged version of this test, covering more search terms and running on an ongoing basis, could uncover all manner of other anomalies.

Despite the promise of comparisons across search engines, this approach suffers important limitations. If one site were found to be missing from Google (and only Google), a few weeks after publicly criticizing some aspect of Google's practices, it might be reasonable to infer that Google had singled out that site for a penalty. But suppose Google instead removed links to a class of sites, dozens or hundreds, that share some characteristic Google characterizes as objectionable. The suggestion is more than speculative: Google has defended its removal of

---

[19] Benjamin Edelman and Benjamin Lockwood, *Measuring Bias in 'Organic' Web Search* (January 19, 2011), http://www.benedelman.org/searchbias/.

links to TradeComet and Foundem by arguing that their sites were not useful and duplicated content elsewhere on the web, suggesting that Google removed their links for good cause.[20]

B. Comparing Results Over Time

A comparison could also focus on changes over time, building on the assumption that any given bias likely had a start date and that the installation of that bias thus causes a change in search results. Of sites alleging bias, many report a *sudden* change in search results.[21] Allegations grounded in change over time are more persuasive when a site suffers multiple losses simultaneously (e.g. a drop in algorithmic search prominence as well as an increase in minimum bids for advertisement purchases). And sometimes such allegations come from sites that are both popular and well-known (e.g. Yelp), circumstances that tend to make it all the more puzzling when their links disappear.

Yet inferences based on change over time also suffer from important limits. For one, changing circumstances threaten the assumption that a site's listings should remain equally prominent - conditions may change, yielding an appropriate reduction in a site's prominence. Even well-known sites can become less appealing to users and, hence, properly made less prominent in search results. Furthermore, if a search engine uncovers a site engaged in some form of impropriety – perhaps using trickery to artificially inflate its apparent importance – a penalty might be appropriate, and such a penalty would ordinarily entail a large drop in rakings. Finally, if change over time were the hallmark of bias, a concerned search engine could design its systems to make changes more slowly – achieving a similar level of bias without suspicious sudden changes.

C. Comparing Across Searches

Occasionally, anomalies in search results may reveal biased rankings. Searches and results are available for free and immediate public inspection by

---

20 Don Harrison, *Texas Inquires on Our Approach to Competition*, Google Public Policy Blog (September 3, 2010), http://googlepublicpolicy.blogspot.com/2010/09/texas-inquires-on-our-approach-to.html.

21 *See, e.g.* Richard Waters, *Unrest Over Google's Secret Formula*, Financial Times, July 11, 2010. (Quoting website Technorati claiming it had "certainly [been] penalized" by Google when its search rankings "tumbled" on multiple occasions.) *See also Foundem's Google Story*, *supra* note 15 (showing dramatic drops in ranking and quality score).

anyone interested, and some combinations may reveal behaviour that supports an inference of bias or other impropriety.

In a recent article,[22] I presented a set of searches and results that, I argued, reveal Google intentionally and systematically putting its own services in undeservedly prominent locations. First, I pointed out that adding a trailing comma to a given search (e.g. searching for "car," rather than just "car") ordinarily yields no change in algorithmic search results. But I showed an important exception to that rule: certain searches yield Google results in exceptionally prominent image-enhanced top-of-page listings, yet the same searches with trailing commas omit those Google results altogether (not merely moving them down a few spots, but rather removing them completely). What technical underpinnings would yield that combination of behaviours? I argued that the best explanation is that Google intentionally "hard-coded" its systems to assure that they link to Google services in the highly-valued top position for selected keywords. But Google failed to hard-code close variations of affected searches, and I argued that this omission reveals that these prominent own-service results come not from Google's core search algorithms but from a separate set of manual overrides.

My hard-coding article addresses just a few classes of search terms. I know of no other articles that attempt to infer bias from patterns in a combination of searches and their respective results. Indeed, for bias embodied in boosted assessments of some sites' overall importance or reduced assessment of others, comparisons across searches probably would not flag any impropriety. But when search bias is implemented by changing a search engine's algorithms, imperfect changes – changing only a portion of the algorithm – can leave anomalies of the form I identified in my hard-coding article.

D. Allegations Grounded in Competition and Market Structure

A final class of inferences draws on competition and incentives, often combining this analysis with the data sources suggested in preceding sections. The key insight is that a search engine has a particularly clear incentive to penalize certain kinds of sites (competitors and prospective competitors) and to

---

[22] Benjamin Edelman, *supra* note 13.

reward certain other sites (its own services and, perhaps, partners). Awareness of these incentives could inform evaluation of bias: all else being equal, an allegation of bias is more persuasive if there is an articulable rationale for a search engine to impose such bias.

One impediment to this approach is that it may be difficult to determine which alleged incentives are actually plausible. In 2009, it might have strained credibility to argue that Google competed with Yelp and Groupon. Yet by late 2010, Google's Places service supplanted Yelp results for numerous search terms;[23] and in January 2011, Google acknowledged a forthcoming Offers service matching Groupon's large discounts and daily email.[24] That said, as soon as Google announced its plan for these services, the incentive for bias was apparent. If competitors subsequently and suddenly drop to less prominent positions in search results, it would be little reach to infer that Google's new aspirations drove those drops.

IV. CLAIMS AND DEFENSES

Making allegations grounded in the theories presented in the prior section, various companies have attempted litigation against Google as to Google's removal or deprioritization of their links. Pasquale presents their claims in detail,[25] while Grimmelmann questions whether such claims are compelling either in theory or at law.[26] I do not attempt to revisit claims and defenses in full; it suffices for present purposes to sketch the essence of the arguments.

Complaints from advertisers would most naturally arise out of Google's contractual obligations to advertisers. But Google's form contract[27] is squarely to Google's advantage. Among other provisions, Google purports to retain unfettered discretion to place an advertiser's listings on whatever sites Google chooses in whatever sequence Google chooses, or alternatively not to show an advertiser's

---

23 Amir Efrati, *supra* note 8.

24 Ben Parr, *Google to Launch Groupon Competitor* MASHABLE, http://mashable.com/2011/01/20/google-offers/.

25 Frank Pasquale, *supra* note 6 at 1188 to 1206.

26 James Grimmelmann, *Some Skepticism About Search Neutrality*, *in* THE NEXT DIGITAL DECADE 435, 435-439 (2011).

27 *Google AdWords Terms and Conditions*, GOOGLE, https://adwords.google.com/select/tsandcsfinder.

ads at all (a right that lets Google in turn demand a higher payment from an affected advertiser, on pain of ceasing to show the advertisement anywhere). A claim in contract would seem to require establishing the unenforceability or other inapplicability of the strong language Google so capably drafted.

Lacking a contractual relationship with Google, ordinary web sites dissatisfied with algorithmic traffic and rankings cannot sue in contract. Instead, their claims typically sound in tort, alleging interference with prospective economic advantage.[28] But as Pasquale argues,[29] it is no small feat to reconcile a claim of search engine bias with centuries of tort law: it is less than obvious how to fit Google's duty to web sites into the framework tort law seeks.

In litigation, Google has repeatedly invoked First Amendment rights against compelled speech – arguing that it must not be forced to link to particular sites plaintiffs believe have been rated unfairly.[30] This argument has proven influential in that at least two courts have ruled in Google's favour on this point.[31] Yet gaps are apparent. For one, Google has also argued that the Digital Millennium Copyright Act and Communications Decency Act immunize Google from tort and copyright theory; Google argues that the underlying web site, and not Google, is the speaker of the information at issue. It is paradoxical for Google to be the speaker for the purposes of enjoying First Amendment protections, yet not for purposes of tort and copyright claims. A similar tension appears in Google simultaneously arguing that search results are "Google's opinion"[32] (which, Google argues, triggers heightened First Amendment protections) while Google also claims its results are "algorithmically-generated", "objective", and "never manipulated"[33] (seemingly making the results more factual and further from First Amendment purposes). Meanwhile, the commerciality of Google's search results suggests, at the very least, a lesser level of First Amendment protection.[34]

---

28 Langdon v. Google, 2007 WL 530156 (D.Del. 2007). *See also* KinderStart v. Google, Case No. C 06-2057 (N.D.Cal. 2006). *See also Search King*, *supra* note 17.

29 Frank Pasquale, *supra* note 6 at 1207.

30 *Langdon*, *supra* note 28. *See also Search King*, *supra* note 17.

31 *See* note 30.

32 Defendant Google's Reply Memorandum in Support of Motion to Dismiss the First Amended Complaint. *Kinderstart v. Google*, *supra* note 28.

33 *See* notes 1 through 3.

34 Frank Pasquale, *supra* note 6 at 1195.

In principle, users might challenge apparent inconsistencies between Google's statements and its practices as to objectivity of search results. If it could be shown that Google delivers a level of objectivity less than it promised, consumers might plausibly allege that they were misled by the untrue promises. Because Google prominently and repeatedly claims to offer objective results, consumers presumptively rely on these claims. Consumers' direct damages are less clear, but given Google's direct profits from users' visits and searches, restitution damages could be substantial.

Considering possible claims against search engines, Pasquale concludes that only antitrust law can adequately address search bias.[35] Yet the laissez-faire instinct is strong – not only among legal academics[36] but also among industry experts[37] and the trade press.[38] And Google claims that regulation of its algorithms would discourage search engines from innovating while also inviting spammers to game the system.[39] Could any plausible remedy achieve reasonable policy interests while avoiding the pitfalls so many seem to anticipate? I turn to that question in the next section.

