COMPARATIVE ANALYSIS OF THE NATIONAL APPROACHES TO THE LIABILITY OF INTERNET INTERMEDIARIES
(Preliminary Version)

prepared by
Daniel Seng, Associate Professor, Faculty of Law, National University of Singapore

Table of Contents

I.	INTRODUCTION	4
II.	AUSTRALIA	7
	Authorizing Infringement and Moorhouse	7
	The Cooper, Kazaa and iiNet decisions	9
	Statutory Defenses and the Safe Harbor Provisions	11
III.	CANADA	14
	Authorizing Infringement and the "Sanction, Approve and Countenance" Test	14
	Statutory Defense for Communication to the Public by Telecommunications – the "Common Carrier" Exception	17
	Judicial Safe Harbors for Caching, Hosting and Referring Content	18
IV.	CHINA	19
	Fault-based Liability	29
	Joint or Accessory Liability	20
	Safe Harbor Defenses - Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006	21
V.	EGYPT	24
	Law on the Protection of Intellectual Property Rights	24
	Transient Copies and Internet Intermediaries as Conduits	25
VI.	INDIA	25
	Authorizing Infringement	25
	Statutory Safe Harbors and the Information Technology (Amendment) Act 2008	26
VII.	JAMAICA	28
	"Exclusive right to do or to authorize other persons"	28
	Absence of Safe Harbor Immunities	28
VIII.	JAPAN	28
	The Karaoke Principle	28
	Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers	30
IX.	MALAYSIA	32
	Malaysian Copyright Act	32
	Communications and Multimedia Act	32
X.	NEW ZEALAND	33
	Australian Performing Right Association Ltd. v. Koolman	33
	Statutory Safe Harbors for ISP Liability	34
	Graduated Response	36
XI.	NIGERIA	36
	"Cause any other person to do an [unlicensed] act"	36
	Absence of Statutory Safe Harbors	36
XII.	REPUBLIC OF KOREA	36
	The Soribada Decision	36
	Statutory Safe Harbors to Reduce or Waive Liability	37
	Graduated Response	39
XIII.	SINGAPORE	40
	Authorizing Infringement and Ong Seow Pheng	40
	BStatutory Safe Harbor Defenses	35
XIV.	SOUTH AFRICA	43
	"Causing any other person to do"	43
	Electronic Communications and Transactions Act 2002	44

XV. UNITED KINGDOM 46
"Sanction, Approve and Countenance" 46
E-Commerce (EC Directive) Regulations 2002 48
Digital Economy Act 2010 49
XVI. UNITED STATES OF AMERICA 50
Vicarious Liability 50
Contributory Infringement 53
Sony Safe Harbor Defense 54
Inducing Infringement 55
Digital Millennium Copyright Act Safe Harbors 56

I. INTRODUCTION

1. As one of the most high profile Internet intermediaries in the world, Google has been at the forefront of legal suits for claims of copyright infringement. It has been sued, *inter alia*, for indexing and making available subscription-only adult images (by Perfect 10),[1] for aggregating third party news content in Google News (in claims brought by Agence France Presse),[2] and for enabling users to share their unlicensed postings of videos (in Viacom's claim against YouTube, a Google subsidiary[3]). But claims against Google as an Internet intermediary are by no means unique. Lawsuits have been brought against Cooper[4] and iiNet[5] in Australia, Scarlet in Belgium,[6] TDC, DMT2 and Tele2 in Denmark,[7] Rokuga Net[8] in Japan, Netease,[9] Baidu,[10] Tudou.com[11] in China, RecordTV[12] in Singapore and isoHunt/TorrentBox[13] in the United States. Rightholders have also prevailed against unlicensed peer-to-peer intermediaries like Napster,[14] Aimster,[15] Grokster/Morpheus,[16] Kazaa,[17] LimeWire,[18] File Rogue[19] and Soribada.[20] In all these cases, the intermediaries are not themselves directly engaged in the infringing activity. Instead, they are sued as "indirect infringers" in that they operate equipment and services that facilitate copyright infringement.

---

[1] Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 727 (9th Cir. 2007), aff'd in part, rev'd in part on rehearing 508 F.3d 1146, 1171 (9th Cir. 2007).
[2] Agence France Presse v. Google. The action was eventually settled. See Danny Sullivan, AFP & Google Settle over Google News Copyright Case, Search Engine Land, Apr. 6, 2007, http://searchengineland.com/afp-google-settle-over-google-news-copyright-case-10926.
[3] Viacom Intern. Inc. v. YouTube, Inc., 718 F.Supp.2d 514 (S.D.N.Y. 2010).
[4] Universal Music Austl. Pty. Ltd. v. Cooper, [2005] FCA 972 (Fed.Ct. Austl.), aff'd [2006] FCAFC 187 (Full Ct. Fed.Ct. Austl.).
[5] Roadshow Films Pty Ltd v iiNet Limited (No. 3), [2010] FCA 24 (Fed.Ct. Austl.).
[6] Societe Belge Des Auters Compositeurs Et Editeurs (SABAM) v. S.A. Scarlet, No. 04/8975/A (Dist. Ct. Brussels, Oct. 2008), appeal filed, S.A. Scarlet Extended v. Societe Belge Des Auters Compositeurs Et Editeurs (SABAM), R.G. 2007/AR/2424 (Ct. App. Brussels, Jan. 28, 2010).
[7] TDC, Danish ISP (Feb. 2006); Tele2 (Oct. 2006); DMT2/Tele2 (Feb. 2008) (Danish Sup. Ct.);
[8] Rokuga Net, 2005 (Ra) No.10007, 10008, 10009, 10010, 10011, 10012 (Intellectual Property High Ct. Japan, Nov. 15, 2005).
[9] Music Copyright Society of China v. Netease Com., Inc. & Mobile Communications Corp., (2002) Er Zhong Min Chu No. 3119 (Beijing No.2 Interm. People's Ct., Sept. 20, 2002).
[10] EMI Group Hong Kong Limited v. Beijing Baidu Network Technology Co. Ltd., (2007) Gao Min Zhong Zi No. 593 (Beijing Dist. High Ct., Nov. 17, 2006).
[11] Shanghai Xinchuan Online Co. Ltd. v. Tudou.com Co. Ltd., (2007) Hu Yi Zhong Min Wu (Zhi) Chu Zi No. 129 (Shanghai No. 1 Interm. Ct., Mar. 10, 2008).
[12] RecordTV Pte Ltd v. MediaCorp TV Singapore Pte Ltd, [2009] SGHC 287 (Sing. H.C.).
[13] Columbia Pictures Industries, Inc. v. Fung, 2009 WL 6355911, 18 (C.D.Cal. 2009).
[14] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1024 (9th Cir. 2004), aff'g 114 F.Supp.2d 896 (N.D.Cal. 2000).
[15] In re Aimster Copyright Litigation, 252 F.Supp.2d 634, 642-644 (N.D.Ill. 2002), aff'd 334 F.3d 643 (7th Cir. 2003).
[16] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F.Supp.2d 1029 (C.D.Cal. 2003), aff'd 380 F.3d 1154 (9th Cir. 2004), vacated 545 U.S. 913, 125 S.Ct. 2764, 162 L.Ed.2d 781 (2005).
[17] Universal Music Austl. Pty Ltd. v. Sharman License Holdings Ltd, [2005] FCA 1242 (Fed. Ct. of Austl.) [hereinafter Kazaa].
[18] Arista Records LLC. V. Lime Group LLC., 2010 WL 2291485, 16 (S.D.N.Y. 2010).
[19] File Rogue, Heisei 16 (Ne) 446 (2003) (Tokyo High Ct., Mar. 31, 2005).
[20] Soribada, 2005 Da 11626 (2007) (Sup. Ct. Rep. of Korea, Jan. 25, 2007).

2. Why do rightholder elect to take legal action against Internet intermediaries who are not directly responsible for any wrongdoing, rather than the end users who have committed the infringing acts? Rightholders plead indirect infringement for a variety of reasons. They sue the intermediaries because intermediaries serve as the informational and access gateways for these infringing activities, and it is more cost effective to seek redress from them than all the individual users. They sue the intermediaries for not preventing or doing enough to help stem the flood of infringing activities facilitated through the intermediaries' facilities and services. They sue because intermediaries are monetizing these "infringing activities" and profiting at their expense.[21] As the EU Copyright Directive explains, "in many cases in the digital environment where, the services of intermediaries may increasingly be used by third parties for infringing activities, such intermediaries are best placed to bring such infringing activities to an end".[22]

3. In response to these claims, policies are being recalibrated and laws changed. Courts are formulating new rules to find intermediaries indirectly liable for the infringing conduct of their users. Judicial solutions in civil and common law jurisdictions include recognizing claims in authorizing infringement, vicarious and contributory liability, inducing infringement, joint tortfeasorship, aiding and abetting and negligence. Administrative solutions include the "graduated-response" laws that have now been enacted into law in Republic of Korea,[23] France,[24] New Zealand[25] and the United Kingdom.[26] All these developments portend recognition by judges and policy makers that the intermediary should be made "more" responsible.

4. At the same time, legislators recognize the important role that intermediaries play on the Internet. In 1998, the Internet intermediary industry prevailed on the U.S. Congress to enact the safe harbor provisions in U.S. Digital Millennium Copyright Act 1998 ("DMCA") to limit their liability.[27] In creating four distinct classes of safe harbors, policy makers are clearly concerned that an expansionistic reading of indirect liability will stifle Internet

---

[21] See e.g., Trial pleading for Plaintiff at 2009 WL 3046097, Scott v. Scribd, Inc., No. 4:09-CV-03039 (S.D.Tex. Sep. 18, 2009). See also Nate Anderson, Scribd sued over copyright ... by Jammie Thomas lawyers, ARSTECHNICA, Sep. 21, 2009, http://arstechnica.com/tech-policy/news/2009/09/scribd-sued-over-copyright-by-jammie-thomas-lawyers.ars (last visited Dec. 14, 2010).

[22] Directive 2001/29/EC of the European Parliament and of the Council of May 22, 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, Recital (59), 2001 O.J. (L 167) 10 (May 22, 2001).

[23] South Korea Copyright Act, art. 133-2.

[24] The HADOPI law or Creation and Internet law ("Loi favorisant la diffusion et la protection de la création sur Internet"). It is named HADOPI after "Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet (High Authority of Diffusion of the Art Works and Protection of the (Copy)Rights on Internet)," the government authority set up to administer the HADOPI provisions. The HADOPI legislation was subsequently re-enacted as the HADOPI 2 legislation after the first legislation failed a challenge under the French Constitutional Court. See Eric Pfanner, France Approves Wide Crackdown on Net Piracy, N.Y. TIMES, Oct. 22, 2009, http://www.nytimes.com/2009/10/23/technology/23net.html. See also News Wires, Top legal body strikes down anti-piracy law, FRANCE 24, Nov. 23, 2009, http://www.france24.com/en/20090610-top-legal-body-strikes-down-anti-piracy-law-hadopi-constitutional-council-internet-france.

[25] New Zealand Copyright Act, § 92A (pursuant to the New Zealand Copyright (New Technologies) Amendment Act 2008). Stemming from public protests and from objections by ISPs, the New Zealand has announced the indefinite suspension of § 92A and its application to New Zealand. See Simon Power, Minister of Commerce, Government to amend Section 92A, PRESS RELEASE: NEW ZEALAND GOVERNMENT, Mar. 23, 2009, http://www.scoop.co.nz/stories/PA0903/S00330.htm.

[26] Digital Economy Act 2010 (c. 24), §§ 3-18 (U.K.).

[27] 17 U.S.C. § 512.

businesses and crimp the innovation and creativity that has led to the rapid and successful development of the Internet.[28] Likewise, the Internet industry has also successfully pushed for the enactment of these safe harbors into national laws outside the U.S. To date, the safe harbor provisions have formed a substantial part of the intellectual property chapter in the free trade agreements entered into between the U.S. and Australia,[29] Bahrain,[30] Central America-Dominican Republic states,[31] Chile,[32] Columbia,[33] Republic of Korea,[34] Morocco,[35] Oman,[36] Panama,[37] Peru,[38] and Singapore.[39] They have also served as the template for the enactment of similar defenses in the European Union[40] (including the United Kingdom[41]), the People's Republic of China[42] and India.[43] Although not without its interpretational problems (which will be discussed below), the safe harbors have indeed become the global standard against which the liability of Internet intermediaries may be limited.

5. Differences in national approaches to the complex issue of indirect intermediary liability and the safe harbor immunities just do not make much sense in an interconnected and transnational digital environment. Both intermediaries and rightholders favor uniform and consistent global laws which will support their markets for the use of digital content. What is needed is an international framework that harmonizes and prescribes the elements of indirect Internet intermediary liability and defenses to such liability.

6. This comparative survey attempts to review the national laws of indirect liability and safe harbor defenses in conjunction with the issue of civil copyright liability of Internet intermediaries. A total of fifteen countries from both the civil and common law jurisdictions will be surveyed. In conjunction with a parallel survey prepared by Professor Juan Jose Marin, it is hoped that both surveys will aid in a better understanding of the developments of indirect liability laws worldwide. It is also hoped that the survey will identify points of convergence in the laws of these countries, and also note the points of deviation and lacuna in these laws. Stating these principles clearly and authoritatively

---

[28] See e.g., Samantha Rose Hunt, DMCA 10 years old, keeping Internet alive, TG DAILY, Oct. 28, 2008, http://www.tgdaily.com/business-and-law-features/39944-dmca-10-years-old-keeping-internet-alive.
[29] U.S.-Australia FTA, art. 17.11, para. 29. See Australia Copyright Act 1968, Part V, Division 2AA.
[30] U.S.-Bahrain FTA, art. 14.10, para. 29.
[31] U.S.-CAFTA-DR FTA, art. 15.11, para. 27.
[32] U.S.-Chile FTA, art. 17.11, para. 23.
[33] U.S.-Columbia FTA, art. 16.11, para. 29.
[34] U.S.-Korea FTA, art. 18.10, para. 30. See Republic of Korea Copyright Act 1986, Chapter 6 (arts. 102-104).
[35] U.S.-Morocco FTA, art. 15.11, para. 28.
[36] U.S.-Oman FTA, art. 15.10, para. 29.
[37] U.S.-Panama FTA, art. 15.11, para. 27.
[38] U.S.-Peru FTA, art. 16.11, para. 29.
[39] U.S.-Singapore FTA, art. 16.9, para. 22. See Singapore Copyright Act, Part IXA.
[40] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, 2000 O.J. (L 178) 1 (June 8, 2000) [hereinafter EC E-Commerce Directive].
[41] Electronic Commerce (E.C. Directive) Regulations, 2002, S.I. 2002/2013, regs. 17 (mere conduit), 18 (caching), 19 (hosting) (U.K.).
[42] Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006 (St. Council P.R.C.), arts. 20-23. See also Interpretations of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network 2006 (Nov. 22, 2006) (Sup. Ct. P.R.C.).
[43] Indian Information Technology Act, 2000, § 79 (pursuant to the Information Technology (Amendment) Act 2008).

in an international treaty or instrument on indirect liability and safe harbor immunities will make it feasible for these principles to be used confidently in the courts[44] and for the future formulation of new policies on Internet intermediary liability.

7. The countries surveyed in this study are:

- Australia
- Canada
- People's Republic of China
- Egypt
- India
- Jamaica
- Japan
- Malaysia
- New Zealand
- Nigeria
- Republic of Korea
- Singapore
- South Africa
- United Kingdom
- United States of America

8. The conclusions of this survey will be set out in a separate study to be jointly authored with Professor Juan Jose Marin.

II. AUSTRALIA

Authorizing Infringement and *Moorhouse*

9. Section 13(2) of the Australian Copyright Act states that the exclusive right to do acts comprised in the copyright in a work, adaptation or subject matter "includes the exclusive right to *authorize* a person to do that act" in relation to that work, adaptation or subject matter. A person who authorizes another to do an act in copyright without the license of the copyright owner and without legal justification infringes the copyright in the work or subject matter[45] and is secondarily liable[46] in "authorizing infringement".

10. In Australia, the law relating to "authorizing infringement" is encapsulated in the decision of the High Court of Australia in *Moorhouse v. University of New South Wales.*[47] Although there are two differing judgments in *Moorhouse*,[48] the test of authorizing infringement advanced by Justice Gibbs has been more frequently. This test focuses on the secondary

---

[44] John H. Merryman, On the Convergence (and Divergence) of the Civil Law and the Common Law, 17 STAN. J, INT'L L. 357 (1981).
[45] Australian Copyright Act, s. 36(1), 101(1).
[46] Australasian Performing Right Assoc. Limited v. Jain, (1990) 26 FCR 53, 57 (Full Fed. Ct.).
[47] Moorhouse v. Univ. of N.S.W., (1975) 133 C.L.R. 1, [1976] R.P.C. 151 (High Ct. Austl.) [hereinafter Moorhouse].
[48] Jacobs J., whose judgment was agreed by McTiernan A.C.J would however have considered authorization as an issue of whether there was an express or implied permission or invitation, and where a general permission or invitation may be implied, it was clearly unnecessary that the authorizing party had knowledge that a particular act comprised in the copyright would be done. Cf. id. at 21.

infringer's knowledge of the infringing activity and his power to control *and* prevent the infringing activity.[49] Justice Gibbs accepted that "inactivity or indifference, exhibited by acts of commission or omission, may reach a degree from which an authorization or permission may be inferred".[50] On the facts, Justice Gibbs considered the measures taken by the University of New South Wales to prevent its reprographic machines and library materials from being used to commit infringements, having supplied both the copyright materials as well as the reprographic machinery.[51] As Justice Gibbs said:

"The University had the power to control both the use of the books and the use of the machines. In the circumstances, if a person who was allowed to use the library made a copy of a substantial part of a book taken from the open shelves of the library, and did so otherwise than by way of fair dealing for the purpose of research or private study, it can be inferred that the University authorized him to do so, unless the University had taken reasonable steps to prevent an infringing copy of that kind from being made".[52] (emphasis added)

11. Applying this test, Justice Gibbs found the university liable for it had under its control the means by which an infringement of copyright may be committed (the library supplied users with the copyrighted material (books) and the reprographic machines) and, knowing or having reason to suspect that it was likely to be used for the purpose of committing an infringement, omitted to take reasonable steps to limit its use to legitimate purposes.[53] The capacity to control the primary infringer is a lynchpin of the test of secondary liability. Conversely, in *Tape Manufacturers Association Ltd v. Commonwealth of Australia*, the High Court held a manufacturer or vendor of the recording equipment not liable for authorizing infringement because it had no control over the purchaser's use of the article.[54]

12. The *Moorhouse* test of authorizing infringement was subsequently codified[55] in sections 36(1A) and 101(1A) of the Australian Commonwealth Copyright Act,[56] which read:

(1A) In determining, for the purposes of subsection (1), whether or not a person has authorized the doing in Australia of any act comprised in the copyright in a work or subject matter without the license of the owner of the copyright, the matters that must be taken into account include the following:

---

[49] Moorhouse, at 13 (Gibbs J.).
[50] Moorhouse, at 12 (Gibbs J.).
[51] Id. at 15.
[52] Id. at 14.
[53] Id.
[54] Tape Mfr. Ass'n Ltd. v. Commonwealth of Austl., (1993) 176 C.L.R. 480, [6]-[7] (High. Ct. Austl.) (Mason C.J., Brennan, Deane & Gaudron J.J.). On the same reasoning, the majority of the High Court also concluded that the sale of blank tapes does not constitute an authorization by the vendor to infringe copyright.
[55] Kazaa, [402]. See also Cooper v. Universal Music Austl. Pty. Ltd., [2006] FCAFC 187, [20] (Full Ct. Fed.Ct. Austl.) (Branson J). However, counsel for the right holders contended, with some force, that section 101(1A) had changed (and in one respect, superseded) the law as regards authorization as stated by Gibbs J. in Moorhouse. See, Kazaa, [360]. Nonetheless, the accepted view is that section 101(1A) did not change the interpretation to the concept of authorizing infringement as developed in Moorhouse. See Cooper, 156 FCR 380 at [136], Kazaa, at [402], Cooper, 150 FCR 1 at [83], iiNet, at [367].
[56] Austl. Copyright Act § 101(1A), amended by Copyright Amendment (Digital Agenda) Act 2000, c. 110, § 87.