V. TOWARDS REMEDIES BOTH EFFECTIVE AND LIMITED

A search industry news site recently questioned the wisdom of investigating search bias by arguing that, even if bias were uncovered, "it's not clear what any remedy would be."[40] Certainly some heavy-handed remedies would be both impractical and ill-advised. Titling a recent paper "Federal Search Commission", Pasquale ends the title with a crucial question mark – flagging the immediate shortfalls of an overly bureaucratic approach. And Google's caricature of

---

35 Frank Pasquale, *supra* note 6 at 1207-1209.

36 *See, e.g.* James Grimmelmann, *supra* note 26. *See also* Geoffrey Manne, *The Problem of Search Engines as Essential Facilities: An Economic & Legal Assessment in* THE NEXT DIGITAL DECADE 419, 419-434 (2011).

37 *See, e.g. Danny* Sullivan, *The Incredible Stupidity Of Investigating Google For Acting Like A Search Engine*, SEARCH ENGINE LAND (November 30, 2010), http://searchengineland.com/the-incredible-stupidity-of-investigating-google-for-acting-like-a-search-engine-57268.

38 *See, e.g.* Kaila Colbin, *Choice Architecture: Why Search Can't Be Totally Objective*, MEDIA POST (July 20, 2010), http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=132290.

39 Marissa Mayer, *Do Not Neutralise the Web's Endless Search*, FINANCIAL TIMES, July 14, 2010.

40 Greg Sterling, *Deconstructing 'Search Neutrality*, SEARCH ENGINE LAND (January 19, 2011), http://searchengineland.com/deconstructing-search-neutrality-61614.

regulation warns of government-mandated homogeneous results and unblockable web spam,[41] suggesting that regulation of search is intrusive and undesirable.

In this section I sketch a competing vision for policy intervention – suggesting remedies to address the improprieties an investigation might plausibly uncover, while avoiding unnecessary restrictions on search engines' activities.

A. Experience from Airline Reservation Systems: Avoiding Improper Ranking Factors

A first insight comes from recognizing that regulators have already – successfully! – addressed the problem of bias in information services. One key area of intervention was customer reservation systems (CRS's), the computer networks that let travel agents see flight availability and pricing for various major airlines. Three decades ago, when CRS's were largely owned by the various airlines, some airlines favored their own flights. For example, when a travel agent searched for flights through Apollo, a CRS then owned by United Airlines, United flights would come up first – even if other carriers offered lower prices or nonstop service. The Department of Justice intervened, culminating in rules prohibiting any CRS owned by an airline from ordering listings "us[ing] any factors directly or indirectly relating to carrier identity" (14 CFR 255). Certainly one could argue that the rule was ill-advised: a travel agent was always free to find a different CRS, and further additional searches could have uncovered alternative flights. Yet most travel agents hesitated to switch CRS's, and extra searches would be both time-consuming and error-prone. Prohibiting biased listings was the better approach.

The same principle applies in the context of web search. On this theory, Google ought not to rank results by any metric that distinctively favours Google. Certainly, web search considers myriad web sites and pages – far more than the number of airlines, flights, or fares. And web search indisputably considers more attributes of each web page – not just airfare price, transit time, and number of

41 Marissa Mayer, *supra* note 39.

stops. But these differences only grant a search engine that much more room to innovate. These differences do not change the underlying reasoning, so compelling in the CRS context, that a system provider must not design its rules to systematically put itself first.

I credit that some metrics might incidentally favour Google even as they are, on their face, neutral. But periodic oversight by a special master (or similar arbiter) could accept allegations of such metrics; both in the US and in Europe, a similar approach oversaw disputes as to what documentation Microsoft made available to those wishing to interoperate with Microsoft software.

B. Evaluating Manual Ranking Adjustments through Compulsory Disclosures

An alternative approach to avoiding improper ranking factors would require disclosure of all manual adjustments to search results. Whenever Google adjusts individual results, rather than selecting results through algorithmic rules of general applicability, the fact of that adjustment would be reported to a special master or similar authority, along with the affected site, duration, reason, and specific person authorizing the change. The special master would review these notifications and, where warranted, seek further information from relevant staff as well as from affected sites.

Why the concern at ad hoc ranking adjustments? Manual modifications are a particularly clear area for abuse – a natural way for Google to penalize a competitor or critic. Discourage such penalties by increasing their complexity and difficulty for Google, and Google's use of such penalties would decrease.

I credit that Google would respond to the proposed disclosure requirement by reducing the frequency of manual adjustments. But that's exactly the point: results that do not flow from an algorithmic rule of general applicability are, by hypothesis, ad hoc. Where Google elects to use such methods, its market share demands outside review.

Grimmelmann argues that these ad hoc result adjustments are a "distraction".[42] But if Google's manual adjustments ultimately prove to be

---

42 James Grimmelmann, *supra* note 26.

nothing more than penalties to spammers, then regulators will naturally turn their attention elsewhere. Meanwhile, by forcing Google to impose penalties through general algorithms rather than quick manual adjustments, Google will face increased burdens in establishing such penalties – more code required and, crucially, greater likelihood of an email or meeting agenda revealing Google's genuine intent.

C. Experience from Browser Choice: Swapping "Integrated" Components

Many complaints about search bias arise when longstanding innovative services are, or appear to be at risk of getting, subsumed into Google's own offerings. No ordinary algorithmic link to Mapquest can compete with an oversized multicolor miniature Google Maps display appearing inline within search results. (And, as Consumer Watchdog documented, Mapquest's traffic dropped sharply when Google deployed inline maps.[43])

On one hand it is troubling to see established firms disappear in the face of a seemingly insurmountable Google advantage. The concern is all the greater when Google's advantage comes not from intrinsic product quality but from bundling and defaults. After all, if Google can use search to push users to its Maps product, Maps will gain market share even if competitors' services are, on their merits, superior.

Yet it would be untenable to ask Google to disavow new businesses. It is hard to imagine a modern search engine without maps, news, or local search (among other functions largely absent from core search a decade ago). If legal intervention prevented Google from entering these fields, users might lose the useful functions that stem from integration between seemingly disparate services.

What remedy could offer a fair chance of multiple surviving vendors (with attendant benefits to consumers), while still letting Google offer new vertical search services when it so chooses? E.C. antitrust litigation against Microsoft is squarely on point, requiring Microsoft to display a large choice screen that prompts users to pick a web browser. An initial listing presents the five market-leading options, while seven more are available if a user scrolls. But there is no default; a user must affirmatively choose one of the various options.

---

43 *Traffic Report*, *supra* note 10.

Taking the "browser choice" concept to search results, each vertical search service could, in principle, come from a different vendor. If a user prefers that her Google algorithmic search present embedded maps from Mapquest along with local search from Yelp and video search from Hulu, the user could configure browser preferences accordingly. Furthermore, a user could make such choices on a just-in-time basis. (A possible prompt: "We noticed you're looking for a map, and there are five vendors to choose from. Please choose a logo below.") Later, an unobtrusive drop-down could allow adjustments. The technical barriers are reasonable: external objects could be integrated through client-side JavaScript, just as many sites already embed AdSense ads, YouTube player, and other widgets. Or Google and contributors might prefer server-to-server communications of the sort Google uses in its partnerships with AOL and with Yahoo Japan. Technology need not stand in the way.

I credit that many users may be content with most Google services. For example, Google Maps enjoyed instant success through its early offering of draggable maps. But in some areas, Google's offerings have little traction. Google's Places service aspires to assess quality of restaurants and local businesses – but Yelp and Angie's List draw on specialized algorithms, deeper data, and longstanding expertise. So too for TripAdvisor as to hotel reviews, and myriad other sites in their respective sectors. A user might well prefer to get information in these areas from the respective specialized services, not from Google, were the user able to make that choice.

Google often argues that competition is one click away.[44] But here too, the E.C.'s Microsoft litigation is on point. Users had ample ability to install other browsers if they so chose, but that general capability was not enough when the standard operating system made one choice a default. Furthermore, at least Windows let other browsers truly immerse themselves in the operating system – as the default viewer for .HTML files, the default application for hyperlinks in email messages, and so forth. But there is currently no analogue on Google – no way for a user, even one who seeks this function, to combine Google algorithmic search with a competitor's maps, local results, or other specialized search services.

---

44 Adam Kovacevich, *Google's Approach to Competition*, Google Public Policy Blog (May 8, 2009), http://googlepublicpolicy.blogspot.com/2009/05/googles-approach-to-competition.html.

D. Banning Other Bad Behaviours: Tying

Using its market power over search, Google sometimes pushes sites to adopt technologies or services Google chooses. Sometimes, Google's favoured implementations may be competitively neutral – simply technical standards Google wants sites to adopt (for example, presenting an index of pages to Google's crawlers in a particular format). But in other instances, Google uses its power in search to promote adoption of Google's own services.

I first flagged this tactic as to Google Affiliate Network (GAN), Google's affiliate marketing service. Affiliate marketing is one of the few sectors of Internet advertising where Google is not dominant, and to date Google has struggled to gain traction in affiliate marketing. However, Google offers remarkable benefits to advertisers who agree to use GAN: GAN advertisers alone enjoy images in their AdWords advertisements on Google.com; their advertisements always appear in the top-right corner above all other right-side advertisements (never further down the page); they receive preferred payment terms (paying only if a user makes a purchase, not merely if a user clicks; paying nothing if a user returns merchandise, a credit card is declined, or a server malfunctions).[45] Moreover, merchants tend to use only a single affiliate network; coordinating multiple networks entails additional complexity and risks paying duplicate commissions on a single purchase. So if Google can convince advertisers to use GAN, advertisers may well abandon competing affiliate platforms.

Google's tying strategy portends a future where Google can force advertisers and sites to use almost any service Google envisions. Google could condition a top AdWords position not just on a high bid and a relevant listing, but on an advertiser agreeing to use Google Offers or Google Checkout. (Indeed, Checkout advertisers who also used AdWords initially received dramatic discounts on the bundle,[46] and to this day Checkout advertisers enjoy a dramatic multicolor logo adjacent to their AdWords advertisements, a benefit unavailable to any

---

45 Benjamin Edelman, *Tying Google Affiliate Network* (September 28, 2010), http://www.benedelman.org/news/092810-1.html.

46 Gavin Chan, *Google Checkout and AdWords*, THE OFFICIAL GOOGLE CHECKOUT BLOG (July 13, 2006), http://googlecheckout.blogspot.com/2006/07/google-checkout-and-adwords_13.html.

other class of advertiser.[47]) Google would get a major leg up in mobilizing whatever new services it envisions, but Google's advantage would come at the expense of genuine innovation and competition.

VI. A WAY FORWARD

Perhaps it's a bit presumptuous to focus on remedies before an appropriate investigation has adequately proven violations of antitrust or other laws. But a widely-circulated critique of search oversight argues that remedies for search bias are "unlikely to be workable and quite likely to make things work"[48] – suggesting that the supposed lack of remedies provides reason to decline to investigate in the first place. Of that, I am less sure. Lightweight remedies like those sketched above could put a reasonable check on many improprieties, while facilitating robust competition in various markets adjacent to search.

Google's market share in many countries is already a rounding error from 100%, and various sites report receiving an overwhelming share of both search and overall traffic from Google.[49] Search plays a uniquely central role in delivering users to web sites, and of course the Internet is crucial to facilitating modern and efficient commerce. It is untenable for one company to clutch such dramatic power over so much, with such opacity, and with opportunity for abuse. We can and should put a check on this control.

---

47 Michael Kaye, *Use Google Checkout To Boost Click Through Rates In AdWords & Base*, eCommerceCircle (August 3, 2009), http://www.ecommercecircle.com/google-checkout-click-through-rates-adwords-base_3912625.html.

48 James Grimmelmann, *supra* note 26 at 438.

49 *See, e.g.* Jeff Atwood. *The Elephant in the Room: Google Monoculture*, Coding Horror (February 9, 2009), http://www.codinghorror.com/blog/2009/02/the-elephant-in-the-room-google-monoculture.html.

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*!

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

VOLUME 7, 2011

FAIR DEALING OF COMPUTER PROGRAMS IN INDIA

Rahul Matthan[*] *& Nikhil Narendran*[**]

ABSTRACT

This essay analyses the amendments to the Copyright Act introduced in 1994 that dealt with fair dealing provisions for computer programs. The authors identify fair dealing as a user right rather than a defense right on the basis of judicial decisions on the point. They discuss the statutory exceptions to copyright for the purposes for which the program was supplied and to achieve inter-operability of a program. The authors also discuss the restrictions upon such fair dealing provisions, such as their accrual only to the lawful possessor of the program and their use solely for the purpose of achieving the purpose of supplying the program. The exceptions provided for research purposes and for making copies for non-commercial use fulfil the need for greater public access to programs and dissemination of such programs to achieve the utilitarian aim of public benefit, rather than merely seeking to vest rights in the copyright holder, despite the resistance of the industry to such methods. The authors conclude that any attempts by a company to enforce its rights to the program by creating stricter license terms to exclude the statutory exceptions for fair dealing ought to be punished under the Act.

TABLE OF CONTENTS

[*] Partner, Trilegal, Bangalore.

[**] Senior Associate, Trilegal, Bangalore.

The utilitarian or public benefit rationale of copyright law suggests that copyright is a legal concept that, contrary to appearances, was not designed to grant unlimited rights to the authors, but rather to limit the monopoly an author has over the author's works.[1] The earliest copyright law - the Statute of Anne of 1709 in England - aimed at restricting the rights of the author by limiting the author's rights to a fixed period, after which they expired. Thus, while copyright entitles an author to certain rights, it also restricts the author's rights on the grounds of principles of public policy, access to information and restraint of monopoly. Copyright is a form of intellectual property right that protects a variety of literary, artistic, musical and dramatic endeavors as well as sound recordings and films. These rights take the form of negative rights using which owner of a copyright can prevent others from copying, reproducing, etc., the work, without obtaining permission.

---

1 Craig W. Dallon, *The Problem with Congress and Copyright Law: Forgetting the Past and Ignoring the Public Interest*, 44 SANTA CLARA L. R. 365 (2004).

I. FAIR DEALING

The fair dealing provisions under the Copyright Act, 1957 ("Copyright Act") state that certain acts will not amount to an infringement of copyright. Under the Copyright Amendment Act, 1994, additional fair dealing provisions with regard to computer programs were introduced. The amendment introduced the triple test laid down in the TRIPS[2] into the provisions relating to fair dealing of computer programs.

Before proceeding to analyse these provisions, it will be useful to examine the fair dealing provisions as a whole. Various questions arise in this connection. For instance, can the fair dealing provisions be excluded by way of a contract? Do fair dealing provisions grant users specific rights or are they mere exceptions/ defenses available to users?

II. FAIR DEALING AND CONTRACTUAL RESTRICTIONS

While it could be argued that an individual can waive a private right by contract,[3] a contract waiving the right to fair dealing may be viewed as being contrary to Indian public policy. Copyright is a right guaranteed under statute. The natural rights theory attached to copyrights has already been put to rest through a plethora of judicial decisions.[4] Copyright as a right is granted to an author under the Copyright Act and derives its basis from Article 19(1)(g)[5] and Article 300A[6] of the Constitution of India. Any restrictions, limitations or exceptions to a person's right to the enjoyment of copyright cannot be anything more than a reasonable restriction on the negative rights available to the copyright owner. Such restrictions manifest themselves in the Copyright Act through provisions relating to compulsory licensing and fair dealing. These reasonable restrictions are imposed in keeping with the utilitarian public benefit

---

2 Article 13: "Members shall confine limitations and exceptions to exclusive rights to certain special cases which do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the right-holder".

3 India Financial Assn., Seventh Day Adventists v. M.A. Unneerikutty. (2006) 6 S.C.C. 351.

4 Donaldson v. Beckett, 1 Eng. Rep. 837.

5 Freedom to practice any profession, or to carry on any occupation, trade or business.

6 No person shall be deprived of his property save by authority of law.

theory of copyright law so that public access to content and its necessary dissemination is not curtailed by the rights granted to the author.

While considering the question of compulsory licensing under the Copyright Act, the honorable Supreme Court in the case of *Entertainment Network (India) Ltd.* v. *Super Cassette Industries Ltd.*[7] held:

> …the owner of a copyright has full freedom to enjoy the fruits of his work by earning an agreed fee or royalty through the issue of licenses. But, this right…is not absolute. It is subject to right of others to obtain compulsory licence as also the terms on which such licence can be granted.[8]

Further, the court went on to say that:

> …In our constitutional scheme of statute, monopoly is not encouraged. Knowledge must be allowed to be disseminated. An artistic work if made public should be made available, subject of course to reasonable terms and grant of reasonable compensation to the public at large.[9]

Copyright law promotes creativity by offering creators legal protection. However, the various exemptions and doctrines implicit in copyright law, whether statutorily embedded or judicially innovated, recognize the equally compelling need to promote creative activity and ensure that the privileges granted by copyright do not stifle dissemination of information.[10] India's ratification of the Berne Convention and TRIPS further supports the argument that fair dealing is a part of public policy of India. Any contract excluding the fair dealing provisions would likely be held to be void under section 23 of the Indian Contracts Act, 1872.

---

7 Entertainment Network (India) Ltd. v. Super Cassette Industries Ltd., 2008 (9) S.C.A.L.E. 69 [hereinafter "Super Cassette"].

8 *Id.* ¶64.

9 Super Cassatte, *supra* note 7, ¶84.

10 The Chancellor Masters and Scholars of the University of Oxford v. Narendera Publishing House., 2008 (106) D.R.J. 482, ¶32.

III. THE NATURE OF FAIR DEALING PROVISIONS

In *Campbell* v. *Acuff-Rose Music*,[11] the United States Supreme Court held that fair dealing is a defense which can be successfully raised and proven by the defendant. The Canadian Supreme court in *CCH Canadian Ltd.* v. *Law Society of Upper Canada*[12] held otherwise and classified it as a user right as opposed to a limitation or exception. There have been conflicting views as to whether fair dealing is a right or an exception.

In India, it is not clear whether fair dealing will be classified as a defense or a user right. Section 52 of the Indian Copyright Act uses the words: "The following acts shall not constitute an infringement of copyright, namely:…"

Based on this language, it could be argued that the fair dealing provisions under the Indian Copyright Act are not a right but a defense or an exception.

The Indian Supreme Court has held that a right is a legally accrued interest.[13] Copyright is a negative right and any exception to copyright would therefore amount to a positive right available to the public at large. While fair dealing is generally seen to be an exception to copyright, it could also be argued on this basis that it is in effect a right made available to the public.

In India the burden of proof is always on the party who claims infringement to prove that the defendant has infringed upon claimant's copyright.[14] Thus, it can be argued that fair dealing is a right granted to public under the Copyright Act and essentially is a user right rather than a defense.

IV. MAKING COPIES/ADAPTATION (SECTION 52(AA))

Section 52(aa) of the Copyright Act, reads as follows:

> The making of copies or adaptation of a computer program by the lawful possessor of a copy of such computer program, from such copy-

---

11 Campbell v. Acuff-Rose Music, 510 U.S. 569 (1994).

12 CCH Canadian Ltd. v. Law Society of Upper Canada, [2004] 1 S.C.R. 339.

13 Mithilesh Kumari v. Prem Behari Khare, 1989 2 S.C.C. 95.

14 R.G. Anand v. Deluxe Films, A.I.R. 1978 SC 1613.

i) in order to utilise the computer program for the purposes for which it was supplied; or

ii) to make back-up copies purely as a temporary protection against loss, destruction or damage in order only to utilise the computer program for the purpose for which it was supplied

Section 52(aa) of the Copyright Act permits copying or making backup copies or adaptation for the purposes for which the program was supplied. A user of a computer program is allowed to adapt the program or make copies in order to utilize it for the purposes for which the computer program was supplied. This seems to indicate that what is critical for the applicability of this provision is the purpose for which the program was supplied. In such case, any document that provides an indication as to the authorized use (such as the license under which the program was supplied) would be relevant. However, there is no clarity as to how to interpret the words "for the purposes for which the program was supplied". A user is also allowed to make back-up copies as a temporary protection against loss, destruction or damage to use the program for the purposes for which the program was supplied.