(a) the extent (*if any*) of the *person's power to prevent the doing of the act* concerned;
(b) the nature of any relationship existing between the person and the person who did the act concerned;
(c) whether the person *took any other reasonable steps to prevent or avoid the doing of the act*, including whether the person complied with any relevant industry codes of practice. (emphasis added)

The *Cooper, Kazaa* and *iiNet* decisions

13. The *Moorhouse* test was first applied by the Federal Court to Internet intermediaries in *Universal Music Australia v. Cooper* ("*Cooper*"). In this case, the issue was whether a portal site had authorized infringement by aggregating third party submissions of hyperlinks to sites where unlicensed music files could be downloaded.[57] In that case, Justice Tamberlin held that though the portal did not host the music files, it was "clearly designed to, and does, facilitate and enable this infringing downloading" as the defendant Cooper "could have prevented the infringements by removing the hyperlinks from his website or by structuring the website in such a way that the operators of the remote websites from which MP3 files were downloaded could not automatically add hyperlinks to the website without some supervision or control by Cooper".[58] Accordingly, Justice Tamberlin found that Cooper's failure to do so amounted to authorization of the infringement.[59] Likewise, Justice Tamberlin found that Cooper's hosting company, an ISP, had authorized the infringement because it "could have taken the step of taking down the website" but instead chose not to prevent the acts of infringement.[60] On appeal, the Full Court of the Federal Court of Australia upheld the decision of Justice Tamberlin on similar grounds, emphasizing that Cooper could have prevented the submission of links or disabled their function, and that the hosting company could have taken down Cooper's website and declined to provide Cooper with hosting facilities.[61]

14. This approach was taken to the next step by the Australian Federal Court in *Universal Music Australia v. Sharman License Holdings Ltd* ("*Kazaa*"), where the key defendants, developers and distributors of P2P software ("Sharman"), were held liable for authorizing infringement.[62] In *Kazaa*, Justice Wilcox read *Moorhouse* as conflating "control" with "preventive measures,"[63] in that a failure to exercise some measure of control to prevent the infringing activities of Kazaa users[64] will amount to authorizing infringement. Despite

---

[57] Universal Music Austl. Pty. Ltd. v. Cooper, [2005] FCA 972 (Fed.Ct. Austl.), aff'd [2006] FCAFC 187 (Full Ct. Fed.Ct. Austl.). Although Cooper was referred to in Kazaa, it was not cited for this proposition.
[58] Universal Music Austl. Pty. Ltd. v. Cooper, [2005] FCA 972, [84]-[85].
[59] Id. [86], [88].
[60] Id. [121].
[61] Universal Music Austl. Pty. Ltd. v. Cooper, [2006] FCAFC 187, [41], [62]-[64] (Branson J.); id. [148]-[152], [155]-[157] (Kenny J.).
[62] Universal Music Austl. Pty Ltd. v. Sharman License Holdings Ltd, [2005] FCA 1242 (Fed. Ct. of Austl.) [hereinafter Kazaa].
[63] It should also be noted that counsel for Sharman seemed to have conceded that "control" is not necessary for there to be a finding of authorization. Kazaa, [371]. However, counsel also argued that section 101(1A) of the Australian Copyright Act did not change the law concerning authorization. Id.
[64] See, Id. [414]. Wilcox J. required "consideration of the extent of Sharman's power to prevent copyright file-sharing and the steps it took to prevent or avoid that practice, including compliance with any relevant industry code of practice". Id. [409] (construing Copyright Act 1968, c.63, §

[Footnote continued on next page]

the fact that Kazaa developers were part of the second generation of P2P software that were designed using decentralized networking models that de-emphasized any control over the users' activities when using such software,[65] Justice Wilcox found that Sharman could exercise "indirect control"[66] through modifications to the Kazaa software's built-in search filter.[67] Even though the filter was designed to remove offensive and adult content when such keywords were used as search terms,[68] Justice Wilcox found Sharman liable because the Kazaa software filter *could be* adapted to filter out unlicensed works and prevent copyright file sharing.[69] His Honor said:

"Counsel for the Altnet respondents argued it would not be possible to find authorization unless I was satisfied that Sharman was in a position to 'control' the file-sharing behavior of Kazaa users. There may be room for debate as to whether it is desirable to continue to use the word 'control' in this context, having regard to the content of the new subs (1A) of s 101. However, it would not be inapt to use the word 'control' to describe Sharman's position. Sharman was not able to control the decisions of individual users as to whether or not they would engage in file-sharing and, if so, which particular works they would place into their 'My Shared Folder' file or download from other people. However, Sharman was in a position, through keyword filtering or gold file flood filtering, to prevent or restrict users' access to identified copyright works; in that sense, Sharman could control users' copyright infringing activities. Sharman did not do so; with the result that the relevant applicant's copyright in each of the Defined Recordings was infringed".[70] (emphasis added)

15. Likewise, Justice Wilcox found that Altnet, the providers of the licensed works or "gold files" via the TopSearch feature in the Kazaa system *could have*, in the light of knowledge that there was substantial copyright infringement by users using the Kazaa system,[71] replaced the users' search requests with false results – empty gold files[72] – based on a list of copyright works provided by copyright owners.[73] Through their technical ability to link their TopSearch results to the Kazaa system,[74] this feature would "drive [the users] mad"[75] when they search for infringing works for downloading. In failing to do something which was within their power,[76] Altnet had thereby authorized the users' infringement[77] by taking "no steps to prevent or avoid the users' copyright infringements".[78]

[Footnote continued from previous page]

101(1A) (Austl.) [hereinafter Austl. Copyright Act]). Although Wilcox J. here preferred to use the language of the factors set out in section 101(1A), Wilcox J. also accepted the continuing applicability of the Moorhouse test. Id. [402].

[65] CNET News.com, The evolution of file swapping (Jun. 27, 2005), http://news.com.com/The+evolution+of+file+swapping/2100-1030_3-5752075.html.

[66] Kazaa, [236] (heading).

[67] Id. [254].

[68] Id. [129], [255], [262].

[69] Id. [294].

[70] Id. [414].

[71] Id. [465].

[72] Id. [312]-[313].

[73] Id. [328].

[74] Id. [310], [318], [322]-[328], [465].

[75] Id. [307], [309] (so that users would be discouraged from looking for licensed works).

[76] Id. [328].

[77] Id. [472].

[78] Id. [465]-[466].

16. The potential expansion of the test in *Moorhouse* was however halted in the recent decision of *Roadshow Films Pty Ltd v iiNet Limited.*[79] In this case, Justice Cowdroy re-read *Moorhouse* and held that an Internet intermediary has to provide the true means of infringement before the *Moorhouse* test was relevant.[80] Justice Cowdroy drew a distinction between providing the "means" of infringement, and providing a precondition to the infringement.[81] Justice Corwdroy held that the provision of access to the Internet was not the "means" of infringement. Instead, it held that the "means" by which the plaintiffs' copyright was infringement was the iiNet user's use of the constituent parts of the BitTorrent system,[82] over which iiNet had no control and was not responsible for its operation.[83] Justice Cowdroy distinguished iiNet's operations from those of the respondents in *Cooper* and *Kazaa*, noting that the respondents there intended copyright infringements to occur, and deliberately structured the website and software respectively to achieve this result.[84] He reiterated that the law of copyright recognized no positive obligation on any person to protect the copyright of another.[85] At the time that this report is drafted, an appeal has been heard on the *iiNet* case, and it remains to be seen if the Full Court of the Federal Court would uphold Justice Cowdroy's decision.

Statutory Defenses and the Safe Harbor Provisions

17. In response to concerns by the Australian Internet industry as to the intermediaries' potential liability for authorizing infringement, various statutory defenses have been enacted into the Australian Copyright Act.

18. Section 112E, inserted pursuant to the Copyright Amendment (Digital Agenda) Act 2000 (Cth), provides that a person "who provides facilities for making, or facilitating the making of, a communication is not taken to have authorized any infringement of copyright in an audio-visual item merely because another person uses the facilities so provided to do something the right to do which is included in the copyright". This section, which is based on the Agreed Statement to Article 8 of the WIPO Copyright Treaty 1996 (with the exception that it removes the need for facilities to be "physical facilities"), has however received a narrow judicial interpretation before the Australian Federal Court in *Kazaa*,[86] *Cooper*[87] and *iiNet*.[88] In particular, in *iiNet*, after considering the previous authorities, Justice Cowdory concluded that section 112E had only minimal application because it would not protect an intermediary from secondary liability if there is a finding of authorizing infringement. In other words, "when a finding of authorization is made against a provider of facilities, section 112E will not assist, as in all of the circumstances that person is doing more than (or in addition to) providing services".[89] On the facts of *iiNet*, however, as there

---

[79] Roadshow Films Pty Ltd v iiNet Limited (No. 3), [2010] FCA 24 (Feb. 4, 2010) [hereinafter iiNet].
[80] iiNet, at [371]-[383].
[81] iiNet, at [400]-[401].
[82] iiNet, at [402].
[83] iiNet, at [404].
[84] iiNet, at [394], [397].
[85] iiNet, at [492].
[86] Kazaa, at [396]-[418], [468] (holding that provision did not protect Sharman, which was not a mere "messenger").
[87] Cooper (Fed. Ct.), at [99], [126]; Cooper (Full Fed. Ct.), at [58]-[60], [169], [170] (holding that Cooper and the ISP fell outside of s. 112E because it had encouraged the infringing activity, elected to turn a blind eye on notice of the activity or failed to take reasonable steps to prevent the infringement).
[88] iiNet, at [570]-[574].
[89] iiNet, at [574].

was no finding that *iiNet* had authorized infringement, the section 112E defense was not relevant.

19. In addition to section 112E, four safe harbor defenses were introduced into the Australian Copyright Act pursuant to the United States Free Trade Implementation Act 2004 (Cth) and the Copyright Legislation Amendment Act 2004 (Cth). These safe harbor defenses originate from section 512 of the United States Copyright Act, although they are "narrower" than their United States counterparts in that they only provide protection for "carriage service providers"[90] (CSPs), defined with reference to the Australian Telecommunications Act as a provider of "a service for carrying communications by means of guided and/or unguided electromagnetic energy".[91] The first safe harbor defense, set out as category A in section 116AC, is in relation to CSPs that "provide facilities or services for transmitting, routing or providing connections for copyright material, or the intermediate and transient storage of copyright material in the course of transmission, routing or providing connections". The second defense, set out as category B in section 116AD, applies to CSPs that cache copyright material through an automatic process. The third defense, set out as category C in section 116AE, applies to CSPs that store, at the direction of a user, copyright material on a system or network controlled or operated by or for the CSP. And the fourth defense, set out as category D in section 116AF, applies to CSPs that refer users to an online location using information location tools or technology.

20. All CSPs have to satisfy the general conditions to qualify for the safe harbor defenses. The general conditions are that the CSPs must adopt and reasonably implement a policy for terminating, in appropriate circumstances, the accounts of repeat infringers, and compliance of a relevant industry code in force that relates to standard technical measures used to protect and identify copyright material.[92] In addition, the CSPs must satisfy the specific conditions for the particular safe harbor category. These conditions, as spelt out in section 116AH(1), are:

Category A – transmission services (section 116AC)	Transmission of copyright material must be initiated by or at the direction of a person other than the CSP CSP must not make substantive modifications to the copyright material transmitted (except as part of a technical process)
Category B – caching services (section 116AD)	CSP to ensure that access to cached copyright material is subject to conditions of user access at originating site CSP to comply with relevant industry code for updating cached copyright material and not interfere with technology used at originating site to obtain information about use of material CSP to expeditiously remove or disable access to cached material upon prescribed notification

[90] iiNet, at [582].
[91] Australian Telecommunications Act 1997, ss. 7, 87 (defining "carriage service" and "carriage service provider" pursuant to the Australian Copyright Act, s. 116AA).
[92] Australian Copyright Act, s. 116AH(1) item 1, conditions 1 and 2.

	that material has been removed or access has been disabled at originating site CSP must not make substantive modifications to the copyright material cached as it is transmitted to subsequent users (except as part of a technical process)
Category C – hosting services (section 116AE)	CSP must not receive financial benefit that is directly attributable to infringing activity if CSP has right and ability to control the activity CSP to expeditiously remove or disable access to hosted material upon receipt of prescribed notification that material has been found to be infringing by a court CSP to act expeditiously to remove or disable access to copyright material residing on its system or network if it becomes aware: – that material is infringing, or – of facts or circumstances that make it apparent that material is likely to be infringing CSP to comply with prescribed procedure in relation to removing or disabling access to copyright material residing on its system or network
Category D – referral services (section 116AF)	CSP must not receive financial benefit that is directly attributable to infringing activity if CSP has right and ability to control the activity CSP to expeditiously remove or disable access to a reference residing on its system or network upon receipt of prescribed notification that material to which reference refers has been found to be infringing by a court CSP to act expeditiously to remove or disable access to a reference residing on its system or network if it becomes aware: – that material to which reference refers is infringing, or – of facts or circumstances that make it apparent that material to which reference refers is likely to be infringing to ensure that access to cached copyright material is subject to conditions of user access at originating site CSP to comply with prescribed procedure in relation to removing or disabling access to a reference residing on its system or network

21. These conditions do not require a CSP to monitor its service or seek facts to indicate infringing activity except to the extent required by a standard technical measure.[93]

22. If the CSPs satisfy both the general and specific conditions attached to the particular safe harbor category,[94] a bar is placed on the court in granting damages, additional damages, account of profits and other monetary relief against the CSPs.[95] In a first such case of its case, the iiNet court held that the defendant ISP in the case, iiNet, qualified for the category A safe harbor defense as it had adopted and reasonably implemented a repeat infringer policy.[96] However, as the *iiNet* court also observed, a failure to satisfy the safe harbor conditions is not evidence that a CSP is liable for copyright infringement, as observance of the safe harbor provisions is voluntary.[97]

III. CANADA

Authorizing Infringement and the "Sanction, Approve and Countenance" Test

23. Section 3 of the Canadian Copyright Act states that copyright owners have the right to "produce or reproduce the work, to perform the work, to publish the work and to *authorize* any such acts". Section 27 in turn provides that it is an infringement of copyright for anyone to do anything that the Copyright Act only allows owners to do,[98] including authorizing the exercise of his own rights.[99]

24. An analysis of the law on "authorizing infringement" in Canada starts with the recent decision of the Canadian Supreme Court in *CCH Canadian Ltd. v. Law Society of Upper Canada*.[100] On a fact situation similar to that before the Australian High Court in *Moorhouse*,[101] the Supreme Court held that the provision of self-service photocopiers in its library by the Law Society did not amount to authorizing infringement.[102] The court accepted that as a question of fact that depends on the circumstances of each particular case, authorization can be inferred from acts that are less than direct and positive, including a sufficient degree of indifference.[103] However, the court took the view that a person does not authorize infringement by authorizing the mere use of equipment that could be used to infringe copyright.[104] Canadian courts should presume that a person who authorizes an activity does so only so far as it is in accordance with law,[105] though

---

[93] Australian Copyright Act, s. 116AH(2).
[94] Australian Copyright Act, s. 116AG(1).
[95] Australian Copyright Act, s. 116AG(2)-(4).
[96] iiNet, at [634].
[97] iiNet, at [589].
[98] Canadian Copyright Act, s. 27(1).
[99] CCH Canadian Ltd. v. Law Soc'y of Upper Canada, 2004 SCC 13, 236 D.L.R. (4th) 395, 317 N.R. 107, 30 C.P.R. (4th) 1, [2004] 1 S.C.R. 339, at [37] (Sup.Ct. Can.) [hereinafter CCH Canadian].
[100] Id.
[101] The Canadian Supreme Court took the view that the Moorhouse approach to authorization shifted the balance in copyright too far in favor of the owner's rights and unnecessarily interferes with the proper use of copyrighted works for the good of society as a whole. Id. 41.
[102] Id. 46.
[103] Id. 38.
[104] Id. 43.
[105] Id. 38, 43.

this presumption may be rebutted if it is shown that a certain relationship or degree of control existed between the alleged authorizer and the persons who committed the copyright infringement.[106] Examples of such a relationship or degree of control include a master-servant relationship or an employer-employee relationship, neither of which exists between the Law Society and its library patrons, "[n]or does the Law Society exercise control over which works the patrons choose to copy, the patron's purposes for copying or the photocopiers themselves".[107] Thus the court held that the Law Society lacked sufficient control over the library's patrons to permit the conclusion that it "sanctioned, approved or countenanced the infringement".[108]

25. The Canadian Supreme Court had the opportunity to apply its reasoning to Internet intermediaries in the case of *Society of Composers, Authors & Music Publishers of Canada v. Canadian Association of Internet Providers*,[109] a decision which was heard just after *CCH*. The plaintiffs represented the musical composers and artists whose Canadian copyright in music downloads were infringed. Initially, in proceedings before the Canadian Copyright Board, they sought to impose royalties on all entities involved in the Internet transmission chain, including the backbone service providers, for communicating the downloaded music.[110] Subsequently, the plaintiffs narrowed their claims to the defendant ISPs that are located in Canada for providing retail access to the Internet both to content providers and to end user subscribers.

26. In relation to their claim that the defendant ISPs were liable for authorizing infringement, the Supreme Court, applying *CCH*, refuted the plaintiffs' claims. The Court accepted that "knowledge of the content available on the Internet, including 'free' music, and of end users' interest in accessing it, are powerful inducements for end users to sign up with access providers, and content providers with operators of host services".[111] However, it also opined that there were "massive amounts of non-copyrighted material" accessible to the end user on the Internet.[112] On the holding in *CCH* that courts should presume that a person who authorizes an activity does so only so far as it is in accordance with law, thus it was not possible to impute to the ISP, based solely on the provision of Internet facilities, an authority to download copyrighted material as opposed to non-copyrighted material.[113] "Knowledge that someone might be using neutral technology to violate copyright (as with the photocopier in the *CCH* case) is not necessarily sufficient to constitute authorization, which requires a demonstration that the defendant did give approval to; sanction, permit; favor, encourage' the infringing conduct".[114] Hence, the court described the participation of the ISPs in communicating copyright works as "content neutral".[115]

27. Nonetheless, the Court accepted that where the ISP has notice that a content provider has posted infringing material on its system and fails to take remedial action, such as to require the customer to remove the offending material through a "take down" notice, it

---

[106] Id. 38.
[107] Id. 45.
[108] Id. 45.
[109] Soc'y of Composers, Authors & Music Publishers of Canada v. Canadian Ass'n of Internet Providers, 2004 SCC 45, 32 C.P.R. (4th) 1, 240 D.L.R. (4th) 193, [2004] 2 S.C.R. 427 (Sup.Ct. Can.) [hereinafter Canadian Association of Internet Providers].
[110] Id. 14-15. These are entities that provide the facilities and long distance connections including fibre optics and telephone lines that support the Internet.
[111] Id. 121.
[112] Id. 123.
[113] Id.122, 123.
[114] Id. 127.
[115] Id. 92, 124.

may cease to be "content neutral".[116] Notice of infringing content and a failure to respond by taking it down may in some circumstances lead to a finding of authorizing infringement.[117] However, the Court also warned against an overly quick inference of "authorization" as this would put ISPs in a difficult position of judging whether the copyright objection is well founded, and to choose between contesting a copyright action or potentially breaching its contract with the content provider.[118] The Court would have favored a statutory notice and take down regime similar to that in the European E-Commerce Directive and the United States DMCA.[119] In its absence, the court gave no further guidance, aside from opining that whether or not authorization could be inferred would depend on the facts.[120]

28. The factual nature of this inquiry in relation to a presumption of non-authorization may be illustrated with the case of *BMG Canada v. John Doe* ("*John Doe*"). In this case, the issue before the Canadian Federal Court is whether an end user who has placed a personal copy of music files on a shared directory linked to a P2P network could be said to have authorized their reproduction.[121] Even though putting such files on a shared directory would make them accessible by other users,[122] the court said it could see no difference between this situation and a library that places a photocopy machine in a room full of copyrighted material.[123] On appeal, the Federal Court of Appeal noted that the case was on a motion for discovery of the identities of the infringing end users and that it was premature to reach any conclusion in this regard.[124] It would be incorrect to rely on the presumption in *CCH* without regard for its factual context. Thus, while library users may legitimately make partial copies of copyrighted material as fair use, and evidence in this regard was received by the *CCH* court, the Federal Court of Appeal noted that copying and placing songs into shared directories could constitute authorization "because it invited and permitted other persons with Internet access to have musical works communicated to them and be copied by them".[125] This suggests that the presumption of non-authorization may be rebutted on the facts and represents a perceptible shift from the approaches taken in *CCH* and *Canadian Association of Internet Providers*.