The license terms under which any software is supplied usually lists all the actions that a licensee can perform with that computer program. This will constitute the purpose for which the program was supplied. The user has the right to adapt the program to use it for the purposes for which the program was supplied. The "purposes for which it is supplied" must be read in the context of the general purpose for which the software was supplied, as opposed to the restrictions on its use, of which reverse engineering and adaptation are examples.

Interpreting the term "purposes for which a program was supplied", it can be argued that such purposes may include:

a) use with a specific operating system;

b) use with one specific computer or multiple computers (single user license or multi-user license);

c) home use, personal use or use in an office;

d) general uses of the software such as for use in legal profession, use in a video library etc.

Unfortunately, there are no judicial decisions that clarify this interpretation.

As discussed earlier, it could be argued that fair dealing provisions cannot be waived as doing so will be contrary to public policy. Any contractual provisions will, to that extent be held to be void. Since the fair dealing exceptions forms part of Indian public policy, any license term preventing the adaptation of a program may be held void.

However, if the license terms specifically lay down restrictions as to the purposes for which the software could be used, any right to copy or adapt the work should only be exercised for the limited purpose of utilizing the software. For example if the license sets out a restriction on the number of systems on which the software can be used, the right to copy or adapt cannot be validly exercised to make the program work on more systems than specified in the license. Similarly software licensed for use in a law firm cannot be modified or copied for use at home.

V. METHODS TO ACHIEVE INTER-OPERABILITY [SECTION 52(AB)]

Section 52(ab) of the Copyright Act reads as follows:

> The doing of any act necessary to obtain information essential for operating inter-operability of an independently created computer program with other program by a lawful possessor of a computer program provided that such information is not otherwise readily available;

Section 52(ab) of the Copyright Act, permits the doing of certain acts in order to obtain information essential for operating inter-operability of an independently created computer program provided that such information is not otherwise readily available. Under this section, a user is permitted to do any act (including by necessary assumption, reverse engineering, testing and copying of the computer program) if this is required in order to obtain necessary information essential for achieving inter-operability.

This right cannot be availed if the information in question is otherwise readily available. The purpose of this section is to deal with situations where the licensee wants to make the software work with some other piece of software for which it has not necessarily been designed to work (in order to achieve inter-operability). In such cases it is likely that the manuals and other secondary sources of information will not carry the required information.

A. Independently created computer program

The section does not clarify what an "independently created computer program" is. Does this imply that the programs in question must have been independently created? Will, for instance, this section be interpreted to mean that software such as MS Project cannot be decompiled to understand how it works with MS Word (which may not be independent of MS Office) but it can be decompiled to understand how it works with Writer software in the Open Office Suite.

It might be better to assume that independently created computer programs are those that have been created without any interface with each other and that can function without reliance on the other. For instance, if a media player software is not inter-operable with a file indexing software, this section allows the user to do certain acts to ascertain the information required to make the media player program inter-operable with the file indexer. The user can do any act that is necessary to ensure the inter-operability of either the media player software or file indexer software.

B. Lawful possessor

It is pertinent to note that this section uses the term "lawful possessor". This means that the right to make a particular computer program inter-operable with another will only be available to the lawful possessor of the program. A person using an illegally obtained (pirated) copy of a computer program cannot exercise this right. If a user is seeking to ensure inter-operability of a program, the user is doing a legal act of ensuring that this program is functioning with some other program. The user will only be allowed to do so if he/she comes with clean hands and has legitimately procured the copy of the program. This ensures that distribution of a computer program and rendering it inter-operable

with another is governed by an intellectual property regime strong enough to recognize the rights of both the user and developer.

C. License terms

Unlike section 52(aa) that mandates that an adaptation can only be done to utilize the program for the purposes for which it was supplied, there is no mention about purpose in section 52(ab). The right under this section has been granted in order to achieve inter-operability and is not restricted by purpose. Under 52(aa), the right to adapt is to an extent restricted by the license terms and can only be done to utilize the program for the purposes for which it was supplied. The right under this section is granted to ensure that inter-operability is achieved and license terms will not in any way hamper this right.

D. Achieving inter-operability

There are two ways of achieving inter-operability of a computer program. A user can make a program work with another program by porting it with another program. For example, if software A is not inter-operable with software C, a user can use the right under section 52(ab) to obtain information about both programs and can write appropriate code, which will allow software A to work with software C.

Another method of achieving inter-operability is by using the rights under both section 52(ab) and section 52(aa). If software A is not interoperable with software C, the user can use the right under section 52(ab) to understand how both software programs function. The user can then adapt either program to make them inter-operable. However, while utilizing the right under section 52(aa), one needs to keep in mind the license terms of the software also.

E. Doing of any act necessary to obtain information

This section permits the user to do any act necessary to obtain information. It is not intended to allow a lawful owner to decompile another person's code and then incorporate that into their independently created code. Such an act

would amount to infringement and will not be entitled to the fair dealing exception. Instead, it allows a user to understand how the software works and then to use the information in order to make the software interact with the other software. The intention of this provision is not to permit someone to incorporate the code into their program. There is, therefore, no need to specifically stipulate that further permission is required to incorporate the information into the independent software.

The act of obtaining the information could amount to an infringement since it could involve the creation of an intermediate copy. This would ordinarily violate the adaptation right under section 14. It is for that purpose that section 52(ab) needs to be included as a fair dealing exception to copyright if the policy of ensuring inter-operability in proprietary software is to be upheld.

While the section talks about obtaining information required to achieve inter-operability, there is no obligation to only obtain that much information as is necessary for the stated purpose. The process of obtaining information could result in greater portions of the code being exposed than is specifically necessary for inter-operability. However, the section specifically permits the doing of *any* act *necessary* to obtain *essential* information and therefore could, by implication, be deemed to permit all acts without limitation.

VI. LIMITED RESEARCH EXCEPTION (52(AC))

Section 52(ac) of the Copyright Act, reads as follows:

> "the observation, study or test of functioning of the computer program in order to determine the ideas and principles which underline any elements of the program while performing such acts necessary for the functions for which the computer program was supplied".

The limited right of research made available under this section does not permit decompiling. The right under this section is limited to observing, studying and testing of functioning of a computer program to understand the principles and ideas underlining the program, while performing such acts for which the program was supplied.

VII. MAKING OF COPIES/ ADAPTATION OF THE COMPUTER PROGRAM FROM A PERSONALLY LEGALLY OBTAINED COPY (SECTION 55(AD))

Section 52(ad) of the Copyright Act, reads as follows:

> The making of copies or adaptation of the computer program from a personally legally obtained copy for non-commercial personal use.

Under this section, one can only use *personally* legally obtained copies as opposed to just *legally obtained copies*. This means that only if the legal copy has been specifically licensed to a user, can that user avail the provisions of this section. For example, if a program licensed for office use is copied and used for home purposes, exception under this section cannot be availed.

However, if the terms of the license agreement prohibit a licensee from making copies or adapting the program, this will not operate so as to nullify the fair dealing right available to licensee under section 52(ad). For example, if A obtains a copy of an operating system for home user, that user can make copies of the program and adapt it for home use without any restrictions, regardless of the terms of a license agreement to the contrary. This seems to suggest that practices of many software companies in enforcing their license conditions may be contrary to law.

Software is often distributed under license conditions which restrict the number of systems on which the software can be installed. Much of the software that comes bundled with laptops or computers have single user licenses. This means that the software can only be used on one computer. The commercial practice indicates that a person having more than one laptop or desktop computer at home for non-commercial personal use cannot install this software on more than one computer at a time without procuring an additional copy of the license. Though this practice is widely followed in the industry, section 52(ad) allows a user to copy or adapt a computer program for non-commercial personal use.

It may be argued that this practice is in violation of the fair dealing right granted under the Copyright Act. Hence, it could also be argued that any software company violating the right of the user to copy a program is violating a right granted under the Copyright Act. It could be argued that such companies be prosecuted under section 63.

Section 63 of the Copyright Act states as follows:

> Any person who knowingly infringes or abets the infringement of - (a) the copyright in a work, or (b) any other right conferred by this Act, except the right conferred by section 53A shall be punishable with imprisonment for a term which shall not be less than six months but which may extend to three years and with fine which shall not be less than fifty thousand rupees but which may extend to two lakh rupees: Provided that where the infringement has not been made for gain in the course of trade or business the court may, for adequate and special reasons to be mentioned in the judgment, impose a sentence of imprisonment for a term of less than six months or a fine of less than fifty thousand.

Since section 63 contemplates not just the infringement of copyright, but also any other right of a person conferred under the Copyright Act, it can be argued that a software company which restricts the right of a user under section 52(dd) is violating the right of a user. As discussed earlier, this is under the assumption that fair dealing is a user right granted under the Copyright Act.

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
VOLUME 7, 2011

NEW CRIMES UNDER THE INFORMATION TECHNOLOGY (AMENDMENT) ACT

Amlan Mohanty[*]

ABSTRACT

This paper delineates the legislative response to cyber crime in India with an analysis of the Information Technology (Amendment) Act, 2008 focussing on the new crimes introduced by the amendment, on the touchstone of cyber crime legislative standards across jurisdictions. Thus, a brief look at the jurisprudential basis for criminalisation of cyberspace activities has been undertaken, following which, the new crimes have been examined section-wise. The paper uses the theoretical framework set out in the first section to probe the various problems that the Amendment Act poses in light of bad drafting and lack of understanding in the area.

TABLE OF CONTENTS

[*] The author is a fourth year student at the National Law School of India University, Bangalore. He may be contacted at mohanty.amlan@gmail.com.

I. INTRODUCTION

On December 22, 2008, the Information Technology (Amendment) Act, 2008 was passed by the Lok Sabha with almost no discussion whatsoever.[1] The Bill had been introduced in 2006 and in the wake of the terrorist attacks in Mumbai on November 26, 2008, the Act was passed as a reactionary measure.[2] The fact that the Bill was not discussed prior to it being passed is clear in its drafting. In some places, apart from being just poorly drafted, it is also vague and criminalises offences without defining the scope of the activity that could classify as criminal.

The Bill was passed by the Rajya Sabha on December 23, 2008, and received Presidential assent in early 2009. However, even after this, the Act did not come into force until October 26, 2009, when it was notified by the Central Government.[3] The Act though passed in such a rush did not come into effect until a year later. This time could have been used to discuss the Bill and address the various problems with it.

This essay looks at the new offences introduced by the Amendment Act as a legislative response to the increasing threat of cyber crime in India today, and analyses these offences in light of similar provisions in other jurisdictions. The essay first looks at the jurisprudential basis for criminalisation of activities over the internet. In this section, the essay looks at self-regulation as an adequate means of policing the internet and whether government intervention and criminalisation of cyberspace activities is necessary. The section concludes with a brief framework which is used in the analysis of the provisions in the rest of the essay. Various new offences introduced by the Act have then been studied section-wise, using the framework as explained in the first section. The scope of this essay is thus limited to the new crimes introduced by the amendment and determining the adequacy of the legislative response to the growing need

---

1 Pavan Duggal, *IT Act Amendments – Perspectives by Mr. Pavan Duggal*, CYBERLAWS.NET, http://www.cyberlaws.net/new/pd_on_ITAmendments.php (last visited Jan. 23, 2010).

2 Karen M. Sanaro & Christyne Ferri, *India's New Information Technology Law Impacts Outsourcing Transactions*, ST. B GA., June, 2009, http://www.technologybar.org/2009/06/indias-new-information-technology-law-impacts-outsourcing-transactions/ (last visited Jan. 23, 2010).

3 Press Release, Ministry of Communications & Information Technology (October 27, 2009), PIB.NIC.IN, http://pib.nic.in/release/release.asp?relid=53617 (last visited Jan. 23, 2010).

for a legislation that brings within its fold emerging forms of cyber crime. The essay concludes by looking at the various problems that the Amendment Act poses in light of bad drafting and lack of understanding in this area.

II. REGULATION OF CYBERSPACE

A. Need for regulation of cyberspace activities

A good starting point for an illuminated argumentation on the criminalisation of activities in cyberspace is the aspect of regulation of these activities itself and associated questions of its desirability, necessity and feasibility. The rhetoric of the cyber libertarians, seeking self-regulation of the internet, while challenging perceived essentialities for any kind of regulation, like territorial boundaries, real relationships and notions of property, is firmly grounded on the assertion that cyberspace is capable of being regulated through the creation of institutions and mechanisms for the regulation of conduct in cyberspace through the formulation of community based rules that are constituted, decreed and enforced by its participants without necessitating state intervention. On the other hand, those demanding government regulation stress on the inadequacy of such a system to combat instances of grievous criminality. A closer look at the contentions of both parties provides an academic space for a discussion on the criminalisation of cyberspace activities and a canvas to contextualise the nature of offences introduced by the amendment.

The cornerstone of the self-regulation theory is that the absence of government involvement in regulatory mechanisms does not result in *cyberanarchy* and suggests that the application of geographically based conceptions of legal regulation to cyberspace activities makes no sense at all, and further, that cyberspace participants are better positioned than the government to design a comprehensive set of rules that are cheaper to enforce and are practically sound.[4] The justification for such an idealistic viewpoint is buttressed by moral considerations often expressed by the participants of cyberspace who unequivocally express their objections to being disciplined by orders of the government and declare the space that they have created for themselves to be independent of the tyrannies of government order.[5]

---

4 Jack L. Goldsmith, *Against Cyberanarchy*, 65(1) U. CHI. L. REV. 1199 (1998).

5 John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUNDATION, http://homes.eff.org/~barlow/Declaration-Final.html (last visited December 5, 2009).

Entrusting the internet community with the power to create legal rules and institutions will overcome inherent difficulties associated with geographical determinacy and territorial enforcement and evolve into a mechanism to govern a wide range of new phenomena that have no clear parallel in the non-virtual world,[6] thus saving the legislature the time and energy to draft laws to deal with such situations. The proponents of self-regulation draw credibility from their claim that State laws enacted to deal with cyberspace activities have been unsuccessful,[7] and that existing laws and methods of lawmaking are inadequate,[8] and so, the internet should be self-regulated. The underlying principle entrenched in these views is that cyberspace is the antithesis of regulations and the impracticalities of regulation by external forces including law enforcement forces are too compelling to make such an attempt. The dispensability of government intervention is intimately twined with the complicated nature of social relationships in cyberspace, wherein criminal acts are reprimanded by third party Internet users who impose community defined sanctions on offenders as a form of punishment akin to State law enforcement mechanisms that seek to penalise the same crimes by utilising additional State resources with less than desired effects.

B. Need for criminalisation of offences in cyberspace

To highlight the limitations of self-regulation, or the opposite parties' contentions in this case, would be to make a case for the criminalisation of offences in cyberspace through State intervention, a position several scholars have taken with the advent of serious offences and increasing criminality on the internet such as paedophilia, cyber frauds, data theft, impersonation and cyber terrorism.[9] The typical self-regulation punishment model is centred on banishment from the group,[10] a procedure for social control that appears lenient and lacking in deterrence value as opposed to criminal sanctions imposed by the State to deter any destructive or anti-social conduct in cyberspace. It appears

---

6 David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 (5) STAN. L. REV. 1367 (May, 1996).

7 Jason Kay, *Sexuality, Live Without A Net: Regulating Obscenity And Indecency On The Global Network*, 4CAL. INTERDISCIPLINARY L.J. 355 (1995).

8 Keith J. Epstein & Bill Tancer, *Enforcement of Use Limitations By Internet Services Providers: How To Stop That Hacker, Cracker, Spammer, Spoofer, Flamer, Bomber*, 9 HASTINGS COMM. & ENT. L.J. 661-664 (1997).

9 S.V. JOGA RAO, LAW OF CYBER CRIMES AND INFORMATION TECHNOLOGY LAW 10 (2004).

10 Based on terms and conditions of access and use, imposed by service providers, commonly referred to as '*netiquette*'.

that the stream of anti-governmentalism has been laid to rest in view of the fact that the internet has quite simply become too mainstream, and being the preferred platform for electronic commerce, the need for governmental regulation cannot be ignored.[11] Perhaps the greatest argument in favour of criminalising unlawful conduct on the internet is its distinctiveness from territorial crime. The very fact that cyber crimes are easier to learn how to commit, require fewer resources relative to the potential damage caused, can be committed in a jurisdiction without being physically present in it and the fact that they are often not clearly illegal[12] make criminalisation of such conduct not only important, but essential. The conclusion that must be reached is that the State must step in with some level of regulation of cyberspace.[13]

C. Types of offences to be criminalised

An analysis of the new crimes introduced by the IT (Amendment) Act on the touchstone of cyberspace conduct sought to be criminalised by statutes and conventions around the world would help in determining the suitability and stringency of the new sections in the Indian scenario.

There are essentially four main types of conduct that a domestic legislation should penalise - (1) offences against the confidentiality, integrity and availability of computer data and systems, (2) computer-related offences with the intention to defraud, (3) content related offences, and (4) offences related to infringements of copyright and related rights.[14] In order to acquire a jurisprudential understanding of cyber crimes in general, and to gain a critical insight into the nature of offences introduced by the amendment and whether they serve the function expected of them, it is important to comprehend *why* these particular forms of conduct are criminalised across jurisdictions. Further, it is also essential to understand the range of unlawful conduct that involves computers. With

---

11 Robert Shaw, *Should the Internet be Regulated*, 2(4) IFO INSTITUTE FOR ECONOMIC RESEARCH AT THE UNIVERSITY OF MUNICH 42 (October, 2000), http://www.ifo.de/DocCIDL/Forum401-pc1.pdf (last visited December 14, 2009).

12 MACCONELL INTERNATIONAL, CYBER CRIME... AND PUNISHMENT? ARCHAIC LAWS THREATEN GLOBAL INFORMATION, (World Information Technology and Services Alliance, 2000), http://www.witsa.org/papers/McConnell-cybercrime.pdf (last visited December 1, 2009).

13 David S. Wall, *Cybercrimes: New Wine, No Bottles?*, *in* INVISIBLE CRIMES: THEIR VICTIMS AND THEIR REGULATION (Pam Davies, Peter Francis &Victor Jupp eds.,1999).

14 European Convention on Cybercrime, Guidelines for member states, 2001, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (last visited December 12, 2009).

the first, second and fourth type of conduct, private individuals may not be able to detect and proceed against the perpetrators and it therefore falls upon the State to intervene and impose criminal sanctions. It is necessary to criminalise acts falling within the third category as they are offences that shock the conscience of society and threaten public morality.

III. NEW CRIMES UNDER THE INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

Having erected a framework for comparative scrutiny of the Information Technology Act, 2000 (hereinafter, "IT Act") with cyber crime legislative standards across the world, it is plainly visible that the IT (Amendment) Act, 2008 (hereinafter "ITAA") was introduced to tackle unresolved cyberspace issues such as internet fraud, pornography, data theft, phishing etc., that were not explicitly covered under the old legislation but are at the heart of internet activity, nevertheless.