---

[116] Id. 110, 124.
[117] Id. 127.
[118] Id.
[119] Id. 127.
[120] Id. 128.
[121] BMG Canada Inc. v. John Doe, 2004 FC 488, [2004] 3 F.C.R. 241 (Fed.Ct. Can.), aff'd in part, rev'd in part 2005 FCA 193, 252 D.L.R. (4th) 342, 39 C.P.R. (4th) 97, [2005] 4 F.C.R. 81 (Fed.C.A. Can.). Cf. Atlantic Recording Corp. v. Howell, 2008 WL 1927353 (D.Ariz. 2008) (holding that where the defendants did not knowingly share their files for downloading via Kazaa, and thus making the work available to the public, they could not be liable for "distribution" of the work).
[122] Id. 28. The court took the view that there was no "positive act" by the owner of the shared directory, such as sending out copies or advertising that they were available for copying, and thus, the placing of copies on a shared directory could not amount to distribution or "making available" such copies. See supra text accompanying note **Error! Bookmark not defined.**. See also THOMAS D. SYDNOR II ET AL., FILESHARING PROGRAMS AND TECHNOLOGICAL FEATURES TO INDUCE USERS TO SHARE: A REPORT TO THE UNITED STATES PATENT AND TRADEMARK OFFICE FROM THE OFFICE OF INTERNATIONAL RELATIONS (Nov. 2006), available at http://www.uspto.gov/web/offices/dcom/olia/copyright/oir_report_on_inadvertent_sharing_v1012.pdf (explaining the dangers of how P2P software are designed to automatically share users' content).
[123] John Doe, 2004 FC 488, 27.
[124] BMG Canada Inc. v. John Doe, 2005 FCA 193, 252 D.L.R. (4th) 342, 39 C.P.R. (4th) 97, [2005] 4 F.C.R. 81, 51 (Fed.C.A. Can.).
[125] Id. 51.

Statutory Defense for Communication to the Public by Telecommunications – the "Common Carrier" Exception

29. Section 2.4(1)(b) of the Canadian Copyright Act also provides as follows:

For the purposes of communication to the public by telecommunication, a person whose only act in respect of the communication of a work or other subject-matter to the public consists of providing the means of telecommunication necessary for another person to so communicate the work or other subject-matter does not communicate that work or other subject-matter to the public.

30. This section as inserted in 1988 pursuant to the recommendations of the Sub-Committee on the Revision of Copyright of the House of Commons Standing Committee on Communications and Culture, and was intended to serve as the counter-balance to the expanded definition of communication which the Sub-Committee had proposed. Known as the "common carrier exception," it was originally intended to ensure that those entities that "serve as an intermediary between the signal source and a retransmitter whose services are offered to the general public" would not be held liable.[126] In *Canadian Association of Internet Providers*, the Supreme Court held that this provision shields from liability the activities of ISPs associated with providing the means for another to communicate by telecommunication, and includes the "routers and other hardware, the software connection equipment, connectivity services, hosting (which will be discussed below) and other facilities and services without which such communications would not occur".[127] By not "engaging in acts that relate to the content of the communication, *i.e.* whose participation is content neutral,"[128] the ISPs are "innocent disseminators" and "conduits," whose role is limited to "providing the means necessary to allow data initiated by other persons to be transmitted over the Internet"[129]. In this regard, the Court equated their role as "conduits" in providing technology infrastructure to those of owners of telephone wires,[130] in that they lack actual knowledge of the infringing content moved through its infrastructure, and it is impractical (both for technical and economic reasons) to monitor the vast amount of material moving through the Internet.[131] The Court opined that this interpretation of section 2.4(1)(b) is consistent with the Agreed Statement to Article 8 of the WIPO Copyright Treaty, 1996[132] and clause 42 of the European E-Commerce Directive.[133]

31. However, the Supreme Court also noted that section 2.4(1)(b) only protected the communication function of an ISP as an intermediary. It does not protect all the activities of the ISP.[134]

---

[126] Sub-Committee on the Revision of Copyright of the House of Commons Standing Committee on Communications and Culture, A Charter of Rights for Creators (1985), at 80.
[127] Id. 92.
[128] Id. 92.
[129] Id. 95.
[130] Id. 96.
[131] Id. 101.
[132] Id. 97.
[133] Id. 98.
[134] Id. 102.

Judicial Safe Harbors for Caching, Hosting and Referring Content

32. No statutory safe harbors in the form similar to the United States DMCA safe harbors exist in the Canadian Copyright Act. However, the Canadian Supreme Court in *Canadian Association of Internet Providers* has interpreted section 2.4(1)(b) of the Canadian Copyright Act to offer a considerable measure of protection to Internet intermediaries engaged in caching, hosting and referral services. It should be noted that section 2.4(1)(b) operates not merely to limit the remedies available to Internet intermediaries nor as an exemption from liability; it provides that intermediaries that are engaged in providing the means of telecommunication necessary to communicate the work "does not communicate that work to the public". In other words, section 2.4(1)(b) provides that the qualifying telecommunication activities of Internet intermediaries will not constitute an activity (communication) that engages a copyright right and fall outside the scope of the Copyright Act.[135]

33. Thus, in *Canadian Association of Internet Providers* has interpreted section 2.4(1)(b) to shield the Internet intermediary from "liability" for providing caching services. The Supreme Court accepted the view that caching services were content neutral and "necessary" to maximize the economy and cost-effectiveness of the Internet conduit[136] providing host server services from liability. Such an interpretation "best promotes the public interest in the encouragement and dissemination of works of the arts and intellect".[137]

34. Likewise, the Canadian Supreme Court in *Canadian Association of Internet Providers* also interpreted section 2.4(1)(b) to shield the Internet intermediary providing host server services from "liability". It accepted the distinction drawn by the Canadian Copyright Board between a person who posts a musical work, and the conclusion that the person who "makes the work available for communication is not the host server provider but the content provider".[138] According to the Court, server operation, housing and maintenance services and services for monitoring hits on web pages are merely ancillary to the provision of disk space and do not involve any act of communication.[139] "To the extent that [the host server providers] act as innocent disseminators, they are protected by s. 2.4(1)(b) of the Act".[140] The Court agreed with the following statement of the Copyright Board:

As long as its role in respect of any given transmission is limited to providing the means necessary to allow data initiated by other persons to be transmitted over the Internet, and as long as the ancillary services it provides fall short of involving the act of communicating the work or authorizing its communication, it should be allowed to claim the exemption.[141]

35. Nonetheless, the Court accepted that where the hosting intermediary has notice that a content provider has posted infringing material on its system and fails to take remedial action, such as to require the customer to remove the offending material through a "take

---

[135] Id. 87.
[136] Id. 115.
[137] Id.
[138] Id. 94.
[139] Id. 103.
[140] Id. 95.
[141] Id.

down" notice, it may be held to have authorized the communication of the copyright material[142] and attract secondary liability.

36. On the issue of referral services such as search engines and hyperlink portals, the Canadian Supreme Court in *Canadian Association of Internet Providers* noted that the Canadian Copyright Board had ruled that the creation of an "automatic" hyperlink – one that instructs a browser that accesses a first site to download a file from a second site – as opposed to a "manual" hyperlink – where the user must take some action such as to click on the link to access the information on the second site,[143] attracts copyright liability in authorizing infringement for communicating the work. However, the Supreme Court made no further reference in its judgment in *Canadian Association of Internet Providers* to the liability of referral service intermediaries (providing "manual" hyperlinks to third party sites) either in its discussion of section 2.4(1)(b) or its discussions concerning authorizing infringement. Nonetheless, it is arguable that the Court will consider referral services as means that are "necessary" in that they are "reasonably useful and proper to achieve the benefits of enhanced economy and efficiency"[144] to communicate the work to the public, such as to acquire the protection of section 2.4(1)(b).

IV. CHINA

37. Under Article 10 of the Chinese Copyright Act, a copyright owner may authorize another person to exercise any of the property rights in copyright and receive remuneration pursuant to an agreement or the Copyright Act.[145] However, an Internet intermediary's potential liability in secondary liability for "authorizing infringement" does not appear to be founded on Article 10. Instead, courts in China have founded an intermediary's liability on fault-based principles such as negligence, or on principles of joint or accessory liability.

Fault-based Liability

38. An example of fault-based principles of secondary liability can be found in *Music Copyright Society of China v. Netease Com., Inc. & Mobile Communications Corp.*[146] In this case, the court analyzed the issue of the liability of Mobile Communications, a mobile operator, on the alternative bases of primary liability for direct infringement of the right of information network dissemination, or secondary liability for its negligence in its duty to examine a work it was disseminating, or its failure to act within its power to stop the transmission of an infringing work after it was so informed by the copyright owner.[147]

Joint or Accessory Liability

39. An example of joint or accessory liability can be found in the case of *Go East Entertainment Co. Ltd. (H.K.) v. Beijing Century Technology Co., Ltd.* (*ChinaMP3.com*

---

[142] Id. 110.
[143] Id. 25.
[144] Canadian Association of Internet Providers, 91.
[145] Chinese Copyright Act, Art. 10.
[146] Music Copyright Society of China v. Netease Com., Inc. & Mobile Communications Corp., (2002) Er Zhong Min Chu No. 3119 (No.2 Intermediate People's Court of Beijing Municipality, Sept. 20, 2002).
[147] See e.g., Music Copyright Society of China v. Netease Com., Inc. & Mobile Communications Corp., (2002) Er Zhong Min Chu No. 3119 (No.2 Intermediate People's Court of Beijing Municipality, Sept. 20, 2002).

case)[148] In this case, the court found that though the defendant, who operated the website chinamp3.com, was not liable for disseminating the plaintiff's sound recordings by merely linking to them, by selecting, organizing and finalizing the various links to infringing third party sources, it demonstrated that it could discriminate between licensed and unlicensed recordings, and its ignorance of its own duties and intentional participation in the illegal dissemination of unlicensed recordings made it jointly liable with the third party websites under Article 130 of the General Principles of the Civil Law.[149] The principle of this rule is encapsulated as "contributory infringement liability" in Article 3 of the Interpretations of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network 2006:[150]

In case an Internet Service Provider is involved in any other person's act of infringement on copyright through the network, or abets any other person to commit or assists any other person in committing an act of copyright infringement, the people's court shall subject the Internet Service Provider and other doers or persons directly committing the infringement act to the contributory infringement liabilities according to the provisions of Article 130 of the General Principles of the Civil Law.

40. Likewise, in *Shanghai Push Sound Music & Entertainment Co., Ltd. v. Beijing FashioNow Co. Ltd.*,[151] the court found the defendants, developers and operators of the P2P website and client software Kuro, liable, pursuant to Article 130 of the General Principles of the Civil Law, in contributory infringement for intentionally providing assistance to its users who shared and infringed the rightholder's copyright in its recordings. The court emphasized the right integration between the P2P client software and the system of selection, classification and categorization of the users' shared recordings which the defendants operated on their website.

41. It is also arguable that the Chinese courts have developed a doctrine similar to that of inducing infringement through a seeming judicial gloss put on Article 4 of the Interpretations of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network 2006,[152] which states:

In case an Internet Service Provider providing content services is aware of the internet users' act of infringement on any other people's copyright through the network, or has been warned by the copyright owner with good evidences, but fails to take such measures

---

[148] Go East Entertainment Co. Ltd. (H.K.) v. Beijing Century Technology Co., Ltd., (2004) Gao Min Zhong Zi No. 713 (Beijing High Court, Dec. 2, 2004).

[149] See also Peter Ganea and Thomas Pattloch, INTELLECTUAL PROPERTY LAW IN CHINA 264 (The Netherlands: Kluwer Law International, 2005).

[150] Article 3 of the Interpretations of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network 2006 was previously Article 4 of the Interpretations of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network 2003, which was referred to in the case.

[151] Shanghai Push Sound Music & Entertainment Co., Ltd. v. Beijing FashioNow Co. Ltd., (2005) Er Zhong Min Chu Zi No. 13739 (Beijing No. 2 Intermediate Court, Dec. 19, 2006).

[152] Article 4 of the Interpretations of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network 2006 was previously Article 5 of the Interpretations of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network 2003, which was referred to in the case.

as removing the infringement contents so as to eliminate the consequences of the infringement, the people's court shall, in accordance with the provisions of Article 130 of the General Principles of the Civil Law, impose contributory infringement liabilities on the Internet Service Provider and the internet users.

42. In the *ChinaMP3.com* case, the Beijing High Court interpreted the predecessor provision to Article 4 as applying only to an Internet service provider who is *not at fault*. In this case, the court concluded that the defendant service provider was at fault in selecting, organizing and finalizing links to infringing recordings, and was thus denied the defense implied in the article (that the defendant intermediary would only be liable if it knew of the users' acts of infringement or had been so warned and had failed to take measures to remove the infringing contents). In other words, the fact that the plaintiff rightholder did not serve any notice to enable the defendant to take measures to remove the infringing links was held not to be relevant to the issue of the defendant's contributory liability. It appears that the *ChinaMP3.com* court chose not to interpret Article 4 to find that the defendant service provider was *constructively* "aware of the Internet users' acts of infringement," which would have brought it within the scope of contributory infringement for joint or accessory liability as provided for in Article 4. In other words, for contributory infringement for joint or accessory liability to apply, there must be evidence of the defendant intermediary's *actual* knowledge of the infringement. What the courts did not define however is the scope and extent of this actual knowledge required.

Safe Harbor Defenses - Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006

Conduit or Passive Transmission Defense

43. The conduit or transmission defense was successfully advanced by a mobile operator in *Music Copyright Society of China v. Netease Com., Inc. & Mobile Communications Corp.*,[153] where the court accepted that Mobile Communications was merely providing a technical and passive service of network dissemination for receiving ringtones sent by Netease and forwarding them to its subscribers. The Beijing Intermediate Court accepted evidence that Mobile Communications was unable to select, examine or selectively delete the contents of the messages (comprising the ringtones) it transmitted, and was thus under no duty and not at fault for the occurrence of the infringement when Netease used Mobile Communications' services to transmit unlicensed ringtones to its subscribers.

44. The *Netease* case, which was decided in 2002, is noteworthy because it pre-dates the promulgation of the Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006. Article 20 of the said Regulations has now partially codified the *Netease* defense for Internet intermediaries providing "automatic access" or "automatic transmission" services, in that it would not be liable to compensate the rightholder in damages. The conditions are that the network service not choose or alter the transmitted works, and that the transmitted works be offered only to its subscribers (described in Article 20 as "designated service objects").

---

[153] Music Copyright Society of China v. Netease Com., Inc. & Mobile Communications Corp., (2002) Er Zhong Min Chu No. 3119 (No.2 Intermediate People's Court of Beijing Municipality, Sept. 20, 2002).

Caching Defense

45. The Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006 was formulated based, *inter alia*, on the United States DMCA safe harbor defense for Internet intermediaries. Article 21 of the Regulations provide that a network service provider that caches works, performances and audio-visual products ("materials") from another network service provider "for the purpose of elevating the efficiency of network transmission," it would not be liable to compensate the rightholder in damages, if (i) it did not alter any of the automatically cached materials, (ii) it did not affect the originating network service provider's ability to obtain information about use of the cached materials, and (iii) it automatically revises, deletes or disables access to the materials where the originating network service provider does the same.

Hosting Defense

46. The safe harbor defense for Internet intermediaries providing hosting services is spelt out in Articles 14 to17, and 22 of the Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006. Articles 14 to17 describe the "notice and take-down and put-up" regime, in which the rightholder may file a written notice with the relevant service provider providing the name, contact information and address of the rightholder, the names of the infringed works, performances and audio-visual products ("materials") and their web addresses and documents that provide preliminary evidence that the materials are infringing and requesting that the service provider delete them.[154] Upon receipt of the take-down notice, the service provider shall "immediately delete" the relevant materials, and at the same time, transfer the notice to the subscriber who made the materials available.[155] The subscriber may issue a "put-up" notice in the form of a written statement requesting that the service provider restore the deleted materials, by supplying his contact information, the names of the materials and submitting documents that provide preliminary evidence that the materials are non-infringing.[156] The service provider on receipt of the notice shall immediately restore the materials and transfer the put-up notice to the rightholder, who cannot further request that the materials be deleted or access disabled.[157]

47. Article 22 protects the intermediary from liability to compensate the rightholder in damages, if (i) it clearly indicates that the hosting services are provided to its subscriber and publicizes the service provider's name, contact person and network address, (Internet intermediary) it does not alter the works, performances and audio-visual products ("materials") made available by its subscriber, (iii) it has no knowledge of and has no justifiable reason to know that the materials are infringing, (iv) it does not obtain any direct economic benefit from the provision of the materials, and (v) upon receiving a take-down notice from the rightholder, it acts to delete the materials according to the Regulations. Thus, in *Shanghai Xinchuan Online Co. Ltd. v. Tudou.com Co. Ltd.*,[158] the defendant,

---

[154] Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006, Article 14.
[155] Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006, Article 15.
[156] Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006, Article 16.
[157] Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006, Article 17.
[158] Shanghai Xinchuan Online Co. Ltd. v. Tudou.com Co. Ltd., (2007) Hu Yi Zhong Min Wu (Zhi) Chu Zi No. 129 (Shanghai No. 1 Intermediate Court, Mar. 10, 2008).

operator of the popular video sharing website www.tudou.com, was held liable and unable to rely on the Article 22 defense because the movie shared on its site, "The Crazy Stone," was a popular movie, and that by organizing the movies uploaded by its users into various channels, it knew of the possibility that infringing movies would be uploaded on its website. Thus, its negligence in overseeing and monitoring these uploads and failure to expeditiously remove these infringing uploads disqualified it from the safe harbor defense.

48. The hosting defense in Article 22 only applies to service providers who host third party materials. Where it is the service provider who puts up the materials for dissemination to the public, it becomes the content provider and is not entitled to the safe harbor defense.[159]

Referring Defense

49. A defense for Internet intermediaries providing referring services is set out in Articles 14-17 and 23 of the Regulations on the Protection of the Right to Network Dissemination of Information Networks 2006. The procedure for serving take-down and put-up notices has been previously described in relation to hosting service providers and are equally applicable to intermediaries providing referring services.

50. In *EMI Group Hong Kong Limited v. Beijing Baidu Network Technology Co. Ltd.*, the Beijing District High Court rejected EMI's claim against the search engine Baidu on the grounds that EMI's take-down notice to Baidu did not comply with the requisite formalities, and failed to specify the names of the works, their authors and the web addresses where the infringing works were found.[160] The court did not cite Article 14 of the Regulations. Instead, the court cited Article 8, Paragraph 1 of the Interpretations of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network (2004), which states:

Where any copyright owner who, upon finding out the infringing information, warns the Internet service provider about this or requests for the network registration material of the infringer, [but] is unable to produce proofs of his [the copyright owner's] identification, ownership of the copyright and the circumstance of the infringement, such warning or request shall be deemed not to have been made.[161]

51. Article 23 protects an intermediary offering referring services from liability to compensate the rightholder in damages. However, Article 23 also provides that if the intermediary knows or ought to know that the material it has linked to is infringing, it shall be subject to joint liability. In *Zhejiang FanYa Co. Ltd. (5fad.com) v. Beijing Yahoo! China & Alibaba Information Technology Co. Ltd.*,[162] the Beijing Intermediate Court interpreted these provisions harmoniously to mean that if the rightholder did not exhaust its obligations to

---

[159] See e.g., 2.12 Shanghai Push Sound Music & Entertainment Co., Ltd. v. Beijing Yobo Century Technology Co. Ltd., (2008) Hai Min Chu Zi No. 6939 (Beijing Haidian District People's Court, Jun. 23, 2008).

[160] EMI Group Hong Kong Limited v. Beijing Baidu Network Technology Co. Ltd., (2007) Gao Min Zhong Zi No. 593 (Beijing District High Court, Nov. 17, 2006).

[161] This official translation of Article 8 of the Interpretations of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Cases Involving Copyright Disputes over Computer Network 2004 is provided by the PRC Ministry of Commerce, http://english.ipr.gov.cn/ipr/en/info/Article.jsp?a_no=1972&col_no=118&dir=200603 (accessed 12 Feb. 2009).

[162] Zhejiang FanYa Co. Ltd. (5fad.com) v. Beijing Yahoo! China & Alibaba Information Technology Co. Ltd., (2006) Er Zhong Min Chu Zi No. 07905 (Beijing No.2 Intermediate Court, Dec. 15, 2006).

notify an intermediary providing referring services through take-down notices, and there is no evidence to suggest that the intermediary knows or ought to know that the material it has linked to is infringing, the rightholder cannot maintain a secondary liability claim against the intermediary. *EMI Group Hong Kong Limited v. Beijing Baidu Network Technology Co. Ltd.*, the Beijing District High Court opined that search engines are prima facie not liable for linking to infringing resources because their indexing engines could not predict, distinguish or control the contents of unrestricted websites they searched.[163] The court appears to take judicial notice that the automated operation of search engines implies that it could not be proved as against the search engine operator that it knows or ought to know that the material the engine links to is infringing.