A. An overview of changes under section 66 and 67

Under the old act, criminal offences were specified under Sections 65,[15] 66[16] and 67[17] of Chapter XI ("Offences"). The provisions were broad in scope and encompassed typical cyber crimes without specificities, a possible explanation for 175 out of the 190 cases in total being booked under Section 66 and 67 of the IT Act, 2000.[18] With the introduction of new offences under the Amendment Act, there are a host of differentiated offences that have criminal penalties attached to them. The new offences range from sending of offensive messages, hardware and password theft to voyeurism, pornography and cyber terrorism, which have been inserted through amendments to Section 66 and 67 of the IT Act, 2000 and form the focus of this paper. In addition, the civil wrongs set out under S.43 of the IT Act have now been qualified as criminal offences under the ITAA 2008, if committed dishonestly or fraudulently.[19]

---

15 Section 65 deals with 'Tampering with computer source documents'.

16 Section 66 deals with 'Hacking with Computer Systems'.

17 Section 67 deals with 'Publishing of Obscene Information'.

18 National Crime Records Bureau, Cyber Crime Statistics (2007), http://ncrb.nic.in/cii2007/cii-2007/CHAP18.pdf.

19 Section 66, IT (Amendment) Act, 2008.

B. Critical analysis of the new offences introduced by the Amendment Act

(i) Sending of Offensive Messages (S.66A)

The introduction of S.66A[20] to the IT Act, 2000 unarguably expands the scope of the act to deal with instances of cyber stalking, threat mails, spam and phishing mails, with an attempt to strengthen the law and circumscribe aspects of unlawful cyber conduct that were left untouched under the old legislation, but a few flagrant issues do emerge on closer inspection of the provision.

The wording in this section has an element of ambiguity in the phrase '*menacing character*', which though perceptibly intended to protect against instances of threat mails or cyber stalking, is too broadly articulated to serve as an effective tool to combat the said offence. While the term '*grossly offensive*' does find mention in similarly purposed legislations, the word '*menacing character*' is conspicuously absent from statutes used by governments to combat instances of cyber stalking and threat mails,[21] which is of assistive value in the assertion that the phrase is misplaced. The expected ineffectiveness of S.66A(a) may be illustrated by the simple example of an employer using a mildly harsh tone in an e-mail correspondence with his employee in order to censure him, declaring possible termination if the employee's indolence continues, or a friend remarking to another in jest, that he will 'beat him up' if he fails to get tickets to the movie they had planned to watch the following weekend. In both cases, one may trace elements of 'menace', so to speak, when it evidently does not exist. Neither does the legislation speak of circumstances where there is reciprocity of sentiments.

---

20 Section 66A: Any person who sends, by means of a computer resource or a communication device,–

a) any information that is grossly offensive or has menacing character; or

b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device,

c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

21 *See*, S.1(a)(i), MALICIOUS COMMUNICATIONS ACT, 1988,(United Kingdom) http://www.harassment-law.co.uk/law/act.htm#, and relevant sections, S.1 and S.4, PROTECTION FROM HARASSMENT ACT, 1997, *available at* http://www.harassment-law.co.uk/law/act.htm#, and CRIMINAL CODE (STALKING) AMENDMENT ACT, 1999, (Australia) *available at* www.legislation.qld.gov.au/LEGISLTN/ACTS/1999/99AC018.pdf.

The fundamental problem with the section, moving on to clauses (b) and (c), is simply that several of the words used in the section such as '*inconvenience*', '*annoyance*', '*obstruction*' or '*ill will*' are not defined either in the primary or Amendment Act, leading to uncertainty in interpretation and increasing the possibility of misuse of the provision, a possible reason for some statutes drafting defences to the charge, within the section itself.[22] However, the efforts of the legislature to address developing situations of cyber crime such as threat mails, e-mail and SMS spamming, cyber stalking and phishing, must be commended.

(ii) Theft of Computer Resource (S.66B)

The relevant section to be analysed in this regard is S.66B[23] of the Amendment Act, which appears to deal with situations where there has been theft of a '*computer resource*' or '*communication device*'. Under this section, an individual who receives a stolen computer, cellphone or any other electronic device fitting the definitions contained within the Act maybe imprisoned for up to three years. Using this section, the police may tackle the growing menace of trading and purchase of stolen laptops and mobile phones, with the caveat of a potentially adverse result ensuing wherein purchasers of second hand phones may be considered suspects or wrongfully charged under this section.[24]

There may be an allegation of redundancy of this section given the pre-existence of a criminal provision for '*dishonestly receiving stolen property*' [25] with identical phraseology and punishment, but such an accusation may be displaced if one exercises scrutiny over the relevant definitions. '*Computer resource*' has been defined to include '*data*',[26] thus markedly different from the IPC provision,

---

22 Title 47, Section 223(e), COMMUNICATIONS DECENCY ACT, 1997 (United States of America), *available at* http://www.cybertelecom.org/cda/47usc223.htm..

23 Section 66B: Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

24 Naavi, *Is ITA 2000 Stringent Enough on Cyber Criminals?*, NAAVI.ORG PORTAL ON INDIAN CYBER LAW (February, 2009), http://www.naavi.org/cleditorial09/editjan27itaaanalysis12deterrance.htm (last visited December 12, 2009).

25 Section 411, INDIAN PENAL CODE, 1860: Whoever dishonestly receives or retains any stolen property, knowing or having reason to believe the same to be stolen property, shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

26 Section 2(1)(k), INFORMATION TECHNOLOGY ACT, 2000: "computer resource" means computer, computer system, computer network, data, computer data base or software.

the significant implication being that an electronic document, CD or text message containing stolen information may be brought within the umbrella of '*computer resource*'. In terms of technological significance, this can be extended to include theft of digital signals of TV transmissions.[27]

Interestingly and more importantly, one finds that this section is in consonance with the statements of objects and reasons of the IT Act, 2000 and ITAA, 2008 as it stresses on the need to protect e-commerce and e-transactions involving informational exchange and electronic data exchange.[28] With the introduction of S.66B, and the criminalisation of stolen information transmission and retention, there is a crucial deterrent factor attached to illegitimate or illegal data exchanges which is the primary focus of the IT Act itself. The immediate focus of the Amendment Act, *inter alia*, is the prevention of cyber and computer crimes and utilising the framework laid down previously in this paper and the identification of unlawful cyberspace conduct, it is also known that offences against the availability of computer data and systems (including the 'misuse of devices' with respect to sale, procurement, import and distribution) must be criminalised[29] and the section succeeds in doing so.

(iii) Identity Theft and Impersonation (S. 66C and S. 66D)

An examination of identity theft protection laws for internet users indicates that the harm sought to be prevented is not radically different from the territorial crime of the same nature. The basic nature of the crime involves the use of identifying information of someone to represent oneself as the individual for fraudulent purposes, essentially, the wrongful appropriation of one's identity by another.[30] While familiar traditional crimes of identity theft would include forgeries featuring credit cards, thefts and making of false statements, online

---

27 Naavi, *Information Technology Act 2000 Amendment Details unveiled*, NAAVI.ORG PORTAL ON INDIAN CYBER LAW (December, 2008), http://www.naavi.org/cleditorial08/editdec25itaaanalysis1.htm (last visited December 12, 2009).

28 Statement of Objects and Reasons of the Information Technology Act, 2000, *available at* http://naavi.org/ita2008/objects2008.htm and Statement of Objects and Reasons of the Information Technology Amendment Act, 2006, *available at* http://naavi.org/ita_2008/index.htm (last visited December 12, 2009).

29 *Supra* note 11.

30 Neal K. Katyal, *Criminal Law in Cyberspace*, 149 (4) U. PA. L. REV. 1027 (2001).

versions of the same crime merely involve the use of computers with similar consequences, for example, logging into someone's account and making a defamatory statement, online shopping using someone else's credit card etc.

Prior to the amendment act, the crime of identity theft was forcibly brought under S.66 within the ambit of 'hacking',[31] which presupposes that there was an infiltration of a computer resource involving '*alteration, deletion or destruction*' of the information residing therein, facilitating the crime of identity theft. However, under the new provision, S.66C,[32] the means by which the identifying information is accessed is discounted and only the act of making fraudulent or dishonest use of the information itself is criminalised. The benefit of separating the two offences cannot be overemphasised, given that a separate criminal provision exists for extraction of such data through fraudulent means.[33]

While S.66C deals with deceitful use of passwords, electronic signatures and the like, S.66D[34] involves use of a '*communication device*' or '*computer resource*' as a means of impersonation, which in effect, entails the use of computers, cellphones and PDA's for fraudulent purposes. While the former provision includes intangible but unique identifiers and symbols attached to individuals, the latter envisages instances where the offender has physical access to someone else's personal devices. However, in the absence of a clear definition of '*unique identification feature*' and the advent of new forms of cyber crime such as SMS spoofing,[35] there may exist grey areas relating to identity theft, such as the misuse of cellphone numbers, which, in the strict sense, may not be consistent with

---

31 Section 66, IT Act, 2000: (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

32 Section 66C, ITAA, 2008: Whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh.

33 Section 43 under the IT Act imposes civil penalties for such acts, but after notification of the IT (Amendment) Act, 2008, under Section 66, it is a criminal offence if *mens rea* exists.

34 Section 66D: Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

35 *See* Vineeta Pandey, *Cell Abuse: SMS Spoofing's Forgery*, The Times of India, July 18, 2004, http://timesofindia.indiatimes.com/india/Cell-abuse-SMS-spoofings-forgery/articleshow/782197.cms (last visited December 16, 2009).

the idea of a '*unique*' identification feature of an individual, and not fitting the definition of 'computer resource' or 'communication device' under S.2(1)(k) and (ha), may lie outside the scope of both, S.66C and S.66D, which is a serious concern for cyber crime officials.