52. In contrast, in *Go East Entertainment Co. Ltd. (H.K.) v. Beijing Alibaba Technology Co., Ltd.*,[164] the Beijing High Court found the defendant search engine Alibaba liable for only taking down 15 of the 26 allegedly infringing recordings pursuant to the take-down notices. Although the defendant only removed those 15 recordings because the plaintiff rightholder supplied web links to them, the court held that after it has received the take-down notices, it should know that its search engine services contained infringing links to all 26 recordings, and that it was negligent in the discharge of its duty to take steps to terminate the links to the other recordings. Its failure to act to remove all the recordings was an indulgence in the infringement, and Alibaba was held jointly liable with the users.

V. EGYPT

Law on the Protection of Intellectual Property Rights

53. In 2002, Egypt repealed its 1954 Law on the Protection of Copyright and replaced it with the new Law on the Protection of Intellectual Property Rights 82 of 2002 ("IP Law"). Book 3 of the IP Law sets out the law of copyright in Egypt, Article 147 provides as follows:

The author and his universal successor shall have the exclusive right to authorize or prevent any form of exploitation of his work, particularly through reproduction, broadcasting, re-broadcasting, public performance, public communication, translation, adaptation, rental , lending or making the work available to the public in any manner, including through computers, internet, information networks, communication networks and other means.

54. On the issue of whether secondary liability is recognized in the copyright law of Egypt, some Egyptian experts have opined that the copyright law of Egypt recognizes that "providing accessories for infringing the exclusive rights or assisting in the making or distribution of infringing copies" is also treated as an infringement.[165] This appears to be borne out by the breadth of Article 147, which refers to "any manner" of exploitation of the author's work "through computers, the Internet, information networks, communication networks and other means". An alternative view is that the IP Law does not contain any provisions that explicitly impose liability upon Internet intermediaries for acts of

---

[163] EMI Group Hong Kong Limited v. Beijing Baidu Network Technology Co. Ltd., (2007) Gao Min Zhong Zi No. 593 (Beijing District High Court, Nov. 17, 2006).
[164] Go East Entertainment Co. Ltd. (H.K.) v. Beijing Alibaba Technology Co., Ltd., (2007) Er Zhong Min Chu Zi No. 02627 (Beijing High Court, Dec. 20, 2007).
[165] See Egyptian Center for Intellectual Property and Information Technology, Copyright & Related Rights, http://www.ecipit.org.eg/English/Copyright_E.aspx (last visited Dec. 9, 2010).

infringement by third parties, or absolve them for liability.[166] Support for this view may be drawn from the recent decision by the Egyptian State Council Administrative Court's decision to overturn the Egyptian telecommunications regulator's decision to require mobile operators and satellite broadcast firms to monitor news feeds.[167]

Transient Copies and Internet Intermediaries as Conduits

55. Analysis of the issue of secondary liability for Internet intermediaries should also take into account Article 171, which is the main exemption provision in Egyptian copyright law. Article 171(9) absolves from the infringement of the economic copyright rights of the author, the making of ephemeral reproductions of works made when a digitally stored work it is relayed, transmitted or received, "within the normal operation of the device used by an authorized person". On its face, Article 171(9) seems to circumscribe the breadth of Article 147, by absolving instances of incidental copyright infringement from transient copies of works made through authorized transmissions. This leaves open the issue of whether Internet intermediaries as conduits would be liable for copyright infringement through their transmissions of *unlicensed* works, for either primary or secondary liability. On the other hand, because of the narrowness of Article 171(9), it could be argued that Article 147 is intended to encompass and render primarily and secondarily liable all activities of Internet intermediaries, including transmission, caching, storing and linking services, unless the services are provided in relation to *licensed* works.

56. Aside from Article 171(9), no statutory safe harbors have been enacted to indemnify Internet intermediaries in Egypt for the provision of services.

VI. INDIA

Authorizing Infringement

57. Section 14 of the Indian Copyright Act 1957 states that copyright means the exclusive right to do or "authorize the doing" of the enumerated acts in respect of a work. Section 51 also states copyright in a work is infringed if a person does the exclusive rights of copyright conferred on the rightholder without the rightholder's license.[168] Thus authorizing another to commit any of the enumerated rights in respect of the work without the license of the rightholder would be an infringement.

58. At the time of this report, there have been no cases dealing with authorizing infringement in India.[169] Indian courts have cited the U.K. decision of *Falcon v. Famous Players Film Co.*[170] and the Australian decision of *Moorhouse v. University of New South Wales.*[171] However, the Indian courts have not given any indication as to which interpretation of the term "authorize" they would adopt. Whichever interpretation is given to the scope of

---

[166] See Consumers International IP Watchlist Report 2010: Appendix A: Country Reports - Egypt 2010, a2knetwork.org, http://a2knetwork.org/reports2010/egypt (last visited Dec. 9, 2010).
[167] See Egypt's court overturns telecom news monitoring, Reuters, Nov. 27, 2010, http://www.reuters.com/article/idUSTRE6AQ12V20101127.
[168] Indian Copyright Act, 1957, s. 51(a)(i).
[169] Sneha Jha and Samar Jha, An Analysis of the Theory of Contributory Infringement, (2006) 11 J. Intellec. Prop. Rights 318, 324.
[170] See Om Prakash v. Radhey Shyam Kathawachak, AIR 1945 All 55 (Allahabad High Ct.).
[171] See Suprecassette Industries v. Nirulas Corner House (P) Ltd., 148 (2008) DLT 487 (Delhi High Ct.).

authorizing infringement in India, the secondary liability of Internet intermediaries for copyright infringement has however been substantially limited by legislation.

Statutory Safe Harbors and the Information Technology (Amendment) Act 2008

59. The position of Internet intermediaries in India has to be considered by reading the Indian Copyright Act 1957 together with the Information Technology Act 2000 (as amended by the Information Technology (Amendment) Act, 2008) ("IITA"). The latest set of amendments came into force on 27 October 2009 and has introduced far reaching changes to the regime for dealing with online service providers ("OSPs") in India. The safe harbor indemnity is set out in section 79 of the IITA.

60. The IITA 2008 introduced a new definition for an "intermediary," defined as follows:

"intermediary," with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.[172]

61. Unlike the safe harbor provisions considered generally in this paper, which are limited in their application to the intermediary's liability for copyright infringement, the operative provision of the safe harbor, section 79, provides for a "non-obstante" clause. In other words, the indemnity that an intermediary acquires from liability "for any third party information, data, or communication link made available or hosted by him" applies "notwithstanding anything contained in any law for the time being in force". Adopting a harmonious interpretation with section 81 of the same act,[173] it therefore "significantly heightens the level of immunity available to service providers" in India.[174] It should also be noted that it operates as a "horizontal immunity" in that its application is not confined to indirect liability for copyright infringement.

62. To qualify for the safe harbor immunity, three conditions must be observed by the Internet intermediary:

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or

(b) the intermediary does not

(i) initiate the transmission,
(ii) select the receiver of the transmission, and
(iii) select or modify the information contained in the transmission;

---

[172] Indian Information Technology Act 2000, as amended by the Information Technology (Amendment) Act 2008, § 2(w).
[173] Aditya Gupta, The Scope of Online Service Providers' Liability for Copyright Infringing Third Party Content under Indian Laws, (2010) J. Intellec. Prop. Rights 35, 37. The amended section 81 provides that nothing in the IITA "restrict[s] any person from exercising any right conferred under the Copyright Act, 1957 or the Patents Act, 1970". Thus there is an apparent inconsistency between s. 79 and s. 81 of the IITA.
[174] Id., 36.

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.[175]

63. These three conditions appear to be disjunctive conditions – the "or" prescribed in section 79(2)(a) suggests that these conditions may be satisfied in the alternative. The reference to "providing access to a communication system" suggests that section 79(2)(a) applies to telecom service providers and ISPs as intermediaries. Web-hosting service providers and search engines would appear to qualify for indemnity under section 79(2)(b), in that these are intermediaries that do not initiate the transmission, select the receiver of the transmission and select or modify the information contained in the transmission, although it remains to be seen if the "crawling" aspect of a search engine's operations will qualify as a transmission which is not initiated by the intermediary.

64. Service providers that providing caching services are conspicuously absent from the definition of "intermediaries," although it can be contended that caching services are linked to an intermediary's function in providing access to content (and may be consequential to the provision of access to a communication system) as set out in section 79(2)(a).

65. The third condition is based upon the decision of the High Court of Delhi in *Avinsh Bajaj v. State*,[176] in which the court rejected a petition for annulling the criminal prosecution of a website that carried a listing which offered for sale a mobile phone video clip of two students engaged in an explicitly sexual act. The court held that the website had failed to exercise due diligence, because it failed to provide filters to screen pornographic content and failed to introduce any policy to prevent the listing, display or sale of such content on the website. However, as implemented in section 79(2)(c), this is one of three *disjunctive* conditions for qualifying for immunity. If so, this implies that a website that satisfies one of the first two conditions will qualify for immunity (subject to ensuring that the exceptions to the immunity in section 79(3), discussed below, are not satisfied), even though it did not "observe due diligence while discharging its duties and observing such other guides as the Central Government may prescribe".

66. Section 79(3) sets out two preclusions to the broad immunity otherwise enjoyed by intermediaries in section 79(1). These are: (a) where the intermediary "has conspired [in] or abetted [in] or aided or induced" the "unlawful act," or (b) where the intermediary fails to expeditiously remove or disable access to the unlawful material upon receiving actual knowledge or upon being notified by "the appropriate Government or its agency" that any material ("information, data or communication link") residing in or connected to a resource controlled by the intermediary is being used to control the unlawful act. The first preclusion appears to import the concept of "authorizing infringement" to disentitle the intermediary to the section 79(1) immunity.[177] If so, the immunity will fail to protect an intermediary where a rightholder can maintain a case of authorizing infringement against the intermediary. Given that most intermediaries will not be directly infringing but their exposure to liability will be for authorizing infringement, if this interpretation is correct, this represents a very big lacuna in the immunity spelt out in section 79(1).

67. The second preclusion in relation to take-down notices is a modification of the take-down notice procedure as spelt out in section 512(c) of the United States DMCA. The

---

[175] Indian Copyright Act, s. 79(2).
[176] Avinsh Bajaj v. State, 150 (2008) DLT 279 (Delhi High Ct.).
[177] Gupta, The Scope of Online Service Providers' Liability, supra, note at 38.

differences are that the notice here is served by a Government agency, rather than a rightholder, and there is no mechanism for a counter-notice.

VII. JAMAICA

"Exclusive right to do or to authorize other persons"

68. The owner of the copyright in a work under Jamaican copyright law has the exclusive right "to do or authorize other persons to do" any of the enumerated acts of copyright in Jamaica.[178] And copyright is infringed by "any person who, without the license of the copyright owner, does, in relation to that work, any of the acts which the copyright owner has the exclusive right to do".[179]

69. As of the date of this report, there have been no cases decided by the Jamaican courts that have resolved the issue of secondary liability for copyright infringement. However, the language of sections 9 and 31 of the Jamaican Copyright Act appears to afford support the view that the Act recognizes secondary liability, and suggests that Internet intermediaries may be liable for the copyright infringements of their users as third parties. For instance, a Jamaican ISP has written into its acceptable user policies provisions rules that state that it is a violation of its user agreements for users to use its ISP services for purposes of infringing copyright.[180]

70. The current Jamaican Copyright Act took as its basis English copyright law, and incorporated various United States copyright law influences, particularly with respect to the defense of "fair use" (described as "fair dealing" in the Jamaican Copyright Act). It is thus open to Jamaican courts to adopt the U.K. judicial interpretation of "authorizing infringement" to found secondary liability. It is also open to Jamaican courts to adopt the three heads of vicarious liability, contributory infringement and inducing infringement developed by the U.S. courts to found secondary liability in Jamaica.

Absence of Safe Harbor Immunities

71. There are currently no safe harbor immunities enacted in Jamaican copyright law to indemnify Internet intermediaries for their secondary liability for copyright infringement.

VIII. JAPAN

The *Karaoke* Principle

72. An author enjoys the exclusive rights of copyright provided in the Japanese Copyright Act,[181] and the author (or the rightholder as transferee of the copyright by the author)[182] may authorize another person to exploit the work which is the subject of his copyright.[183]

---

[178] Jamaican Copyright Act 1993, § 9(1).
[179] Jamaican Copyright Act 1993, § 31(1).
[180] See FlowJamaica, Acceptable Use Policy, http://www.flowjamaica.com/index.php?option=com_content&task=view&id=284 (last visited Dec. 9, 2010);
[181] Japanese Copyright Act, Art. 17(1).
[182] Japanese Copyright Act, Art. 61(1).
[183] Japanese Copyright Act, Art. 63(1).

However, until the *Club Cat's Eye/Singing at a Karaoke Lounge* case in 1988,[184] it was unclear as to whether there could be an action for infringement against a secondary defendant where it is the primary defendant who has committed the act of copyright infringement.

73. In the *Club Cat's Eye/Singing at a Karaoke Lounge* case, the issue before the Supreme Court was whether the defendant, a snack bar, was liable for the musical performance by its customers who had sang on the karaoke equipment and licensed tapes provided by the defendant and had to pay additional license fees to Japanese Society for Rights of Authors, Composers and Publishers (JASRAC). In answering this question in the affirmative, the leading judgment by the Japanese Supreme Court emphasized that the snack bar's hostesses and employees had encouraged their customers to sing to the music and the customers' singing to singing by the snack bar management as part of their business strategy. Subsequently, in the *Video Mates* case,[185] the Supreme Court further applied the *Karaoke* principle to hold liable a karaoke equipment lessor who had leased karaoke equipment to a lessee without first verifying that the lessee had concluded a copyright licensing agreement with JASRAC. It held, among others, that as most works played by karaoke equipment were subject to copyright, that it was likely that such equipment would be used in the infringement of copyright unless there was consent from the copyright owner. It also held that the lessor profited from such leasing arrangements and that it was easy for the lessor to verify that the lessee had concluded a licensing agreement with JASRAC. Thus, by merely advising the lessee to conclude such an agreement without actually verifying it, the lessor had breached its reasonable duty of care owned to JASRAC, and that it was due to this breach that infringement took place and losses were suffered by JASRAC.

74. In addition to founding liability on the duty of care that the secondary defendant owed to the rightholder, Japanese courts have also held the secondary defendant liable to the rightholder as a joint tortfeasor with the primary infringer. In the *Miruku* case,[186] on a fact situation similar to that in *Video Mates*, the Osaka High Court found in favor of JASRAC in its claim against the defendant karaoke equipment lessor.

75. It was on these principles that Japanese courts have found liable the Internet service provider MMO Japan Ltd, for offering the File Rogue file sharing service which enabled its users to search for and share unlicensed music files. In the *File Rogue* case,[187] the court held that the defendant's service enabled a high degree of illegal use and that there was no evidence that licensed MP3 files were shared. Also, the defendants were aware of the nature of the files exchanged based on the names and song titles, and that they had exercised control or supervision over their users' conduct because they were in a position to take the necessary steps to prevent copyright infringement, even if it was impossible to detect all infringements. Furthermore, even though the service was currently free, the provider intended to charge fees for its use and that its services were profit-oriented. On this basis, the court held that the provider had contributory infringed the music rightholders' rights.

---

[184] Club Cat's Eye/Singing at a Karaoke Lounge, 1984 (O) No.1204 (1988) (Japanese Sup. Ct., Mar. 15, 1988).
[185] Supply of Karaoke Equipment for Business Use ("Video Mates" Case), 2000 (Ju) No.222 (2001) (Japanese Sup. Ct., Mar. 2, 2001).
[186] Japanese Society for Rights of Authors, Composers and Publishers v. Miruku Bar & Anor., HANREI JIHO (No. 1624) 131 (27 Feb. 1997, Osaka High Ct.).
[187] File Rogue, Heisei 16 (Ne) 446 (2003) (Tokyo High Ct., Mar. 31, 2005).

76. The degree of control and management which the intermediary has over the activities of the user appears to be the key factor to determine if there has been contributory infringement. In *Rokuga Net*,[188] the Japanese Intellectual Property High Court held a service provider liable for providing a for-profit service that involved the re-transmission of free-to-air broadcasts received in Japan to overseas users via the Internet. In contrast, in *Maneki TV*,[189] the service provider was held *not* liable for providing a for-profit service that also involved a re-transmission of free-to-air Japanese broadcasts to users via the Internet. The distinction between these two cases appears to turn on the technical setup of the defendant service providers and the degree of control exercised by the providers: the provider in Rokuga Net managed the entirety of his own setup and equipment for recording and transmitting the rightholders' broadcasts, whereas the provider in Maneki TV required the user to purchase a piece of equipment (a Location-Free TV "base station") which was actually owned and remotely operated by the users, and that the provider was only entrusted with them.[190] Whether or not it is correct to actually downplay the role of the service provider in Maneki TV would turn on factual considerations such as the fact that Maneki "operated" each of the user's "base station" by largely providing connectivity services, and that each "base station" was a stand-alone piece of equipment for recording and transmitting TV programming over the Internet. But these factual distinctions upon which to conclude that the requisite degree of control and management had been established to found contributory infringement may be hard to discern.[191]

77. However, if the recent decision by the Osaka High Court in the *Winny II* decision[192] (a criminal prosecution case) is any indication, Japanese courts may be adopting a more discriminatory approach towards accessory liability and joint tortfeasorship. Although the defendant in Winny II developed P2P software for file sharing, the court considered this "value-neutral technology" in that it could be used for both infringing and non-infringing purposes. To be held liable for distributing "value-neutral technology," it had to be shown that the defendant distributor had to recognize that the software was used for illegal activities and had to recommend its use only or mainly for illegal activities. In overturning the conviction of the defendant, the court held that being merely aware of such a possibility that the software could be abused did not constitute aiding or abetting in violations of the law.

Act on the limitation of liability for damages of specified telecommunications service providers

78. In November 2001, the Japanese Diet passed a new law to regulate the online infringement of third party rights, including defamation, copyright infringement and privacy violations. Enacted as the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers 2001, it is also known as the Provider Liability

---

[188] Rokuga Net, 2005 (Ra) No.10007, 10008, 10009, 10010, 10011, 10012 (Intellectual Property High Court, Nov. 15, 2005).
[189] Maneki TV, 2006 (La) No. 10012 (Tokyo District Court, Jun. 20, 2008).
[190] Kazuo Ohtake, Two IPHC Decisions on the Infringement of Neighbouring Rights (May 2007), http://www.asialaw.com/Article/685066/Article.html (accessed 19 Feb. 2009).
[191] See e.g., "Yoridori-midori"/Hard Disk Video Recorder System (2005 (Wa) No.488) (24 Oct. 2005, Osaka District Court, 26th Civil Division, Japan); "Rokuraku" (30 Mar. 2007, Tokyo District Court), aff'd "Rokuraku II" (28 May 2008, Tokyo District Court).
[192] High court overturns guilty ruling against developer of file-sharing software Winny, MAINICHI DAILY NEWS (8 Oct. 2009), at http://mdn.mainichi.jp/mdnnews/news/20091008p2a00m0na016000c.html.

Law. The law applies to "specified telecommunications service," which is defined in Article 2(i) of the Provider Liability Law as follows:

> The term "specified telecommunications service" means transmission (except transmission of telecommunications (hereinafter in this item only referring to "telecommunications" as defined in Article 2 item i) of the Telecommunications Business Law(Law No. 86 of December 25, 1984)) with the aim of *direct reception* thereof by the public) of telecommunications with the *aim of reception thereof by unspecified persons.* (emphasis added)

79. Article 3(1) of the Provider Liability Law indemnifies a "specified telecommunications service provider" for any infringement that occurs where the service provider distributes a third party's communications (that is, the provider is not the sender of the infringing communications). However, this indemnity does not apply where (a) it is technically feasible to take measures to prevent the transmission of the infringing communications,[193] and (b) the provider either (i) knows of the infringement by distributing the communications,[194] or (ii) knows of the information in the communications and could reasonably know of the infringement by distributing the communications.[195]

80. Article 3(2) of the Provider Liability Law indemnifies the provider from any loss incurred by the sender of the communications by disabling such communications. The provider may do so where there were reasonable grounds for the provider to believe that rights of others were infringed without due cause by the distribution of the communications.[196] Alternatively, the provider may do so where it receives a petition filed by a person who alleges his right is infringed, and upon relaying the petition to the communication sender, the provider does not, within 7 days, receive any notice from the sender indicating that he disagrees with the allegation of infringement and with the blocking measures to be implemented by the provider.[197]

81. Several observations can be made about the Provider Liability Law. First, the indemnity applies not just to secondary liability for copyright infringement, but operates in a fashion similar to the "horizontal exceptions" in the EC's E-Commerce Directive to exempt the provider "for any loss incurred from such infringement". Secondly, only a "specified telecommunications service provider" qualifies for the indemnity. As defined, this does not include a telecommunications service provider providing "direct reception" of telecommunications. This would appear to preclude from its ambit ISPs who operate as conduits for "direct reception" of communications from sender to recipient. On the other hand, this would include hosting service providers and referral service providers, who distribute communications "with the aim of reception by unspecified persons". This could be justified on the basis that ISPs as conduits would not be liable in any event for transmitting communications, and would not be obliged to take measures to filter communications. Neither are they obliged to disable their senders' communications.

---

[193] Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers 2001, Art. 3(1).
[194] Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers 2001, Art. 3(1)(i).
[195] Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers 2001, Art. 3(1)(ii).
[196] Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers 2001, Art. 3(2)(i).
[197] Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers 2001, Art. 3(2)(ii).

82. Finally, the indemnification regime set out in the Provider Liability Law does not oblige the telecommunications service provider to pro-actively monitor and filter the communications it transmits. Where it becomes feasible to take technical measures to filter such communications, the provider has little obligation or incentive to implement them because to do so will be to attract knowledge of infringing communications, which will disqualify it from the Article 3(1) indemnity, and potentially require it to take steps, presumably expeditiously, to disable the communications to qualify for the Article 3(2) indemnity. However, the Provider Liability Law is silent as to whether disabling the communications restores to the provider the Article 3(1) indemnity from an action by the party aggrieved by the infringing communications, although from a factual standpoint, the extent of the damage caused by disabling the infringing communications will be reduced. On the other hand, a provider faces increased liability if it intentionally ignores complaints and risks aggravating its exposure to damages if it fails to take remedial action.[198] This puts a provider in a difficult catch-22 situation not unlike that faced by Internet intermediaries in the United States and the DMCA safe harbours.[199]

IX. MALAYSIA

Malaysian Copyright Act

83. Section 36 of the Malaysian Copyright Act provides that copyright is infringed by any person "who does, *or causes any other person to do*," (emphasis added) without the license of the copyright owner, an act the going of which is controlled by copyright in the Act. Although there have been no decided cases on secondary liability for "causing another person to commit an infringing act," the language of section 36 provides ample support for a Malaysian court to found liability.

84. As the law of copyright in Malaysia can be traced to the U.K. Copyright Act 1911, U.K. cases on the elements of "authorizing infringement" will be highly persuasive to Malaysian courts. As noted below in the discussion of U.K. cases, because of the emphasis on control that a secondary defendant has to exercise over a primary infringer to be held liable for "causing" the primary infringer to commit an infringing act, if a Malaysian court were to apply the line of U.K. authorities, it is generally unlikely to find an Internet intermediary liable for the acts of its users or subscribers.

Communications and Multimedia Act

85. Perhaps it is for this reason that no safe harbor provisions exists in the Malaysian Copyright Act to protect or indemnify Internet intermediaries. Instead, section 263 of the Malaysian Communications and Multimedia Act ("CMA") reads:

General duty of licensees.

(1) A licensee shall use his best endeavor to prevent the network facilities that he owns or provides or the network service, applications service or content applications service that

---

[198] J. Dax Hansen and Keiji Sugiyama, A Web of rules: how the Internet is affecting Japanese content liability, privacy and consumer protection laws - Case Study, BNET – THE CBS INTERACTIVE BUSINESS NETWORK (Nov. 2002), http://findarticles.com/p/articles/mi_m0NTN/is_37/ai_108882018/.

[199] See e.g., Mark A. Lemley, Rationalizing Internet Safe Harbors, STANFORD PUBLIC LAW WORKING PAPER NO. 979836 (Apr. 10, 2007), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=979836.

he provides from being used in, or in relation to, the commission of any offence under any law of Malaysia.

(2) A licensee shall, upon written request by the Commission or any other authority, assist the Commission or other authority as far as reasonably necessary in preventing the commission or attempted commission of an offence under any written law of Malaysia or otherwise in enforcing the laws of Malaysia, including, but not limited to, the protection of the public revenue and preservation of national security.

86. Section 264 of the CMA goes on to indemnify a licensee and its employees from liability in any criminal proceedings of any nature for any damages suffered, whether directly or indirectly, for any act or omission done in good faith in its performance of its section 263 duty.

87. The CMA is the legal and regulatory framework for the telecommunications, broadcasting and online industries in Malaysia. Within the framework, providers of network facilities (including telecommunications and broadcast equipment and stations), network services, application services and content applications. Internet intermediaries operating in Malaysia will fall within the definition of a "licensee" and be required to "use his best endeavors" to prevent his facilities or services "from being used in, or in relation to, the commission of any offense under any law of Malaysia". Internet intermediaries in Malaysia are thus not protected from secondary liability, and though in practice, they do not practice filtering (presumably because section 264 does not indemnify the licensees from civil liability), that is set to change. In August 2009, the Malaysian government announced a proposal to introduce an Internet filtering system operating at the Internet gateway level, to be overseen by the Ministry of Information, Communications and Culture.[200] Although the Malaysian government appears to have resiled from the proposal,[201] it remains to be seen if this will trigger a practice of self-censorship against infringing content by Malaysian Internet intermediaries.

X. NEW ZEALAND

Australian performing right association ltd. V. Koolman

88. The leading decision on secondary liability in New Zealand is the Supreme Court decision of *Australian Performing Right Association Ltd. v. Koolman.*[202] Referring to the English decisions of *Performing Right Society Ltd. v. Ciryl Theatrical Syndicate Ltd.*[203] and *Falcon v. Famous Players Film Co. Ltd.*,[204] the court took the view that the question of authorization was largely one of fact. It also referred to Australian decisions and held that as the defendant's coffee bars were under its control and management, by receiving the admission charge from its patrons, it was conducting a public performance by impliedly authorizing the band or booking agency to select the music the band played. Likewise, by

---

[200] Niluksi Koswanage, Malaysia examines Internet filter, tougher controls, Reusters, Aug. 6, 2009, http://www.reuters.com/article/idINSP37415520090806.
[201] Razak Ahmad and Royce Cheah, Malaysia backs off Internet filter plan, Reuters, Aug. 7, 2009, http://www.reuters.com/article/idUSKLR48361520090807; Niluksi Koswanage and Razak Ahmad, Malaysia to cancel Internet filter – source, Reusters, Aug. 12, 2009, http://www.reuters.com/article/idUSKLR53468220090812.
[202] Australian Performing Right Association Ltd. v. Koolman, [1969] NZLR 273 (N.Z. Sup. Ct.).
[203] Performing Right Society Ltd. v. Ciryl Theatrical Syndicate Ltd. [1924] 1 K.B. 1.
[204] Falcon v. Famous Players Film Co. Ltd., [1926] 2 K.B. 474.

installing the jukeboxes on its premises and making the records available for selection, the defendants had authorized the performance of the plaintiff's music.

89. A learned commentator has observed that *Koolman* is notable for the thin line drawn between primary liability (actually having conduct of the infringement) and secondary liability (authorizing the infringement).[205] It should also be noted that *Koolman* was decided on the 1962 edition of the New Zealand Copyright Act, and the 1994 edition of the New Zealand Copyright Act appears to characterize the fact situation in *Koolman* as primary infringement.[206] However, these statutory provisions deal with performances of recordings and audio-visual works and the supply of equipment thereto in premises, and thus the issue of the secondary liability of Internet intermediaries as network service providers has to be resolved with reference to common law principles of authorizing infringement. In deciding this issue, it remains to be seen whether New Zealand courts are more inclined to follow the conservative approach of the U.K. courts, starting with *Falcon v. Famous Players Film Co. Ltd.*,[207] or whether they would follow the approach taken by the Australian courts, as illustrated by the case of *Moorhouse v. University of New South Wales.*[208] In any event, because of amendments made to the New Zealand Copyright Act to introduce the graduated response law, it is now a moot point that an Internet intermediary may be liable for authorizing the infringing activities of its user.[209]

Statutory Safe Harbors for ISP Liability

90. Pursuant to a major review of the New Zealand Copyright Act 1994 initiated in 2001, the New Zealand government introduced the Copyright (New Technologies and Performers' Rights) Amendment Bill in 2006. This was eventually passed as the Copyright (New Technologies) Amendment Act 2008.

91. Internet intermediaries are defined in the revised Copyright Act as "Internet service providers" (hereinafter "ISPs" in the ensuing discussion about the NZ Copyright Act) to encompass providers of transmission, routing and connection services (usually described as "Internet service providers" in technical texts, but not in the Act), and hosting service providers.[210] To deal with the issue of their exposure to both primary and secondary liability, provisions were introduced to address this issue in three circumstances.

92. Section 92B, modeled after the Agreed Statement to Article 8 of the WIPO Copyright Treaty 1996, states that an ISP does not infringe the copyright in a work (for both primary[211] as well as secondary[212] infringement) "merely because" the ISP's user used those services to infringe the copyright in the work. However, this indemnity does not limit the rightholder's ability to seek injunctive relief against the ISP.[213]

---

[205] Andrew Brown and Anthony Grant, THE LAW OF INTELLECTUAL PROPERTY IN NEW ZEALAND 376 (1989).
[206] New Zealand Copyright Act, ss. 38, 39.
[207] Falcon v. Famous Players Film Co. Ltd., [1926] 2 K.B. 474.
[208] Moorhouse v. Univ. of N.S.W., (1975) 133 C.L.R. 1, [1976] R.P.C. 151 (High Ct. Austl.) [hereinafter Moorhouse].
[209] The Explanatory Note to the Copyright (New Technologies and Performers' Rights) Amendment Bill 2006 affirms, without citing further authority, that an Internet intermediary may face potential liability for both primary and secondary infringement of copyright.
[210] New Zealand Copyright Act, s. 2 (definition of "Internet service provider").
[211] New Zealand Copyright Act, s. 92B(2)(a) ("does not infringe the copyright in the work").
[212] New Zealand Copyright Act, s. 92B(2)(b) ("must not be taken to have authorized [the user's] infringement of copyright in the work").
[213] New Zealand Copyright Act, s. 92B(3).

93. Section 92C, modeled after section 512(c) of the United States DMCA, states that an ISP who provides hosting services for a user does not infringe copyright in the hosted work unless it knows or has reason to believe that the material infringes copyright[214] and does not delete or prevent access to it, as soon as possible after becoming so aware.[215] After deleting or prevent access to the material, the ISP has to give notice to the user of what it has done.[216] However, as is the case in section 92B, the indemnity does not limit the rightholder's ability to seek injunctive relief against the ISP.[217]

94. Section 92E, modeled after section 512(b) of the United States DMCA, states that an ISP who caches infringing material does not infringe copyright, provided it does not modify the material, complies with conditions imposed by the copyright owner for the material for access to that material, does not interfere with the lawful use of technology to obtain data on the use of the material and updates the cached material in accordance with reasonable industry standards.[218] However, the ISP "does infringe" by continuing to cache the material if it became aware that the material had been deleted from its original source, or access to it had been prevented or a court has so ordered the material to be deleted or access to be denied.[219] Likewise, as is the case in sections 92B and 92C, the indemnity does not limit the rightholder's ability to seek injunctive relief against the ISP.[220]

95. Officially, the position taken by the New Zealand government is that no safe harbor provision is required to protect ISPs providing referral or linking services from liability, because the provision of such services will not constitute copyright infringement.[221]

Graduated Response

96. One of the most controversial provisions introduced in the New Zealand Copyright (New Technologies) Amendment Act 2008 is a condition in section 92A that an ISP "must adopt and reasonably implement a policy that provides for termination, in appropriate circumstances, of the account with that ISP of a repeat infringer," defined as a user who uses one or more of the ISP's services "to do a restricted act without the consent of the copyright owner".[222] While other provisions of the Amendment Act 2008 took effect, the implementation of section 92A was delayed until March 2009. ISPs and rightholders had attempted to negotiate an effective Code of Practice to describe who a repeat infringer was, but under strong protests from Internet users and interest groups, who regard the section and the Code as introducing "guilt by accusation,"[223] New Zealand's second largest ISP, TelstraClear, announced its withdrawal from the proposed Code. Under

---

[214] New Zealand Copyright Act, s. 92C(2)(a)(i).
[215] New Zealand Copyright Act, s. 92C(2)(a)(ii).
[216] New Zealand Copyright Act, s. 92C(4).
[217] New Zealand Copyright Act, s. 92C(5).
[218] New Zealand Copyright Act, s. 92E(1).
[219] New Zealand Copyright Act, s. 92E(2).
[220] New Zealand Copyright Act, s. 92E(3).
[221] Nate Anderson, New ACTA leak shows major resistance to US-style DRM rules, ARSTECHNICA, Mar. 2010, http://arstechnica.com/tech-policy/news/2010/03/new-acta-leak-shows-major-resistance-to-us-style-drm-rules.ars.
[222] New Zealand Copyright Act, s. 92A.
[223] Wikipedia, New Zealand Internet blackout, http://en.wikipedia.org/wiki/New_Zealand_Internet_Blackout.

pressure, the New Zealand Cabinet announced on 23 March 2009 that section 92A would not come into force, and will be amended to address areas of concern.[224]

XI. NIGERIA

"Cause any other person to do an [unlicensed] act"

97. Under section 5 of the Nigerian Copyright Act, copyright is the exclusive right "to do and authorize the doing of any of the [enumerated] acts" of copyright.[225] And by section 14 of the Copyright Act, copyright is infringed by any person "who without the license or authorization of the owner of the copyright" "does, *or cause any other person to do an act*, the doing of which is controlled by copyright".[226]

98. As of the date of this report, there have been no cases decided by the Nigerian courts regarding what constitutes secondary liability. However, the language of section 14 appears to amply support the view that the Nigerian Copyright Act recognizes secondary liability, as it describes copyright as infringed by any person who "cause[s] any other person to do" an act of copyright infringement. This suggests that Internet intermediaries may be liable for the copyright infringements of their users as third parties.[227]

Absence of Statutory Safe Harbors

99. Currently, no statutory safe harbors exist for Internet intermediaries to limit their exposure to secondary liability in Nigerian copyright law.

XII. REPUBLIC OF KOREA

The *Soribada* Decision

100. The Korean Copyright Act provides that the basis of infringing liability may be intentional infringement or negligent infringement. Article 125 of the Korean Copyright Act provides that the copyright owner may claim compensation for damages against an infringer who has infringed his rights "intentionally or by negligence". (In contrast, a distinction is made as regards the penal sanctions in the Copyright Act between an intentional and a negligent copyright infringement or one made by a person lacking in the knowledge of the fact that the act causes or conceals an infringement).[228]

101. Does the Korean Copyright Act recognize secondary liability, and if so, does it fall under the rubric of intentional or negligent infringement? The leading decision on secondary liability is the *Soribada* decision decided by the Korean Supreme Court in 2007,[229] which confirms that the Korean Copyright Act protects all direct and indirect acts that facilitate a breach of copyright. In a series of civil and criminal complaints mounted by the record

---

[224] Simon Power, Minister of Commerce, Government to amend Section 92A, Press Release: New Zealand Government, Mar. 23, 2009, http://www.scoop.co.nz/stories/PA0903/S00330.htm.
[225] Nigerian Copyright Act, s. 5(1).
[226] Nigerian Copyright Act, s. 14(1)(a).
[227] See also Consumers International IP Watchlist Report 2010: Appendix A: Country Reports – Nigeria 2010, a2knetwork.org, http://a2knetwork.org/reports2010/nigeria (last visited Dec. 9, 2010).
[228] Korean Copyright Act, Article 136 Paragraph (2)-6.
[229] Soribada, 2005 Da 11626 (2007) (Sup. Ct. Rep. of Korea, Jan. 25, 2007).

labels against the defendants, developers of the Soribada P2P file sharing service (which went through several iterations in the course of the proceedings), the court also affirmed that either negligence or willful conduct leading to aiding and abetting may be a basis of secondary liability against an Internet intermediary. On the facts, the court found the defendant provider liable for negligently assisting in the copyright infringement as it had breached the obligation to be cautious not to assist in the infringement of copyright – the defendant need not be specifically aware of the details of the work infringed, the actual act or the identity of the actual infringer. The court also held the defendants liable for aiding and abetting in the users' infringing use of the Soribada service because they were aware that the service had infringing uses but they nonetheless still developed and freely distributed the software and service, thereby facilitating the infringement of the rightholders' copyright.

102. The use of the tortious standard of negligence necessitates the court's resolution of the further issue of what constitutes the obligation to be cautious. In the ensuing *Soribada* litigation, the defendants modified the Soribada software introduce a "passive filtering system," which would deny a user's request to download a file for which the copyright holder had specifically requested protection. Sustaining the rightholders' application for a preliminary injunction against the defendants, the Seoul High Court held that the defendant service provider would only be absolved if it had used its best efforts to use technical measures to prevent copyright infringement, and the "passive filtering system" did not amount to its use of best efforts. Instead, the court would have preferred the use of an "affirmative filtering system," in which a user could only download music files for which the provider had a license.[230]

Statutory Safe Harbors to Reduce or Waive Liability

103. Special provisions to regulate and protect "online service providers" ("OSPs"), defined as persons who "provide others with services that reproduce or interactively transmit works, etc. through information and communication networks",[231] were introduced into the Korean Copyright Act in 2003 (originally as Chapter 5-2). There are two classes of "online service providers" whose activities are regulated: OSPs providing services "related to the reproduction or interactive transmission of works etc," and "special" OSPs "whose main purpose is to enable different people to interactively transmit works etc". The latter class of "special OSPs" would encompass hosting companies and P2P providers.[232]

104. Article 102 provides that the liability of OSPs *may* be reduced or waived in cases where it prevents or stops an allegedly infringing reproduction or transmission when it is so "made aware".[233] Its liability *shall* be waived where it attempts to prevent or stop an allegedly infringing reproduction or transmission, but it is "technically impossible to do so".[234] In this regard, Article 102 operates differently from the safe harbor provisions in the DMCA in that it does not provide a qualifying OSP with a complete indemnity against secondary liability: the preventive measures undertaken by the OSP only serve to limit or reduce its liability, and only provide a complete indemnity when these measures are "technically" infeasible or ineffective to prevent or stop the infringing activity.

---

[230] Soribada, 2006 La 1535 (2007) (Seoul High Ct., Oct. 10, 2007).
[231] Korean Copyright Act, Art. 2, sub-para 30.
[232] Jaick Kim, Consumers International IP Watchlist Report 2010: Appendix A: Country Reports - Republic of Korea, a2knetwork.org, Feb. 20, 2009, http://a2knetwork.org/reports/south-korea.
[233] Korean Copyright Act, Art. 102(1).
[234] Korean Copyright Act, Art. 102(2).

105. An OSP may be "made aware" of the infringing activity pursuant to the notice and take-down procedures spelt out in Article 103, in which a rightholder may request that an OSP shall "immediately stop the reproduction or interactive transmission" of such works and give notice to the person who reproduced or interactively transmitted such works. This person (referred to as the reproducer/transmitter in Article 103) may in turn issue the OSP a "put up" notice to request resumption of these works, by proving that he is doing so "based on legitimate rights," whereupon the rightholder will be promptly notified of the resumption.[235] The OSP shall designate an agent for receipt of these take-down notices.[236] An OSP that is "made aware" of the infringing activity pursuant to the take-down notice and acts to stop the reproduction or interactive transmission of the works (or restore access to such works pursuant to the "put up" notice) *may* have its damages (to the rightholder and to the reproducer/transmitter) reduced or waived.[237] However it should be noted that this partial indemnity does not apply to the OSP's liability between the times it gains knowledge of the infringing activity to the time it receives the take-down notice.[238]

106. Additionally, Article 104, enacted in 2006, imposes an additional obligation on special OSPs.

It states:
Article 104 (Liability, etc. of Special Types of Online Service Providers)
(1) Online service providers whose main purpose is to enable different people to interactively transmit works, etc. among themselves by using computers, etc. (hereinafter referred as "special types of online service providers") shall take necessary measures such as technological measures intercepting illegal interactive transmission of works, etc. upon the requests of rights holders. In such cases, matters related to requests of rights holders and necessary measures shall be determined by the Presidential Decree.
(2) The Minister of Culture and Tourism may determine and notify the scope of special types of online service providers in accordance with Paragraph (1).