A comparative analysis of the punishment stipulated under these provisions with identity theft provisions of other jurisdictions may be attempted to critically examine the nature of punishment under the Amendment Act. One must acknowledge the fact that similar legislations have different degrees of punishment based on the nature of crime committed subsequent to the identity theft taking place, a provision that could have been transplanted into the Indian legislation to make it more comprehensive, instead of having a uniform punishment of three years for the crime of identity theft.[36] So, for example, if the crime involves drug trafficking, or is a violent crime, the punishment is lesser[37] than if the offence is committed to facilitate an act of domestic terrorism.[38] It may also depend on the value of goods or money accumulated over a period of time as a result of the identity theft[39] and may also vary based on the number of identifying markers stolen.[40]

(iv) Voyeurism (S. 66E)

Based on the theoretical framework laid down earlier, the offence of voyeurism would locate itself under the heading 'content-related offences' and based on the subject of the crime, may be slotted into the category of crimes against individuals, specifically, against their person. While the Expert Committee's Report made a recommendation for imprisonment for a period of one year and fine not exceeding rupees two lakh,[41] the Amendment Act

---

36 *See* Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, § 1028 112 Stat. 3007 (1998).

37 *See* Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, § 1028(b)(3)(A) 112 Stat. 3007 (1998).

38 *See* Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, § 1028(b)(4) 112 Stat. 3007 (1998).

39 *See* Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, § 1028 (b)(1)(D) 112 Stat. 3007 (1998).

40 *See* Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, § 1028(b) 112 Stat. 3007 (1998).

41 Ministry of Information Technology, Report of the Expert Committee, http://www.mit.gov.in/download/ITAct.doc (last visited December 16, 2009).

prescribes imprisonment for a period of three years but similar fine of rupees two lakh. However, it does not make mention of compensation to the victim which was explicitly recommended by the Expert Committee, to the tune of rupees twenty five lakhs.[42]

The issue that immediately springs up on an analysis of the provision is whether it is appropriate to refer to the wrongful conduct represented in the section as 'voyeurism' in the literal sense since 'observation' of the 'private area' of persons is not criminalised. While this is understandable if one assumes the circumstances under which the offence was introduced in the Bill[43] as not requiring such a provision, since it was not observation as such, which was the concern at the time, but rather, capturing, transmitting and publishing the image of private parts of an individual.

However, on glossing over the Standing Committee's Report, it is clear that it acknowledges the emergence of new forms of computer misuse and is concerned with situations of '*video voyeurism*'.[44] Based on these considerations, it is absurd to exclude from the purview of the section, the 'observation' of private areas of a person. To reinforce this assertion, we may divert our attention to similar criminal legislations, which do include 'observation' within the section, such the Sexual Offences Act, 2003 of the United Kingdom[45] and the Canada Criminal Code.[46] It is also relevant to note that these statutes include viewing of 'private acts' besides 'private areas' of persons, which has been ignored in the Amendment Act. Finally, the observation that may be made, taking into account cyberlaw jurisprudence and the nature of acts that the IT Act seeks to criminalise, is that viewing of such images or videos through online streaming on a website such as YouTube or downloading and viewing on a communication device or computer resource as defined under the Act should also have been specified as illegal within this particular section.

---

42 *Id.*

43 One of the main circumstances for the introduction of this provision was the DPS MMS scandal. The scandal involved a video clip featuring two students from Delhi Public School, one of whom recorded the video on his cellphone, distributed it to his friends, which was further forward to the others, eventually finding its way on to the internet and being listed for sale online. The episode resulted in criminal proceedings being launched against the CEO of Baazee.com. See Avnish Bajaj v. State, 2008 150 D.L.T. 769.

44 Ministry of Information Technology, Report of the Standing Committee (2006), ¶¶ 3 and 6, *available at* http://www.naavi.org/cleditorial07/standingCommitteereportita2006.pdf (last visited December 16, 2009).

(v) Cyber Terrorism (S.66F)

Perhaps the most contentious issue in relation to the Amendment Act is that of cyber terrorism, which is essentially the convergence of terrorism and cyberspace.[47] Terrorism, by itself is not a new phenomenon, but with the development of modern technologies, the creation of laws specifically dealing with the same or related acts, conducted through the medium of cyberspace, was imminent.

An analysis of this section can be fractioned into the first and second clause, the subject matter of each being considerably dissimilar with their own particular complications. The section is comprehensive in that sub-clause (A) first enumerates the methods by which the act is committed, the wrongful conduct, as it were,[48] and then proceeds to describe the potential damage that may be caused by such acts. However, in the portion describing the likely damage, the definition is restricted to cases linked to destruction of property or death of individuals.[49] While the clause also speaks of damage to essential supplies and critical information infrastructure, there is no mention of damage to private property. Using the generally accepted definition of cyber terrorism,[50] it is clear that damage need not be restricted to property belonging to the government. So long as it induces fear in the minds of people, it may be regarded as terrorism. Also, being a provision specific to cyber terrorism, it is surprising that the term

---

45 Section 67(1): A person commits an offence if— (a) for the purpose of obtaining sexual gratification, he observes another person doing a private act, and (b) he knows that the other person does not consent to being observed for his sexual gratification....

46 Section 162(1): Every one commits an offence who, surreptitiously, observes — including by mechanical or electronic means — or makes a visual recording of a person who is in circumstances that give rise to a reasonable expectation of privacy....

47 *Supra* note 9, at 62.

48 *See* Section 66F 1(A) (i), (ii) and (iii).

49 Section 66F 1(A):...and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure....

50 'Unlawful attacks against computers, networks and the information stored therein, when done to intimidate or coerce a government or its people in furtherance of political or social objective', Peter Grabosky & Michael Stohl, *Cyberterrorism*, 82 REFORM 8 (Autumn, 2003).

'virtual properties',[51] belonging to both the government or private citizens, has not been used anywhere in the section.[52]

In the second sub-clause,[53] predominantly dealing with access to sensitive information, data and computer databases (possibly belonging to the military), there is no explicit mention of specific cyber-related activities or offences, which may have provided additional clarity as to the manner in which the penetrated data or information may be used to imperil the security of the State. For example, the data may be used to locate sensitive targets, private bank accounts may be used to fund terrorist programmes and terrorist propaganda may involve dissemination of confidential data divulging military capabilities of the State in question. It is obligatory for the definition to cover acts involving the internet such as money settlement through internet banking, use of internet channels to communicate terrorist plans across countries, hacking and defacement of governmental and non-governmental websites, virus and trojan attacks aimed at secure infrastructural and cyber assets of the country etc.[54] What is undesirable is to have an overlap of functional definitions between the IT Act, the IPC and the Unlawful Activities Prevention Act as this will only create ambiguities and loopholes that will aid the terrorists eventually. Thus, the section does not seem comprehensive enough to cover most unlawful conduct on the internet that would typically be associated with cyber terrorism.

In an effort to analyse and contrast this section with similar criminal provisions across territorial jurisdictions, we may divert our attention to the issue of punishment prescribed under the section and whether the section is devised in a manner that exhibits recognition of international developments

---

51 Virtual property may include accounts, websites, virtual currency, virtual housing spaces and other real estate in cyberspace, virtual pets, weapons and characters etc.

52 *See* Naavi, *ITA 2000 Amendment Bill defines Cyber Terrorism, prescribes life sentence*, BLOGGER NEWS NETWORK (December, 2008), http://www.bloggernews.net/119157 (last visited December 10, 2009).

53 Section 66F 1(B):...knowingly or intentionally penetrates or accesses a computer resource without authorisation... any restricted information, data or computer database... so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State....

54 Naavi, *IT Acts Amendments and Cyber Terrorism*, MERI NEWS (December, 2008), http://www.merinews.com/article/it-act-amendments-and-cyber-terrorism/152449.shtml (last visited December 8, 2009).

in cyber crime, especially in relation to cyber terrorism. Considering the content of the law, there does not appear to be widespread discrepancies with cyber terrorism-centred legislations across the world taking cognisance of the fact that there is an increasing use of computers to facilitate attacks of terrorism,[55] and that 'it is safer and more convenient to conduct disruptive activities from a remote location over the Internet than it is driving planes into buildings'.[56] As regards penalties, imprisonment for life appears to be the norm across jurisdictions[57] and uniformly the harshest amongst all internet-related crimes.[58]

It is inconceivable to think that the cyber terrorism provision in the IT Act will lie stagnant in the years to come, given the dynamic nature of terrorist activity, which is bound to traverse yet unforeseen criminal territories, but it is discomforting to see that the first legislation addressing the incidence of cyber terrorism falls drastically short in terms of comprehensiveness, clarity and particularity.

(vi) Sexually Explicit Content and Child Pornography (S.67A and S.67B)

Without entering into complicated questions of internet content regulation and obscenity on the internet, an analysis strictly of the provisions of the amendment Act reveals the section dealing with sexually explicit content, S.67A, a sub-section of S.67, which was present prior to the Amendment Act, to be well drafted and clearly defined. The terms used in the section such as 'publishes', 'transmits' have been previously defined in the act, assisting interpretation of the section to a considerable extent. In terms of penalties, compared to S.67, S.67A has an enhanced imprisonment term as well as fine for both first and subsequent convictions. Since the offence of obscenity is not a new addition to the list of offences, it has been excluded from the scope of this paper.

---

55 *E.g.*, in Australia, § 100.2(2)(h) and (i) of the Criminal Code Act (Cth), include the term '*electronic communication*', to stress on the increasing use of computers as a medium in terrorist activities. The Criminal Code Act was amended by the Security Legislation Amendment (Terrorism) Act, 2002.

56 Yee F. Lim, CYBERSPACE LAW: COMMENTARIES AND MATERIALS 353 (2007).

57 *See* Section 66F(2) of the IT (Amendment) Act, 2008 and Section 101.1(1) Criminal Code Act (Cth).

58 *Supra* note 56, at 355.

On the matter of child pornography, S.67B is a welcome introduction to the list of offences under the IT Act, particularly for the stringency that has been embedded into the provision, with not only 'publishing' or 'transmitting' of pornographic content involving children, constituting offences, but so also its collection, online viewing, downloading, promotion, exchange and distribution. This is in contrast to the offence of voyeurism as operationally defined under this Act, and previously discussed in this paper, which does not criminalise the act of viewing itself. The problem with the section however, is definitional, with ambiguity in the meaning of the phrase '*abusing children online*',[59] when read along with S.67B(e) which also discusses abuse in relation to children, but specifically mentions the phrase '*sexually explicit*' to indicate the nature of abuse. The absence of the same in the previous sub-clause leads on to believe that the constitution of 'abuse' under S.67(d) is not of a sexual nature, although it is not necessary that they must be mutually exclusive. Further, the use of the word '*indecent*' in S.67B(b) appears problematic when read in conjunction with the word '*obscene*' placed before it in the same sub-clause given that in India, there are obscenity tests laid down through precedent,[60] but nowhere has the word '*indecent*' been defined or explained.

C. The Void for Vagueness Doctrine

In order to support the view that an absence of clarity in criminal statutes is indeed a ground for protest, the researcher would like to briefly examine the Doctrine of Void for Vagueness, indigenous to the American legal system, having been derived from the due process clauses of the Fifth and Fourteenth Amendments to the U.S. Constitution.[61] The basis of the doctrine is uncertainty and lack of specificity and the philosophy underlying the principle appears to be quite simple - no one may be required at peril of life, liberty, or property to speculate as to the meaning of a penal law.[62] Thus, if it is found that a reasonably prudent man is unable to determine by himself the nature of the punishment,

---

59 Section 67B(d) of the Information Technology Act, 2008.

60 *See* Rahul Matthan, *Obscenity and Pornography on the Internet*, in THE LAW RELATING TO COMPUTERS AND THE INTERNET 45 (2000).

61 *Void for Vagueness Doctrine*, LAW.JRANK.ORG, http://law.jrank.org/pages/11152/Void-Vagueness-Doctrine.html (last visited on April 24, 2011).

62 *Id.*

the prohibited conduct as envisaged under the statute, and what class of persons the law seeks to regulate, for lack of definiteness, the law may be regarded as 'void for vagueness'.[63] The objective of a criminal statute is fairly simple, allowing citizens to organise the affairs of their lives with the knowledge of acts that are forbidden by the law, and the negation of this should logically be considered an infirmity of the legal system.

The researcher has used the example of this doctrine to buttress the argument that a criminal statute must be drafted with precision, leaving no room for ambiguity, particularly with reference to phrases that enumerate classes of persons, acts constituting an offence or a generic term that may be susceptible to multiple interpretations. Thus, for example, the phrase 'gangster' when used in a penal statute, may render the statute void, since the phrase is open to wide-ranging interpretations, both by the court and the enforcing agencies.[64]

While there exist several such instances, the author would like to limit the illustrations to this one specific case, merely to demonstrate the fact that mere uncertainty in a single phrase of a hastily drafted statute could render the law unconstitutional and void, thereby necessitating precaution in the framing of penal statutes that are bound to affect a majority of citizens, as is certainly the case with a statute regulating activities on the internet in a country as large as ours.

IV. CONCLUSION

The Information Technology (Amendment) Act, 2008 serves as a suitable case study for an analysis of the legislative exercise of law and policy formulation in the field of cyber crime legislation, revealing quite emphatically the need for carefully worded provisions, foresight in the drafting process and imagination with respect to explanations to particular sections. The inadequacies of the legislation and the resultant realistically anticipated problems reinforce the notion that criminal legislations cannot be left open to broad interpretations, especially with regard to internet regulations, considering the fact that cyberspace provides

---

63 A. G. A., *The Void for Vagueness Doctrine in the Supreme Court*, 109(1) U. Pa. L. Rev. 67 (1960).

64 Lanzetta v. New Jersey, 306 U.S. 451 (1939); Edelman v. California, 344 U.S. 357 (1953).

certain liberties in action that make it easier to transgress laws, and with such characteristics inherent to the environment, any regulatory mechanism or legislative measure must seek to be comprehensive, clear and narrow in interpretive scope.

While the purpose of the Information Technology (Amendment) Act was to address increasing trends of cyber crime and in effect, make it difficult to be a cyber criminal, the irony rests in the fact that what the Amendment Act eventually has created is a situation wherein it perhaps, isn't '*easier to be a criminal*', but rather, '*easier to be classified as a criminal*'. The danger, in both cases, cannot be overemphasised.

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY
VOLUME 7, 2011

BOOK REVIEW: INDIAN PATENT LAW AND PRACTICE, KALYAN C. KANKANALA, ARUN K. NARASANI AND VINITA RADHAKRISHNAN (OUP, 2010)

Feroz Ali Khader[*]

Patent law is a curious discipline. As a field of knowledge, it requires the practitioners to have some expertise in the two diverse fields of science and law. The science part pertains to the technology covered or protected in the patent. As we know, the branches of science are manifold: we have biotechnology, pharmaceuticals, chemical engineering, life sciences, mechanical engineering, computer sciences, electrical engineering and many others, each begetting diverse technologies of every kind. The legal part of patent law is relatively simpler. It pertains to carving out an exclusivity from what is already known (prior art) and seeking protection for the same in a manner prescribed by law.

There is no book that can guide one in the aspects of science, as a patent, by definition, is granted for cutting-edge science and technology. It then follows that any book on patent law would essentially deal with the legal aspects. Here too, there are two divisions a book can cater to – what is referred to here as the two faces of patent law. A book on patent law can serve the needs of a legal practitioner who deals with the contentious aspects of patent law. *Terrell on the Law of Patents* (Sweet and Maxwell, 17th edition, 2010) holds a special place among practitioners from the Commonwealth. A book on patent law can also serve patent agents – a group of 'hybrid' professionals who practice at the intersection of law and science. The nature of their work is different from that

[*] Advocate, High Court at Madras.

of a contentious patent lawyer. Their work involves preparing patent specification (a document which embodies the rights in a patent) and prosecuting them at the Patent Office leading to the grant of a patent. The book under review, *Indian Patent Law and Practice*, is a book written by a group of patent agents primarily targeting practising and prospective patent agents.

Oxford University Press has done a commendable job of bringing out this book in 360 pages. The book's appeal strikes you immediately: in a world where law books proclaim their arrival with the enormous bulk of their appendices (yes, in this great country, we have Appendices that are sold as law books in separate hard bound volumes charged at the price of the written commentary), this book is refreshingly lean and unintimidating.

The authors state at the beginning that they got into this business to render a service that was traditionally offered by lawyers having no technology or management background. The book asserts that patent law has two faces. True, just as there are too many lawyers with no technology background, there are also many technologists with no legal background. It is commendable that the book 'attempts to fill the dearth in Indian patent literature' in this regard.

The preliminary chapters of the book discuss the history of the patent system, the patentability requirement and the procedure for obtaining and amending patents. In the section on the patent system in India, the authors provide some useful statistical information on patent filings in India. Apart from that, there is not much the book contributes, other than referring to some of the recent case laws, which have been discussed. The authors do well in summarising the facts of most of the case laws mentioned in the book. A difficulty the reader may face while reading this book is the lack of appropriately placed citations for the case laws discussed in the book. Some case laws are discussed in the commentary with endnote references. However, these endnote references do not contain the citation of the case laws, although they do cite the paragraph number of the said cases. To find the citation of a case, one has to go to the table of cases at the beginning of the book. It may cause hardship to the reader to move back and forth to find the citation of the case and the relevant paragraph number. Footnotes would have been more desirable.

The book scores over other published books catering to patent agents through its focus on drafting techniques relating to a patent specification. The two chapters on patent specification drafting and claim drafting stand out in presenting a good introduction to the basics of drafting. The chapter on claim drafting is conveniently arranged technology-wise, with separate sections on electronics, software, mechanical and chemical inventions. Biotechnology receives some special treatment in the book. The authors safely premise their conclusions on patentability (especially on patenting gene sequences) based on the Patent Office Manual. Routine chapters on assignment, infringement, revocation, PCT applications and mining patent information appear in the latter half of the book. The book gives a good introduction to all the topics covered. However, a serious reader may find it difficult to do further research using this book as a starting point. The book does not give any reference to the rich literature that has emerged around patent drafting. Except for references to primary sources like statutes, treaties and manuals of practice, the book does not refer to any prior reference work. It would have helped the reader if such references had been provided.

The authors have taken great care in generating instructive tables and flow charts to describe the complicated procedures before the Patent Office. The sample forms in the appendices give a hands-on feel to beginners: the authors were thoughtful in adding sample invention disclosure forms, draft specification and assignment deeds.

The book is replete with amusing illustrations. The authors' fondness for the time machine can be seen at various places where they use the time machine to illustrate their point. Sample this: "For example, X invents a time machine and allows his colleagues to use it every weekend under an agreement of secrecy. Such use by X will not be considered to be public use or public knowledge." Though the said illustration may blur the line between science and science fiction, it opens many wonderful questions (hypothetical, of course) on time machines as inventions. Does an invention to travel through the fourth dimension (time), popularised by H.G. Wells, fall foul of section 3(a) of the Patents Act, which prohibits claiming anything contrary to well – established natural laws. Or, better still, does a prior travel back in time qualify for prior use that can kill the invention's novelty?

Like most first editions, there is scope for improvement here too. The utility of the book can be enhanced by inserting case citations, either within the commentary or as footnotes. In most chapters, the case laws appear at the end of a section, in isolation, titled 'A study of relevant cases'. The authors can instead try to incorporate the various case laws within the commentary. On the whole, this is a good book for a beginner. Any aspiring patent agent will stand to benefit from it.