107. An OSP who fails to take the necessary measures prescribed in Article 104 shall be subject to penal sanctions and "shall be punished by a fine for negligence not exceeding thirty million won".[239] This has been interpreted to require special OSPs like hosting companies and P2P service providers to implement filters or monitor the distribution of potentially infringing copyright material.[240] Thus, in 2008, the Seoul Central Prosecutors' Office prosecuted NHN corporation, the operator of Naver, the largest Internet portal in Republic of Korea, and Daum Communications Co., the operator of Daum, another Internet portal, for aiding copyright infringement, because they had ignored requests from the Korea Music Copyright Association and the Korea Association of Phonogram

---

[235] Korean Copyright Act, Art. 103(3).
[236] Korean Copyright Act, Art. 103(4).
[237] Korean Copyright Act, Art. 103(5). In a recent case, the Seoul Southern District Court ordered the rightholder to compensate the reproducer/transmitter, who uploaded a clip of his daughter singing and dancing to a famous Korean female singer's song, for damages suffered from the take-down notice served on the portal site Naver, an OSP. The court held that this was a fair use of a copyrighted work. Naver was however exempted from the obligation to compensate the father. See Wonil Chung, Seoul Court Ruled Uploading a 15-Second Video of Toddler's Dancing to a Famous Singer's Song Is Not a Copyright Infringement and the Copyright Holder Who Sent an Unfair Take Down Notice Should Pay a Monetary Compensation, 2010, http://korealaw.wordpress.com/2010/10/05/ucc/.
[238] Id.
[239] Korean Copyright Act, Art. 142(1).
[240] Jaick Kim, Consumers International IP Watchlist Report 2010: Appendix A: Country Reports - South Korea, a2knetwork.org, Feb. 20, 2009, http://a2knetwork.org/reports/south-korea.

Producers to remove illegal music files on their sites and took no action in response to the requests.[241]

Graduated Response

108. In March 2009, Korea's National Assembly's Committee on Culture, Sports, Tourism, and Broadcasting & Communications passed a bill to amend the Korean Copyright Act to include the world's first graduated response system. As provided in Article 133-2, where illegal copies of works or information circumventing technological protection measures are transmitted ("illegal copies"), the Minister of Culture, Sports and Tourism may order an OSP to issue warnings against its reproducers/transmitters and even delete or suspend the transmission of these illegal copies.[242] A reproducer/transmitter who has received three or more warnings may have his account(s) suspended by the OSPs as ordered by the Minister.[243] A bulletin board, a type of OSP, may also have its services suspended by the Minister if it has received three or more warnings to delete or suspend the transmission of illegal copies, and "is considered to seriously damage the sound use of works in the light of the format of the corresponding bulletin board, the amount or nature of copies posted on it etc".[244] The suspension may be for up to a period of 6 months.[245] Before the accounts are suspended, the reproducer/transmitter and the bulletin board will be given an opportunity to submit an opinion to the Minister.[246]

109. Some Korean websites that host user-generated content have contended that these rules are unfair, because in spite of their deployment of filtering software and personnel to monitor and remove copyrighted content, some content will remain available long enough to be flagged by the government. Concerns have been expressed as to how much money Korean web portals to spend to filter and monitor copyright violations, and how it is relatively easy for the Korean government to find three instances of infringing activities and order the web portals shut down.[247]

---

[241] Wonil Chung, Two Korean Internet Portal Giants Prosecuted for Aiding Copyright Infringement, (Dec. 29, 2008), http://korealaw.wordpress.com/2008/12/29/two-internet-portal-giants-prosecuted-for-aiding-copyright-infringement.

[242] Korean Copyright Act, Art. 133-2(1).

[243] Korean Copyright Act, Art. 133-2(2). (3).

[244] Korean Copyright Act, Art. 133-2(4).

[245] Korean Copyright Act, Art. 133-2(2), (4).

[246] Korean Copyright Act, Art. 133-2(7).

[247] See e.g., Kim Tong-hyung, Upload a Song, Lose your Internet Connection - New Copyright Law Causes Uproar Among Bloggers, Internet Companies, KOREA TIMES, May 4, 2009, http://www.koreatimes.co.kr/www/news/tech/2010/05/133_42594.html; Mark Hefflinger, South Korea Adopts "Three-Strikes" Law on File-Sharing, DIGITAL MEDIA WIRE, Apr. 16, 2009, http://www.dmwmedia.com/news/2009/04/16/south-korea-adopts-%2526quot%3Bthree-strikes%2526quot%3B-law-file-sharing.

XIII. SINGAPORE

Authorizing Infringement and *Ong Seow Pheng*

110. The leading case on authorizing infringement in Singapore is the Court of Appeal decision of *Ong Seow Pheng v. Lotus Development.*,[248] In this case, the court followed the U.K. decisions of *CBS Songs Ltd. v. Amstrad Consumer Electronics Plc.*[249] and *CBS Inc. v. Ames Records & Tapes Ltd.*[250] and held that a secondary defendant would be liable for authorizing infringement if it had "sanctioned, approved or countenanced" the primary infringer's infringement. The court clearly preferred the view that to "authorize an act" means "to grant or to purportedly grant the right to do the act complained of," and construed the test of authorization set out by the Australian High Court in *Moorhouse v. University of New South Wales*[251] to apply only where the secondary defendant had control over what the primary defendant could do with the infringing material. Thus, on the facts of *Ong Seow Pheng*, the court held that the secondary defendants were not liable for authorizing the infringement of the primary defendant by simply passing one copy of an unlicensed piece of software to the primary defendant, a known software pirate, who then made the requisite copies for subsequent sale and distribution.

111. This narrow interpretation suggests that generally, it is difficult to hold an Internet intermediary liable for the infringing conduct of its subscribers. Applying a narrow reading of *Ong Seow Pheng*, the intermediary would have merely provided the means for infringement, and could in no way control the activities of users. As the court in *Ong Seow Pheng* said:

> *We accept that Ong, the defendant and secondary infringer, supplied Lur, the primary infringer, with a copy of the programme [sic] together with the manuals. In doing so, he might well have suggested to Lur that copies of the programmes [sic] could be made. However, that is [sic] was a far cry from saying that the appellants thereby authorized Lur to make copies of the programme [sic]. He might have facilitated, and even incited, Lur's infringements, but as was held in CBS Songs and Amstrad, that is not the same thing as authorization. As the learned judge held, and we agree with her, once the appellants had sold and delivered the infringing copies of the manuals or programmes [sic] to Lur, these copies were out of their hands and they had no control over what Lur would do with reference to them. Clearly, the Moorhouse case has no application here.*[252]

112. The narrowness of the *Ong Seow Pheng* decision presumably led the Singapore High Court in the recent case of *RecordTV Pte Ltd v. MediaCorp TV Singapore Pte Ltd*[253] to strain to find "authorizing infringement" on the facts of the case.[254] This the court did by reading into the terms and conditions of the service offered by the RecordTV, an Internet intermediary that offered remote-store digital video recorder ("RS-DVR") services,[255] a

---

[248] Ong Seow Pheng v. Lotus Development Corp., [1997] SGCA 23, [1997] 3 S.L.R 137 (C.A. Sing.).
[249] CBS Songs Ltd. v. Amstrad Consumer Elec. Plc., [1988] A.C. 1013 (H.L.) (Eng.), aff'g Amstrad Consumer Elec. Plc. v. British Phonographic Indus. Ltd., [1986] F.S.R. 169 (H.C. & C.A. Eng.).
[250] CBS Inc. v. Ames Records & Tapes Ltd., [1982] Ch. 91 (H.C. Eng.).
[251] Moorhouse v. Univ. of N.S.W., (1975) 133 C.L.R. 1, [1976] R.P.C. 151 (High Ct. Austl.) [hereinafter Moorhouse].
[252] Ong Seow Pheng, [1997] SGCA 23, [34].
[253] RecordTV Pte Ltd v. MediaCorp TV Singapore Pte Ltd, [2009] SGHC 287 (Sing. H.C.).
[254] Id., [68], [110].
[255] The RS-DVR service enabled users to time shift their video programming online. The court called this an iDVR service. Id., [5].

statement that it had secured "all necessary regulatory licenses" to be a representation to its (infringing) users that it had actual authority to provide its service to end users.[256] This, coupled with the court's conclusion that users were not entitled to make time-shifted recordings of programming online,[257] enabled the court to rule that RecordTV had authorized the infringing recordings made by its users. An appeal has however been filed by RecordTV and at the time of this report, the case is before the Court of Appeal.

Statutory Safe Harbor Defenses

113. In 1999, Singapore made its first amendments to the Copyright Act to introduce various safe harbor defenses for Internet intermediaries as network service providers. Arising from its obligations under the U.S. Singapore Free Trade Agreement,[258] Singapore further revised in 2004 the safe harbor defenses in the Copyright Act for network service providers. By seeking to shield a network service provider from any damages for copyright infringement, the safe harbor defenses seem to tacitly recognize liability for authorizing infringement beyond that set out in *Ong Seow Pheng*.[259]

114. Section 193A of the Copyright Act states that the safe harbor defenses are to apply to "network service providers," which includes ISPs as intermediaries providing services and connections for data transmission or routing, as well as intermediaries who provide or operate facilities for online services or network access. It would seem that "network service providers" are broadly defined so that most Internet intermediaries would qualify for the safe harbor defenses. However, in *RecordTV*, the High Court chose to interpret section 193A to apply only to "bona fide" network service providers.[260] The court did not explain what it meant by a "bona fide" network service provider, only that as RecordTV made copies of the rightholders' programming, it was not considered one that is bona fide.[261] With respect, however, this judicial gloss placed on the safe harbor defenses appears to be erroneous and is not supported by the plain language of section 193A.

115. The four safe harbor defenses mirror the same defenses in the United States Digital Millennium Copyright Act. Section 193B, modeled after section 512(a) of the United States DMCA, indemnifies an ISP (as a subclass of a "network service provider") from monetary relief for any copyright infringement that occurs by reason of the transmission, routing, provision of connections or transient storage by the ISP of an electronic copy of the material. To qualify for this defense, the transmission must be initiated by a person (other than the ISP), the transmission must be carried out without any selection of the material, the ISP must not select the recipients of the material except by way of an automatic response, and the ISP must not make any substantive modifications to the material during its transmission.[262] In *RecordTV*, the Internet intermediary sought to bring itself under this safe harbor defense. This was rightly rejected by the court, because the operations of

---

[256] Id., [42].
[257] Id., [57] (holding that the s. 114(3) defense of time-shifting did not apply), [109] (holding that the safe harbor and fair dealing defenses did not apply).
[258] United States – Singapore Free Trade Agreement, May 6, 2003, available at http://www.ustr.gov/assets/Trade_Agreements/Bilateral/Singapore_FTA/Final_Texts/asset_upload_file708_4036.pdf (last visited May 15, 2008); United States – Singapore Free Trade Agreement Implementation Act, Pub. L. 108-78, 117 Stat. 948 (2003) (codified in scattered sections of 8 & 19 U.S.C.).
[259] Second Reading of the Copyright (Amendment) Bill 2005, 80 SING. PARL. DEBATES, OFFICIAL REPORT (July 18, 2005) 779 (Professor S. Jayakumar, Deputy Prime Minister and Minister for Law).
[260] RecordTV, [91].
[261] Id.
[262] Sing. Copyright Act § 192B(2).

RecordTV could hardly be characterized as an "automatic technical process"[263] of an ISP, although it would have been easier for the court to dismiss this defense simply on the grounds that RecordTV is *not* an ISP.

116. Section 193C of the Singapore Copyright Act, modeled after section 512(b) of the United States DMCA, indemnifies a network service provider for making, through an automatic process, a cached copy of a work on its network from the originating network, in response to a user's action, in order to facilitate efficient access to the material by its users. The conditions are that the network service provide not make any substantive modifications to the content of the cached copy,[264] and if it is furnished with a take-down notice, it is to expeditiously take reasonable steps to remove or disable access to the cached copy of the work on its network.[265] In addition, it has to satisfy other conditions that the Minister may prescribe, including conditions relating to access to the copy, the refreshing, reloading or updating of the cached copy and non-interference with any technology used by the originating network to obtain information about usage of the material.[266]

117. Section 193D of the Singapore Copyright Act, modeled after sections 512(c) and (d) of the United States DMCA, indemnify a network service provider for providing hosting and referral services from monetary relief for any copyright infringement arising from its activities. To qualify for protection, a network service provider providing hosting services that involve storing an electronic copy of the infringing material on its work must not receive any direct financial benefit from the infringement, and has to designate a representative to receive the prescribed take-down notices.[267] Likewise, a network service provider providing referral or linking services must not receive any direct financial benefit from the infringement, and has to designate a representative to receive the prescribed take-down notices.[268] The hosting or referring network service provider will lose the indemnity if upon acquiring actual knowledge or such facts or circumstances "which would lead inevitably to the conclusion" of infringement, or is furnished with a prescribed take-down notice, it does not expeditiously take reasonable steps to remove or disable access to the infringing material.[269] Section 193D would appear to be a better safe harbor defense that is applicable to the Internet intermediary in *RecordTV*. However, this safe harbor defense was not pleaded by the intermediary in that case.

118. Notwithstanding the safe harbor conditions which a network service provider has to observe to qualify for indemnity, section 193A of the Copyright Act states that a network service provider is not obliged to monitor its service or affirmatively seeking facts to indicate infringing activity, or to gain access to, remove or disable access to any infringing material.[270] However, to qualify for the safe harbors, a network service provider has to adopt and reasonably implement a policy for termination of repeat offenders, and must accommodate and not interfere with standard technical measures for identification or protection of copyrighted material.[271]

---

[263] RecordTV, [93]-[94].
[264] Sing. Copyright Act § 193C(2)(a).
[265] Sing. Copyright Act § 193C(2)(b).
[266] Sing. Copyright Act § 193C(2)(c).
[267] Sing. Copyright Act § 193D(2)(a), (c).
[268] Sing. Copyright Act § 193D(4)(a), (c).
[269] Sing. Copyright Act § 193D(2)(b) proviso, (4)(b) proviso.
[270] Sing. Copyright Act § 193A(3).
[271] Sing. Copyright Act § 193DE(2)(b); Sing. Copyright (Network Service Provider) Regulations 2005, Reg. 8 (Rg 7, 2009 Rev. Ed.).

XIV. SOUTH AFRICA

"Causing any other person to do"

119. Section 23 of the South African Copyright Act states:

Copyright shall be infringed by any person, not being the owner of the copyright, who, without the licence of such owner, does or causes any other person to do, in the Republic, any act which the owner has the exclusive right to do or to authorize. (emphasis added)

120. To date, there have been no cases decided by the South African courts regarding what constitutes authorizing infringement. Academic writing has suggested that secondary liability (also described as third party liability) falls within the terms of section 23(1) of the Copyright Act, as distinct from "secondary infringement"[272] or "contributory negligence" (which deal with infringements arising from commercial dealings in unlicensed copyright works).[273] The language of section 23(1) amply supports this conclusion, as it describes copyright as infringed by any person who "causes any other person to do" an act of copyright infringement. Although the enactment of the statutory indemnities for Internet intermediaries in the Electronic Communications and Transactions Act 2002 has somewhat relieved obviated the issue of secondary liability, as the Act explicitly preserves the position at common law, the limits of liability for authorizing infringement may still be pleaded by Internet intermediaries where they do not qualify for one of the four safe harbor indemnities as set out in the Act.[274]

Electronic Communications and Transactions Act 2002

121. In 2002, in conjunction with revisions made to the South African Copyright Act, the South African parliament enacted the Electronic Communications and Transactions Act 2002. It is intended to be a comprehensive restatement of the law as it relates to electronic communications and transactions, and encompasses provisions ranging from electronic commerce to electronic signatures, from consumer protection to the limitation of Internet intermediary liability. The Internet intermediary provisions, modeled after the United States DMCA, introduces four safe harbors defenses for Internet intermediaries, defined as "service providers" providing "information system services". The term "information system services" is in turn defined as:

includes the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the individual request of the recipient of the service.[275]

122. Section 73 indemnifies a service provider for operating facilities and services as a "mere conduit" "for information systems or transmitting, routing or storage of data messages".[276] This includes the "automatic, intermediate and transient storage of information

---

[272] See Fiona Margaret Polak, Copyright and Digital Music Collections in South Africa 72, Dec. 2009, http://researchspace.ukzn.ac.za/xmlui/bitstream/handle/10413/1253/Polak_F_2009.pdf (citing Dean, O.H. 1987-2006, 1 HANDBOOK OF SOUTH AFRICAN COPYRIGHT LAW 44. (loose leaf, updated regularly) Kenwyn: Juta).

[273] See Roux de Villiers, Copyright and the Internet, http://www.cyberlawsa.co.za/cyberlaw/cybertext/chapter2.htm - 8 (last visited Dec. 9, 2010).

[274] South Africa Electronic Communications and Transactions Act 2002, §§ 73(3), 74(2), 75(3).

[275] South Africa Electronic Communications and Transactions Act 2002, § 1.

[276] South Africa Electronic Communications and Transactions Act 2002, § 73(1).

transmitted" for this purpose.[277] It must not initiate the transmission, select the addressee, modify the transmitted data contents and must perform the function in an automatic, technical manner without selection of the data.[278]

123. Sections 74 indemnifies a service provider for caching data to make transmissions more efficient, provided it does not modify the data or interfere with lawful use of technology to obtain usage information about the data, and it complies with conditions on access to the data and industry rules for updating the data.[279] In addition, it has to remove or disable access to the data in response to a take-down notice.[280]

124. Section 75 indemnifies a service provider from damages for providing hosting services (storage of data that is "provided by a recipient of the service"), as long as it does not have actual knowledge that the data or activity relating to the data is infringing third party rights, is not aware of facts or circumstances from which the infringing nature of the data or activity is apparent, and upon receipt of a take-down notice, "acts expeditiously" to remove or disable access to the data.[281] To qualify for this indemnity, it has to designate an agent to receive infringement notifications and has to publicize the agent's information.[282]

125. Section 76 indemnifies a service provider from damages for providing "information location" services, in referring or linking users to a web page that contains infringing content or infringing activity, as long as it does not have actual knowledge that the data or activity relating to the data is infringing third party rights, is not aware of facts or circumstances from which the infringing nature of the data or activity is apparent, does not receive a financial benefit directly attributable to the infringing activity, and upon receipt of a take-down notice, acts "within a reasonable time" to remove or disable access to the data.[283]

126. In addition, to qualify for the all safe harbor indemnities, the service provider has to be first a member of an industry representative body for Internet intermediaries – the Internet Service Providers' Association, and has to adopt and implement the official code of conduct[284] of that representative body.[285] Unlike the United States DMCA ,where the only formality is the registration of the designated agent with the Register of Copyrights. [286] This has the effect that only South African service providers within a closed group of the industry will qualify for the indemnity.

127. The "horizontal" nature of the safe harbor indemnities must also be noted: service providers qualifying for indemnity are generally exempted from all liability, except in relation to obligations founded on an agreement, licensing and regulatory obligations, and any court or legal obligations to remove, block or deny access to "data message".[287] In addition, notwithstanding the broad indemnities, the statutory safe harbors may

---

[277] South Africa Electronic Communications and Transactions Act 2002, § 73(2).
[278] South Africa Electronic Communications and Transactions Act 2002, § 73(1)(a)-(d).
[279] South Africa Electronic Communications and Transactions Act 2002, § 74(1)(a)-(d).
[280] South Africa Electronic Communications and Transactions Act 2002, § 74(1)(e).
[281] South Africa Electronic Communications and Transactions Act 2002, § 75(1)(a)-(c).
[282] South Africa Electronic Communications and Transactions Act 2002, § 75(2).
[283] South Africa Electronic Communications and Transactions Act 2002, § 76(a)-(d).
[284] Internet Service Providers' Association, Code of Conduct, http://www.ispa.org.za/code-of-conduct (last visited Dec. 9, 2010) [hereinafter ISPA Code].
[285] South Africa Electronic Communications and Transactions Act 2002, § 72.
[286] 17 U.S.C. § 512(c)(2).
[287] South Africa Electronic Communications and Transactions Act 2002, § 79.

nonetheless still oblige a transmission, caching and hosting provider to terminate or prevent unlawful activities "in terms of any other law".[288] Also, the statutory indemnities do not affect any limitations of liability at common law or based on the South African Constitution.[289]

128. Although the safe harbor indemnities absolve the service provider of a general obligation to monitor the data which it transmits or stores, or actively seek facts or circumstances indicating an unlawful activity,[290] the Minister may, subject to the Constitution, prescribe procedures for service providers to inform the competent public authorities of its subscribers' alleged illegal activities or illegal information, and communicate information to enable the competent authorities to identify these subscribers.[291] This is reflected in the ISPA's Code of Conduct, which requires an ISPA member who becomes aware of conduct or content which has been determined to be illegal to terminate the relevant customer's service and report it to the relevant law enforcement authority.[292] The ISPA has also codified a notification and take-down procedure for unlawful content and activity, which *all* ISPA members *voluntarily*[293] comply with by responding expeditiously to such notifications.[294]

129. The Act also sets out provisions for the appointment of "cyber inspectors," who may monitor "any web site or activity on an information system in the public domain and report any unlawful activity to the appropriate authority".[295] Subject to the obligation of confidentiality,[296] cyber inspectors are also given extensive powers to inspect, access and search information systems in the discharge of their functions.[297]

XV. UNITED KINGDOM

"Sanction, approve and countenance"

130. Section 16 of the U.K. Copyright, Designs and Patents Act 1988 provides:
Copyright in a work is infringed by a person who without the licence of the copyright owner does, or authorizes another to do, any of the acts restricted by the copyright.

131. The U.K. courts adopt a narrow view of authorization, and interpret the term "authorization" to mean to "sanction, approve and countenance".[298] As the leading decision of *Falcon v. Famous Players Film Co.* explains, to "authorize" means "to grant or

---

[288] South Africa Electronic Communications and Transactions Act 2002, §§ 73(3), 74(2), 75(3).
[289] South Africa Electronic Communications and Transactions Act 2002, § 79(d).
[290] South Africa Electronic Communications and Transactions Act 2002, § 78(1).
[291] South Africa Electronic Communications and Transactions Act 2002, § 78(2).
[292] ISPA Code of Conduct, para. 24.
[293] ISPA Code of Conduct, paras. 22-27. See also Paul Esselaar, What ISPs can do about Undesirable Content, ISPA 15, May 2008, http://www.ispa.org.za/wp-content/uploads/2010/10/ISP_undesirable_content.pdf (last visited Dec. 9, 2010).
[294] ISPA Code of Conduct, para. 25. See also ISPA, How to request a Take-Down Notice, http://www.ispa.org.za/code-of-conduct/take-down-guide and http://www.ispa.org.za/code-of-conduct/take-down-procedure (last visited Dec. 9, 2010)..
[295] South Africa Electronic Communications and Transactions Act 2002, § 81(1)(a).
[296] South Africa Electronic Communications and Transactions Act 2002, § 84.
[297] South Africa Electronic Communications and Transactions Act 2002, § 82(1).
[298] Falcon v. Famous Players Film Co., [1926] 2 K.B. 474, 498-499 (C.A. Eng.) (Atkin L.J.), subsequently approved in CBS Songs Ltd. v. Amstrad Consumer Elec. Plc., [1988] A.C. 1013, 1055 (H.L.) (Eng.) (Lord Templeman).

purport to grant the right to do the act complained of".[299] A distinction is maintained between facilitating an infringement and authorizing an infringement. As Justice Whitford said in *CBS Inc. v. Ames*, "an act is not authorized by somebody who merely enables or possibly assists or even encourages another to do that act, but does not purport to have any authority which he can grant to justify the doing of the act".[300] Thus, in a finding that there is no "authorizing infringement," the U.K. decisions emphasize the free will of the primary infringer, over whom the secondary infringer has no control. In *CBS Inc. v. Ames*, the fact that the secondary defendant very likely knew[301] or was indifferent to the possibility[302] of the primary infringer infringing copyright by borrowing the recordings lent by Ames thus facilitating infringing home taping was held to be irrelevant. Similarly, in *Amstrad Consumer Electronics Plc. v. British Phonographic Industry Ltd.*, the court observed that even though Amstrad in selling the high speed copying device was "intentionally placing in the hands of purchasers a facility which they must know is inevitably going to be used for the purposes of infringement," this did not warrant a finding of authorization.[303] Likewise, on appeal, in *CBS Songs Ltd. v. Amstrad Consumer Electronic Plc.*, the court described Amstrad's conduct in advertising that its copying device could be used to copy copyrighted works as deplorable and cynical, but held that "the operator of an Amstrad tape recording facility, like all other operators, can alone decide whether to record or play and what material is to be recorded".[304] A recent English High Court decision, *Philips Domestic Appliances & Personal Care B.V. v. Salton Europe Ltd.*, came to the same conclusion. It held that merely passing on something which will inevitably be used for infringement is not authorizing – there being no control over the use of a product once it is sold.[305] Thus most Internet intermediaries are likely to be able to successfully assert that they do not "sanction, approve and countenance" any copyright infringement on the part of users of their facilities, services and software.

132. However, this narrow view of authorization looks set to change. In the most recent decision, *Twentieth Century Fox Film Corp. v. Newzbin Ltd*,[309] the defendant Newzbin.com, a subscription-only search service that indexes Usenet content and categorizes them into films, software, music and so on, was held liable for authorizing its users' infringement. The court found that the categorizations were carried out by editors who were encouraged to do so by the defendant, and the defendant also offered facilities to simplify the download of files by its users. Considering all relevant circumstances, including the nature of the relationship between the defendant and the primary infringer,

---

[299] Id.
[300] CBS Inc. v. Ames Records & Tapes Ltd., [1982] Ch. 91, 106 (Eng.).
[301] Id. at 112.
[302] Id.
[303] Amstrad Consumer Elec. Plc. v. British Phonographic Indus. Ltd., [1986] F.S.R. 169, 211 (C.A. Eng.) (Slade L.J.).
[304] CBS v. Amstrad, [1988] A.C. at 1053.
[305] Philips Domestic Appliances & Pers. Care B.V. v. Salton Europe Ltd., [2004] ECHC. 2092 (Ch.), [44]-[45] (H.C. Eng.).
[306] See e.g. Kazaa Media Desktop End User License Agreement ("EULA"), clause 2.6, available at http://www.oldversion.com/program.php?n=kazaa (last visited May 10, 2008). Although the Kazaa software has been removed from the official Kazaa website, backup copies of the software can still be found at archive sites.
[307] See e.g. CBS Inc. v. Ames Records & Tapes Ltd., [1982] Ch. 91, 107 (H.C. Eng.). Of course, the courts could come to the opposite conclusion that the copyright warning notices were, notwithstanding their inclusion, insignificant and not intended to be seriously regarded.
[308] See e.g. Amstrad Consumer Elec., [1986] F.S.R. at 185-186; Twentieth Century Fox Film Corp. v. Newzbin Ltd, [2010] EWHC at [42], [45].
[309] Twentieth Century Fox Film Corp. v. Newzbin Ltd, [2010] EWHC 608 (Ch), [2010] All ER (D) 43 (Apr), (Eng. Chancery Div.).

the equipment or other material supplied and whether it is inevitable it would be used to infringe, the degree of control which the defendant retains and whether he has taken any steps to prevent infringement, the court held that a reasonable member of the defendant's service would deduce that it possesses the authority to grant any required permission to copy a film from the "Movies" category. The court concluded that the defendant had "sanctioned, approved and countenanced" the copying of the claimants' films,[310] and had so involved itself with the infringement that they were also liable for procurement and participation in a common design with the infringing users.[311]

133. A possible alternative basis for secondary liability can be found in section 24(1) of the U.K. Copyright, Designs and Patents Act 1988, which provides that there is infringement in the copyright in a work by, *inter alia*, the making in the course of a business or engaging in a commercial dealing in "an article specifically designed or adapted for making copies" of a work, knowing or having reason to believe that it is to be used to make infringing copies.[312] However, it has been explained that the "article" referred to in section 24(1) is not one that is generally designed for making copies, but articles such as photographic negatives, moulds, master recordings and other articles which may be used to make copies of specific works.[313] On this interpretation,[314] this section is unlikely to be relevant to Internet intermediaries and their facilities and services since these are not articles, let alone articles "specifically designed or adapted for making copies," given the narrow legal explanation of this expression.

---

[310] Id., [102].
[311] Id., [112].
[312] Copyright, Designs and Patents Act 1988, c. 48, § 24(1) (U.K.) [hereinafter U.K. C.D.P.A.].
[313] KEVIN GARNETT ET AL., 1 COPINGER AND SKONE JAMES ON COPYRIGHT ¶ 8-15 at 464 (15th ed. 2005), [hereinafter COPINGER AND SKONE JAMES].
[314] On this interpretation, the articles themselves ("negatives, moulds, master recordings") are actually copies of the works in a new medium of expression, for which the law of copyright offers protection. See U.K. C.D.P.A. § 27(2) ("An article is an infringing copy if its making constituted an infringement of the copyright in the work in question".). See also Kalem Co. v. Harper Brothers, 222 U.S. 55 (1911) (illustrating that article specifically designed for making infringing copies of a work is itself an infringing copy of the work). Perhaps therefore section 24(1) is intended to refer to articles which are not themselves copies of the specific works.

E-Commerce (EC Directive) Regulations 2002

134. Arising from the EC E-Commerce Directive 2000, the U.K. enacted into the law Electronic Commerce (EC Directive) Regulations 2002. Among the regulations enacted are the safe harbor defenses for "information society service" providers. It should however be noted that these defenses in the Regulations are "horizontal" defenses in that they apply to exempt the service provider of damages, pecuniary remedy and criminal sanctions as a result of the provision of information society services, and not just for liability in copyright infringement.

135. The "conduit defense" in Regulation 17 indemnifies information society service providers providing transmission or access services to communication networks, the service provider is exempt if it did not initiate the transmission, did not select the receiver of the transmission and did not select or modify the information contained in the transmission. The transmission and access include the "automatic, intermediate and transient storage of the information transmitted" which takes place for the sole purpose of carrying out the transmission and the information is not stored for any period longer than is reasonably necessary for the transmission.[315]

136. The "caching defense" in Regulation 18 indemnifies information society service providers that store information pursuant to automatic, intermediate and temporary processes for the sole purpose of making onward transmissions more efficient, and the service provider does not modify the information, complies with conditions for access to the information, complies with industry rules regarding updating of the information, and does not interfere with technology used to obtain data on the use of information. The provider must also act expeditiously to remove or disable access to the cached information upon obtaining actual knowledge that the cached information has been removed from the source network, or access to it has been disabled, or that a court or administrative authority has ordered its removal or disablement.[316]

137. The "hosting defense" in Regulation 19 indemnifies information society service providers for providing information storage services, if it does not have actual knowledge of unlawful activity or information, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful, or upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to that information. The subscriber for the hosting services must also not be acting under the authority or control of the service provider.[317]

138. In determining whether a service provider has actual knowledge for purposes of the caching and hosting defenses in Regulations 18 and 19, the court shall take into account all matters which appear to the court to be relevant in the circumstances, and shall have regard to whether the service provider has received a notice through the means of contact which it has made available, and the extent to which the notice includes the full name and address of the sender, the details of the location of the information in question and the details of the unlawful nature of the activity or information in question.[318]

---

[315] Electronic Commerce (EC Directive) Regulations 2002, Regulation 17(2).
[316] Electronic Commerce (EC Directive) Regulations 2002, Regulation 18(b)(v).
[317] Electronic Commerce (EC Directive) Regulations 2002, Regulation 19(b).
[318] Electronic Commerce (EC Directive) Regulations 2002, Regulation 22.

139. It should be noted that there are no defenses in the Regulations for information society service providers providing referral services. The liability of referral service providers will presumably be determined by the law on authorizing infringement.

Digital Economy Act 2010

140. In June 2010, the U.K. became the fourth country in the world (after Republic of Korea, New Zealand and France) to enact what is known as a "graduated response" law. The Digital Economy Act 2010 imposes obligations on ISPs to notify its subscribers of reported infringements by rightholders,[319] to supply to rightholders a "copyright infringement list" that sets out an anonymous list of its subscribers who have reached a prescribed threshold of infringement reports ("relevant subscribers"),[320] and to take "technical measures" to limit, suspend or terminate Internet services of relevant subscribers.[321] Sections 17 and 18 also empower the Secretary of State to make regulations to get a court order to direct a service provider block access to Internet locations which the court is satisfied is likely to be involved in an activity that infringes copyright. In November 2010, on an application by two U.K. ISPs, the U.K. High Court granted permission for a judicial review of the aforesaid provisions of the Digital Economy Act.[322]

XVI. UNITED STATES OF AMERICA

141. Section 106 of the U.S. Copyright Act provides that the owner of copyright has the exclusive rights "to do and to authorize" any of the rights of copyright.[323] While there is some debate as to whether section 106 provides the statutory basis for secondary liability under U.S. copyright law,[324] there is no doubt that two distinct theories of secondary liability have been developed under U.S. copyright law: "vicarious liability" and "contributory infringement".

Vicarious Liability

142. The accepted view is that "authorizing infringement" in non-U.S. common law jurisdictions such as Australia, Canada and the U.K. is regarded as "a form of vicarious liability for the infringement authorized" under U.S. copyright law.[325] Indeed, the development of vicarious liability under U.S. copyright law is based on an extended interpretation of the tort principle of vicarious liability.[326] The rule today in U.S. copyright law is that "when the right and ability to supervise coalesce with an obvious and direct financial interest in the

---

[319] U.K. Digital Economy Act 2010 (c. 24) § 3.
[320] U.K. Digital Economy Act 2010 (c. 24) § 4.
[321] U.K. Digital Economy Act 2010 (c. 24) §§ 9-12.
[322] Out-law.com, Digital Economy Act to be reviewed by courts and Parliament, Nov. 10, 2010, http://www.out-law.com/page-11538.
[323] U.S. Copyright Act § 106.
[324] See e.g. Brief of Sixty Intellectual Property and Technology Law Professors and the United States Public Policy Committee of the Association for Computing Machinery, as Amici Curiae Supporting Respondents, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 125 S.Ct. 2764 (2005), 2005 WL 508123, at *8 n.9.
[325] See RCA Corp. v. John Fairfax & Sons Ltd., (1981) 52 FLR 71, 78, [1981] 1 NSWLR 251, 34 ALR 345, [1982] R.P.C. 91 (Sup.Ct. N.S.W.); Amstrad Consumer Electronics Plc. v. British Phonographic Industry Ltd., [1986] F.S.R. 169, 188 (C.A. Eng.).
[326] 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12.04[A][1], at 12-76 (Supp. 2007) [hereinafter NIMMER ON COPYRIGHT]. See also A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2004).

exploitation of copyrighted materials – even in the absence of actual knowledge that the copyright monopoly is being impaired, the purposes of copyright law may be best effectuated by the imposition of liability upon the beneficiary of that exploitation".[327]

143. Thus, a U.S. court has held liable an adult material age verification service ("AVS") because this Internet service provider had a monitoring program for infringing images found on the participating websites,[328] where it also receives payment from customers to access the adult materials.[329] On the other hand, another U.S. court has absolved the ISP AOL of vicarious liability for providing its subscribers with access to its USENET[330] servers that contained infringing materials on a particular newsgroup. It reasoned that while AOL could delete or block access to the infringing postings, this was possible only be done *after* the postings had found their way onto AOL's USENET servers. Since this ability could not be targeted directly at the primary infringer, this would not amount to "the right and ability to control the infringing activity" to found vicarious liability.[331] Likewise AOL could not be said to derive a direct financial benefit from that infringing activity, since there was no evidence to suggest that AOL attracted or retained subscriptions from its customers because of the infringement or lost subscriptions arising from its eventual obstruction of the offending newsgroup.[332]

144. Much of the litigation in the United States for vicarious liability against Internet intermediaries stemmed from actions against developers of P2P software. In the widely followed *A&M Records, Inc. v. Napster, Inc.* ("*Napster*") decision, the U.S. 9th Circuit held the Napster developers vicariously liable for the massive infringement of copyright through the swapping and exchange of unlicensed music files between Napster users. The court found that Napster had the ability to locate infringing material listed on search indices that

---

[327] H.L. Green Co., 316 F.2d at 307. Otherwise, the secondary infringer, who has a financial interest in the activities of the activities of the primary infringer, and who may also supervise the primary infringer, would otherwise unfairly reap the benefits of the latter's infringing behavior. See Artists Music, Inc. v. Reed Pub. (USA), Inc, 1994 WL 191643, *4 (S.D.N.Y. 1994).

[328] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F.Supp.2d 1146, 1173 (C.D.Cal. 2002).

[329] Id. at 1171-1172. The AVS provider in turn pays the third party websites a commission for using the AVS.

[330] Ellison v. Robertson, 189 F.Supp.2d 1051, 1053-1054 (C.D.Cal. 2002), aff'd in part, rev'd in part 357 F.3d 1072 (9th Cir. 2004) ("USENET, an abbreviation of 'User Network,' is an international collection of organizations and individuals (known as 'peers') whose computers connect to each other and exchange messages posted by USENET users. Messages are organized into "newsgroups," which are topic-based discussion forums where individuals exchange ideas and information. Users' messages may contain the users' analyses and opinions, copies of newspaper or magazine articles, and even binary files containing binary copies of musical and literary works. 'Alt.binaries.e-book', the newsgroup at issue in this case, seems to have been used primarily to exchange pirated and unauthorized digital copies of text material, primarily works of fiction by famous authors, including Ellison".).

[331] Id. at 1061-1062. On appeal, the 9th Circuit upheld the district court's holding that AOL was not liable in vicarious infringement, but on the separate point that AOL could not be said to have received a direct financial benefit from the copyright infringement. Id. 357 F.3d at 1079.

[332] Id. at 1062-63 (C.D.Cal. 2002). The trial judge had held that since AOL did not receive any financial compensation for its participation in USENET, and USENET usage only constituted 0.25% of AOL's total member usage, of which the offending newsgroup only constituted approximately 0.00000596% of AOL's total usage, which is such a minuscule portion that "if any benefit exists at all, [it] is too indirect and constitutes far too small a 'draw' to support the imposition of vicarious copyright liability on AOL". This point was reversed on appeal. "The essential aspect of the "direct financial benefit" inquiry is whether there is a causal relationship between the infringing activity and any financial benefit a defendant reaps, regardless of how substantial the benefit is in proportion to a defendant's overall profits". Ellison, 357 F.3d at 1079.

it maintained on its servers, and could consequently terminate its users' access to the shared files.[333] Likewise, the court also found that Napster derived commercial benefit from these infringing activities by increasing its user base, which it planned to exploit in the future,[334] even though Napster was, at the point in time when it was sued, offered as a free service.[335]

145. Aimster was a hybrid version of the first generation of P2P software that replaced Napster when it fell.[336] In re *Aimster Copyright Litigation* ("*Aimster*"), the Illinois District Court, in an interlocutory application, found against the Aimster defendant developer for vicarious infringement. The court held that the Aimster defendant could control the access of Aimster users because the software required Aimster users to log on to the Aimster server to use the service to search for files.[337] On appeal, the 7th Circuit distanced itself from this holding of vicarious liability and instead favored liability for contributory infringement,[338] but no substantive reasons were offered.[339]

146. The second generation of P2P software developers made the use of a central server obsolete. Instead, the P2P software sets up various users as "supernodes" which are interconnected to all the other users. These connections serve to relay search queries and results between users independently of any computers owned or controlled by the

---

[333] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1024 (9th Cir. 2004), aff'g 114 F.Supp.2d 896 (N.D.Cal. 2000).

[334] Napster, 114 F.Supp.2d at 921-922; 239 F.3d at 1023.

[335] Napster, 114 F.Supp.2d at 902 (holding that potential revenue sources included targeted email, advertising, commissions from links to commercial websites, direct marketing of CDs, Napster branded products and CD burners and rippers, and a premium or commercial version of the Napster software for a fee). This part of the judgment has been criticized as an expansion of the scope of vicarious infringement in which direct financial benefit was satisfied without proof of any revenue generated from such activities. See PAUL GOLDSTEIN, 1 GOLDSTEIN ON COPYRIGHT § 8.2.1 at 8:24 (3rd ed. 2005 & Supp. 2007) [hereinafter GOLDSTEIN] (describing Napster as a "high watermark"); Mark A. Lemley, Rationalizing Internet Safe Harbors, STANFORD PUBLIC LAW WORKING PAPER NO. 979836 (Apr. 10, 2007), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=979836.

[336] In re Aimster Copyright Litigation, 252 F.Supp.2d 634, 642-644 (N.D.Ill. 2002), aff'd 334 F.3d 643 (7th Cir. 2003). The judgments described the Aimster as comprising proprietary software that integrated with the instant-messaging service provided by AOL through a server that users had to log on to for free. Subsequently, the Aimster developer required Aimster users to pay subscription for this service.

[337] Aimster, 252 F.Supp.2d at 655-656.

[338] Aimster, 334 F.3d at 654-655.

[339] One can only surmise that the 7th Circuit was in some doubt as to the actual operation of Aimster and whether there was the requisite level of supervisory control to satisfy the requirements of vicarious liability on the facts. For instance, the District Court's judgment described the Aimster service as one which enables "every Aimster user ... to search for and download files contained on the hard drives of any other" by "designating every Aimster user as the 'buddy' of every other Aimster user" and thereby "greatly [expanding] the file transferring capability of AOL IM". Aimster, 252 F.Supp.2d at 642. This seems to suggest that Aimster belongs to the second generation of "serverless" P2P networks, or at least, the server maintained by Aimster appears to be used only to enable Aimster users to ascertain if other Aimster users are online. The Federal Circuit's judgment described an Aimster user as using the Aimster service by supplying the Aimster server which "collects and organizes information obtained from the users but does not make copies of the swapped files themselves" with the names of the files he wants. The judgment stated that it was Aimster's server that searched the computers of those users who were online and who were available to be searched for files, and connected the requesting users with those users with the available files. Aimster, 334 F.3d at 646. This would suggest that the Aimster program was configured in a manner more akin to Napster.

developers.[340] This approach found some success before the courts. In *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, the U.S. 9th Circuit held that the second generation P2P software did not give their developers the ability to block access to individual users, to monitor and supervise the use of their software.[341] Furthermore, unlike Napster, none of the communications between the developers and users provided a point of access for filtering of or searching for infringing files, since infringing material and index information did not pass through the developers' computers.[342] In the absence of an effective point of control, the developers were held not vicariously liable for the users' infringement.

147. On appeal, the U.S. Supreme Court in *Grokster* agreed that the second generation P2P developers could not monitor or control the use of P2P software, or had any agreed upon right or current ability to supervise their use.[343] Perhaps it is for this reason that it sidestepped the issue of vicarious liability and resolved the case on the basis of "inducing infringement".[344] Realizing the same difficulty, rightholders also rely on the law of "contributory infringement" to found their claims of secondary liability against Internet intermediaries.

Contributory Infringement

148. The second avenue of indirect liability under U.S. copyright law is "contributory infringement". Where a party, "with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another," he may be held liable as a "contributory infringer".[345] U.S. courts have adopted a very broad view of contributory infringement because U.S. jurisprudence[346] has developed this avenue of liability based on the tort principle of "joint enterprise" or "enterprise liability".[347] In developing this jurisprudence, U.S. courts have held that the "knowledge" required encompasses both actual as well as constructive knowledge, and found liable a secondary infringer who "knows or has reason to know" of the direct infringement.[348] Likewise, U.S. courts have adopted a liberal interpretation of the requirement of "material contribution". For instance, they have found liable the operators of a swap meet or flea market for sales of infringing records by vendors who lease premises from the operators, on the basis that "it would be difficult for the infringing activity to take place in the massive quantities alleged without the support services provided by the swap meet. These services include, *inter alia* the provision of space, utilities, parking, advertising, plumbing and customers".[349]

---

[340] Grokster, 259 F.Supp.2d at 1040-1041; 380 F.3d at 1159.
[341] Grokster, 380 F.3d at 1165.
[342] Id.
[343] Grokster, 125 S.Ct. 2764, 2781 (2005).
[344] Id., 125 S.Ct. at 2781 fn. 12 (2005).
[345] See Gershwin Pub. Corp. v. Columbia Artists Mgmt., Inc, 443 F.2d 1159, 1162 (C.A.N.Y. 1971)
[346] See e.g. Demetriades v. Kaufmann, 690 F.Supp. 289 (D.C.N.Y. 1988); Screen Gems-Columbia Music, Inc. v. Mark-Fi Records, Inc., 256 F.Supp 399, 403 (D.C.N.Y. 1966). See also NIMMER ON COPYRIGHT § 12.04[A] at 12-79.
[347] By analogy with the law of partnership, enterprise liability arises in connection with an undertaking by several associates to carry out a small number of acts or objectives, in such circumstances that all have an equal voice in directing the conduct of the enterprise. See PROSSER AND KEETON § 72 at 517.
[348] See e.g. Screen Gems-Columbia Music, 256 F.Supp at 404-405; Cable/Home Commc'n Corp. v. Network Productions, Inc., 902 F.2d 829, 846 (11th Cir. 1990); Religious Technology Ctr. v. Netcom On-Line Communication Services, Inc., 907 F.Supp. 1361, 1373-74 (N.D.Cal. 1995).
[349] Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996).

149. Content holders have had more success applying contributory infringement to Internet intermediaries like P2P software developers. Napster was found by the U.S. 9th Circuit to be liable in contributory infringement. Its executives had industry knowledge of infringing activities by its users and also received notices of infringing files sent by the Recording Industry Association of America ("RIAA").[350] Relying on *Fonovisa,* the 9th Circuit held that Napster had also materially contributed to the infringement by providing the support services that enabled Napster users to find and download the music they wanted.[351] Similarly, in *In re Aimster Copyright Litigation*, the court held the Aimster developer liable for contributory infringement. The court found that the developer knew that users were sharing and exchanging unlicensed music files place using the Aimster software, although the developer had implemented an encryption scheme so that there was no way for him to know when the file sharing was taking place, the nature of the files being exchanged and the identities of the file sharers. The court held that the developer could not suggest that he lacked the requisite knowledge when his ignorance was because of an encryption scheme that he had himself put in place.[352] The Aimster developer was deemed to have had constructive knowledge of the infringing activity, since he had also written a tutorial that instructed users on how they can exchange infringing music files.[353]

Sony Safe Harbor Defense

150. Napster and Aimster both tried to bring themselves within the *Sony* "safe harbor" defense. In *Sony*, the U.S. Supreme Court held that a manufacturer and retailer of video tape recorders (VTRs) (also known as video cassette recorders or VCRs[354]) could not be liable for contributory infringement on the basis that they had sold equipment with constructive knowledge of the fact that customers may use that equipment to make unauthorized copies of copyrighted material. It held that "the sale of copying *equipment*, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses".[355] In declining to apply this defense, the District Court in *Napster* held that *Sony* was inapplicable to a *service* such as one maintained by Napster where it continues to exercise control over the device's use, as opposed to a piece of equipment offered for sale.[356] On appeal, the 9th Circuit ruled that Napster could not avail itself of the *Sony* safe harbor because Napster had actual knowledge that specific infringing material was available using its system, and upheld the District Court's finding that Napster had contributed to the Napster users' direct infringement.[357] The 7th

---

[350] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020 n.5 (9th Cir. 2004).
[351] Id. at 1022.
[352] In re Aimster Copyright Litigation, 252 F.Supp.2d 634, 651 (N.D.Ill. 2002); aff'd 334 F.3d 643, 650 (7th Cir. 2003).
[353] Id. at 651.
[354] Wikipedia, Video tape recorder, http://en.wikipedia.org/wiki/Video_tape_recorder (last visited May 4, 2008).
[355] Sony, 464 U.S. at 439.
[356] Napster, 114 F.Supp.2d at 916-7.
[357] Id. at 1021-1022. The 9th Circuit's narrow interpretation of the Sony safe harbor, repeated in the 9th Circuit's decision in Grokster, 380 F.3d at 1160-1161, became known as the Napster gloss on Sony. As a gloss on Sony, this was disavowed by the Supreme Court in Grokster. Grokster, at 2778. However, the Napster gloss was reformulated as a test for contributory infringement in Perfect 10, Inc. v Amazon.com, Inc., 508 F.3d 1146, 1172 (9th Cir. 2007) ("Accordingly, we hold that a computer system operator can be held contributory liable if it 'has actual knowledge that specific infringing material is available using its system,' Napster, 239 F.3d at 1022, and can 'take simple measures to prevent further damage' to copyrighted works, Netcom, 907 F.Supp. at 1375, yet continues to provide access to infringing works".).

Circuit in *Aimster* also declined to apply the *Sony* defense, holding that the Aimster developer had failed to produce any evidence that his service was ever used for a non-infringing use, let alone evidence regarding the frequency of such uses.[358]

151. The *Sony* defense however succeeded before the 9th Circuit in *Grokster*, which noted that the software developers "have not only shown that their products are capable of substantial non-infringing uses, but that the uses have commercial viability".[359] On appeal, the Supreme Court affirmed the continued relevance of the *Sony* "staple article of commerce" safe harbor. It held that a developer of a product with substantial lawful and unlawful uses is *generally* protected under the law of copyright. Justice Souter, delivering the opinion of the Court, said:

> In sum, where an article is "good for nothing else" but infringement, there is no legitimate public interest in its unlicensed availability, and there is no injustice in presuming or imputing intent to infringe. Conversely, the *Sony* doctrine absolves the equivocal conduct of selling an item with substantial lawful as well as unlawful uses, and limits liability to instances of *more acute fault than the mere understanding that some of one's products will be misused.* It leaves breathing room for innovation and a vigorous commerce.[360] (emphasis added)

Inducing Infringement

152. While the *Grokster* court affirmed the relevance of the *Sony* defense to an action in contributory infringement, the court also excluded its application in a claim for "inducing infringement". The court said:

> *Sony's* rule limits imputing culpable intent as a matter of law from the characteristics or uses of a distributed product. But nothing in *Sony* requires courts to ignore evidence of intent if there is such evidence, and the case was never meant to foreclose rules of fault-based liability derived from the common law. Thus, where evidence goes beyond a product's characteristics or the knowledge that it may be put to infringing uses, and shows statements or actions directed to promoting infringement, *Sony's* staple-article rule will not preclude liability.[361]
>
> *...We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties. We are, of course, mindful of the need to keep from trenching on regular commerce or discouraging the development of technologies with lawful and unlawful potential. Accordingly, just as Sony did not find intentional inducement despite the knowledge of the VCR manufacturer that its device could be used to infringe... mere knowledge of infringing potential or of actual infringing uses would not be enough here to subject a distributor to liability. Nor would ordinary acts incident to product distribution, such as offering customers technical support or product updates, support liability in themselves. The inducement rule, instead, premises liability on purposeful, culpable expression and conduct, and thus does nothing to compromise legitimate commerce or discourage innovation having a lawful promise.*[362] *(emphasis added)*

---

[358] In re Aimster Copyright Litigation, 334 F.3d at 653.
[359] Grokster, 259 F.Supp.2d at 1035, aff'd 380 F.3d at 1162.
[360] Id. at 2777-2778.
[361] Id. at 2779.
[362] Id. at2780.

153. On the facts, the Supreme Court found evidence that Grokster and StreamCast engaged in inducing infringement. The court noted that StreamCast sought to develop promotional materials to advertise itself as the best Napster alternative.[363] On remand, the District Court in *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.* ("*Grokster II*") received evidence about how StreamCast executives used their own P2P software to search for songs by commercial artists available on their networks, compared them against other similar networks, and complained to their own developers about whether users will be able to locate these songs.[364] The court was also prepared to draw adverse inferences from the song categorization features (such as the "Top 40" song searches) of the programs, their advertisement driven models and the defendants' failure to develop filtering tools to limit any infringing uses of their software as evidence that complemented or gave direct evidence of the unlawful objective or intent "added significance".[365] In contrast, courts seem to view the implementation of filtering features as evidence that the intermediary did not have the requisite intent to induce infringement, even though doubts may remain about their efficacy.[366]

154. The introduction by the *Grokster* court of a new cause of action in inducing infringement that precludes the *Sony* defense puts into even sharper focus the United States DMCA safe harbor defenses, in that they remain viable defenses for the Internet intermediaries. It is to these that this paper now turns.

Digital Millennium Copyright Act Safe Harbors

155. The breadth of the judicial approach towards contributory infringement and cases such as *Playboy Enterprises Inc. v. Frena*,[367] *Sega Enterprises v. MAHPHIA*[368] and *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*[369] prompted the telecom and Internet industry groups in the United States to lobby Congress to enact the Online Copyright Infringement Liability Limitation Act, part of the DMCA. The ensuing safe harbor defenses shield Internet intermediaries as network "service providers"[370] from monetary relief[371]and greatly limit the equitable relief available against them[372] for any direct and secondary copyright liability. The activities of four categories of service providers are protected under the safe harbor provisions, subject to their compliance with two general conditions. The first condition is that the service providers must adopt and reasonably implement, and inform its subscribers and account holders, of a policy for

---

[363] Id. at 2773. StreamCast developed advertisements for its users such as "Napster Inc. has announced that it will soon begin charging you a fee. That's if the courts don't order it shut down first. What will you do to get around it?" and "StreamCast's software as the '# 1 alternative to Napster' – '[w]hen the lights went off at Napster ... where did the users go?' " In Grokster II, the court took evidence that similar promotional materials were developed by StreamCast for its potential investors and business partners. Grokster II, at 978.

[364] Grokster II, at 979.

[365] Grokster, at 2780-2781; Grokster II, at 987-988.

[366] See e.g., Monotype Imaging, Inc. v. Bitstream Inc., 376 F.Supp.2d 877, 889 (N.D.Ill. 2005). See also Tim Wu, The Copyright Paradox - Understanding Grokster, STANFORD LAW AND ECONOMICS OLIN WORKING PAPER NO. 317, Supreme Court Review, 2006, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=828784.

[367] Playboy Enterprises Inc. v. Frena, 839 F.Supp 1552 (M.D. Fla. 1993).

[368] Sega Enterprises Ltd. v. MAPHIA, 857 F.Supp 679 (N.D. Cal. 1994).

[369] Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).

[370] 17 U.S.C. § 512(k)(1).

[371] 17 U.S.C. § 512(a), (b), (c), (d).

[372] 17 U.S.C. § 512(j).

termination of repeat infringers.[373] The second is that the service providers must accommodate and not interfere with standard technical measures used by copyright owners to identify or protect copyrighted works.[374]

156. The first safe harbor, set out in section 512(a), indemnifies service providers for copyright infringements for providing transmission, routing and connection services, and for the intermediate and transient storage of material in the course of providing such services. The conditions are that the transmission of the material be initiated by a third party, the services be carried out by way of an automatic technical process without selection of the material by the service provider, the provider does not select the recipients of the material except as an automatic response to the request of another, no copy of the material made for intermediate or transient storage is ordinarily accessible, or accessible to anticipated recipients for a longer period of time than is reasonably necessary for the provision of transmission, routing or connection services, and that the material is transmitted without modification of its content.

157. The second safe harbor, set out in section 512(b), indemnifies service providers for copyright infringement for the "intermediate and temporary storage of material" on a system or network which the providers control. The conditions are that the material is made available by an originating party (other than the service provider), it is transmitted to another party, the storage is carried out through an automatic technical process, the material is transmitted without modification to its content, the provider complies with generally accepted industry data communication rules concerning the refreshing, reloading and updating of material, the service provider does not interfere with the technology used by the originating party to return usage information to that party, the provider ensures that conditions to access the material imposed by the originating party such as payment of fees are met, and the provider responds expeditiously to a take-down notice to remove material that is claimed to be infringing.

158. The third safe harbor, set out in section 512(c), indemnifies a service provider for copyright infringement for storage, at a user's direction, of the user's material on the provider's system or network. Four conditions have to be satisfied before the indemnity applies: (a) the provider must not have actual knowledge that the material or an activity using the material is infringing, is not aware of facts or circumstances from which infringing activity is apparent, and upon obtaining such knowledge or awareness, it acts expeditiously to remove or disable access to the material,[375] (b) where the provider has the right and ability to control such activity, it does not receive a financial benefit directly attributable to the infringing activity,[376] (c) where it receives a take-down notice alleging infringement, it responds expeditiously to remove or disable access to the material,[377] and (d) the provider has publicly designed an agent to receive notifications of claimed infringement.[378]

159. The last safe harbor, set out in section 512(d), indemnifies a service provider for referring or linking users to an online location containing infringing material or infringing activity. Three conditions have to be satisfied before the indemnity applies: (a) the provider must not have actual knowledge that the material or an activity using the material or activity is

---

[373] 17 U.S.C. § 512(j)(1)(A).
[374] 17 U.S.C. § 512(i)(1)(B), (i)(2).
[375] 17 U.S.C. § 512(c)(1)(A).
[376] 17 U.S.C. § 512(c)(1)(B).
[377] 17 U.S.C. § 512(c)(1)(C).
[378] 17 U.S.C. § 512(c)(2).

infringing, is not aware of facts or circumstances from which infringing activity is apparent, and upon obtaining such knowledge or awareness, it acts expeditiously to remove or disable access to the material,[379] (b) where the provider has the right and ability to control such activity, it does not receive a financial benefit directly attributable to the infringing activity,[380] and (c) where it receives a take-down notice alleging infringement, it responds expeditiously to remove or disable access to the material.[381]

160. The judicial interpretation of the conditions to the safe harbor provisions, especially that for hosting providers in section 512(c), has attracted a fair measure of controversy. Judicial debate has surrounded elements such as what constitutes the "right and ability to control" an infringing activity,[382] what constitutes a "direct financial benefit,"[383] and what is the requisite state of knowledge that triggers the "apparent knowledge" condition (described in the United States Congressional reports as "red flag" knowledge) in section 512(c). For instance, while the United States Senate and House reports agree that "apparent knowledge" is to be assessed both subjectively (whether the provider was subjectively aware of the facts or circumstances of infringing activity in question) and objectively (whether it would be apparent to a reasonable person "operating under the same or similar circumstances" that those facts and circumstances would constitute infringing activity),[384] how is this test to be applied to the facts? Will a "general awareness of infringement" that is prevalent on the Internet[385] suffice?[386] The United States House Report suggests that the use of site names that make their illegal purpose "obviously and conspicuously pirate" will deny the provider the safe harbor indemnity.[387] Yet in *Perfect 10, Inc. v. CCBill LLC*, the court refused to accept the argument that intermediaries that provide hosting and payment services to "illegal.net" and "stolencelebritypics.com" must have been aware of apparent infringing activity on these sites, on the basis that these words are not actually admissions of infringing activity but attempts to increase their salacious appeal.[388] On the other hand, the approach that the requisite knowledge is that

---

[379] 17 U.S.C. § 512(d)(1)(A).
[380] 17 U.S.C. § 512(d)(1)(B).
[381] 17 U.S.C. § 512(d)(1)(C).
[382] See e.g., Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082, 1093-94 (C.D. Cal. 2001); Costar Group, Inc. v. Loopnet, Inc., 164 F. Supp. 2d 688 (D. Md. 2001); UMG Recordings, Inc. v. Veoh Networks Inc. 665 F.Supp.2d 1099, 1112-13 (C.D.Cal. 2009)Io Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1151 (N.D.Cal. 2008).
[383] See e.g., Ellison v. Robertson, 357 F.3d 1072, 1079 (9th. Cir. 2004) ("The record lacks evidence that AOL attracted or retained subscriptions because of the infringement or lost subscriptions because of AOL's eventual obstruction of the infringement".); Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1117 (9th. Cir. 2007) (construing the meaning of "direct financial benefit" consistently with the common law standard for vicarious liability). Cf.. H.R. Rep. 105-551(I), at 11 (Judiciary Committee); H.R. Rep. 105-551(II), at 54.
[384] S. Rep. 105-190, at 44; H.R. Rep. 105-551(II), at 53 ("The 'red flag' test has both a subjective and an objective element. In determining whether the service provider was aware of a 'red flag,' the subjective awareness of the service provider of the facts or circumstances in question must be determined. However, in deciding whether those facts or circumstances constitute a 'red flag'–in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances–an objective standard should be used".).
[385] UMG Recordings, Inc. v. Veoh Networks Inc., 665 F.Supp.2d 1099, 1111 (C.D.Cal. 2009) ("it is common knowledge that most websites that allow users to contribute material contain infringing items").
[386] See e.g. Columbia Pictures Industries, Inc. v. Fung, 2009 WL 6355911, 18 (C.D.Cal.) (C.D.Cal.,2009).
[387] H.R. Rep. No. 105-551(II), at 58 (referring to sites that typically use words such as 'pirate,' 'bootleg,' or slang terms in their URL and header information).
[388] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1114 (9th Cir. 2007).

of "specific and identifiable infringements of particular individual items" spelt out in *Viacom Intern. Inc. v. YouTube, Inc.*[389] seems to adopt an unduly narrow interpretation of what constitutes "apparent knowledge". Yet such an interpretation appears consistent with the absence of any obligation to monitor its services or affirmatively seek facts indicating infringing activity (except in relation to standard technical measures) as provided in section 512(m)(1).

161. So while the DMCA safe harbor defenses may have been propagated in and assimilated into the copyright laws of various countries, considerable interpretational difficulties still exist as to the exact scope and detailed application of these defenses to Internet intermediaries.

[389] Viacom Intern. Inc. v. YouTube, Inc., 2010 WL 2532404, 15 (S.D.N.Y. 2010).