Copyright Enforcement on the Internet – in Three Acts

Justin Hughes♠

The attached text represents several draft sections of a forthcoming paper. The complete outline of the paper is shown below; sections listed in the Table of Contents without page numbers are not included in this text. Please contact the author for more information. **justin@justinhughes.net**

♠ Professor of Law, Cardozo School of Law. The author is thankful for helpful comments received at talks and workshops at the University of Houston, the Institut für Zivilprozessrecht der Universität Bonn, the Johann-Wolfgang Goethe Universität, Frankfurt, the University of Pennsylvania, and the University of Hokkaido. The remaining shortcomings are the exclusive intellectual property of the author. **Email: justin@justinhughes.net**

Introduction

Changes in law are driven by widespread changes in the conditions of economic exchange, in available technology, in accepted morality, and, just maybe, in human nature. The liability of internet service providers (ISPs) for copyright infringements by ISP customers is a small, intriguing – and unfinished – story of such legal development. This is not the way it seemed to many of us just a few years ago.[1] In the period 1998 – 2004, the issue seemed to become settled for two important reasons. First, it seemed that ISPs would have to be shielded from most or all financial liability for the torts done by internet users in order to have low cost business models that would ensure wide availability of internet services. Second, it seemed that unless shielded from such financial liability, ISPs would be forced to become private censors – with little guidance and strong incentives to err conservatively -- against any questionable communications. For these reasons, ISPs have generally been shielded from liability as long as they disable offending material when they know or are put on notice of the information tort.[2]

But there are now shifts in the terrain – and those of us who thought the issue was largely settled may have been quite wrong. More and more, courts and legislators are calling on ISPs to have greater responsibility for copyright infringement by customers. One might consider this just a pendulum swing of policy.[3] One might also

---

1 Justin Hughes, *The Internet and the Persistence of Law*, 44 BOSTON COLLEGE L. REV. 359, 383 - 387 (2003).

2 While copyright is generally regarded as a form of property, infringement is often regarded as a form of tortuous conduct, particularly when explaining the rationale behind secondary liability. See Fonovisa, Inc. v. Cherry Hill Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996) ("Contributory infringement originates in tort law and stems from the notion that one who directly contributes to another's infringement should be held accountable."); Screen Gems-Columbia Music, Inc. v. Mark-Fi Records, Inc., 256 F. Supp. 399, 403 (S.D.N.Y. 1966).

3 Such pendulum swings sometimes begins with scholars' critical analyses (and sometimes not!). In the area of ISP liability, these have included Doug Lichtman and Eric Posner, *Holding Internet Service Providers Accountable*, 14 S. CT. ECON. REV. 21 (2006); Douglas Lichtman & William Landes, *Indirect Liability for Copyright Infringement: An Economic Perspective*, *16* HARV. J.L. & TECH. 395, 404-05 (2003); (proposing that ISPs should have some responsibility when their subscribers introduce 'malicious code' into the Internet); Assaf Hamdani, *Who's*

consider this a reassessment broadly possible because, in the 2009 words of the Ninth Circuit in 2008, the internet "is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses."[4]

This Article explores the reassessment of ISP liability that is occurring on a variety of fronts, explaining how the resulting instability is the result of technological advances and changing business models; how some of these advances have decoupled policy considerations concerning copyright liability from other kinds of liability, particularly for defamation; and how this form of copyright liability moved from a knowledge standard to an intent standard, and *may* be moving now from these fault-based standards to mechanistic, regulatory standards of responsibility more familiar to areas like banking law than intellectual property. Technological developments are leading us into a period when the relative responsibility of ISPs for copyright infringement may be shaped by the "cheapest cost avoider: theory,"[5] but we must still ask if there remain countervailing social considerations with ISPs, just as in other areas where we do not (yet) impose such tort liability.

For the moment this story can be understood in three parts, although not in the sense that a third "act" implies the conclusive phase of the drama. In the discussion that follows "internet service provider" is used in a very broad sense –

Liable for Cyberwrongs?, 87 CORNELL L. REV. 901 (2002) (proposing complex test for ISP liability for a variety of information torts); Brian McManus, *Rethinking Defamation Liability for Internet Service Providers*, 35 SUFFOLK U. L. REV. 647 (2001) (proposing a return to common law liability standards in place of section 230 for defamation).

4 Fair Housing Council of San Fernando Valley v. Roommates.Com, LLC, 521 F.3d 1157, 1164, fn 15 (9th Cir. 2008). As the *en banc* court noted, instead of being "fragile," the internet "has become a dominant – perhaps the preeminent – means through which commerce is conducted." *Id.*

5 *See generally* GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 135-73 (1970); Posner, *A Theory of Negligence,* 1 J. LEGAL STUD. 29, 33 (1972) ("[if] the benefits in accident avoidance exceed the costs of prevention, society is better off if those costs are incurred and the accident averted, and so . . . the enterprise is made liable, in the expectation that self-interest will lead it to adopt the precautions in order to avoid a greater cost in tort judgments.").

covering all the entities that provide "online," "network," and even "carriage" services.[6] Part I describes how courts momentarily struggled with the issue until legislatures intervened to give mainstream ISPs substantial protection from liability for torts by their customers. I have described this elsewhere as a kind of "invisible hand" convergence – rough harmonization of different nations' laws driven neither by a multilateral treaty nor model standards, but by market conditions. Part II then describes how, just as this was becoming a loosely harmonized legislative agenda, courts around the world began crafting theories to (re)impose liability on a specific, unanticipated genre of digital intermediary: peer-to-peer (P2P) software.

Part II describes these P2P cases as another kind of rough convergence in which different legal theories have produced results strikingly similar among different jurisdictions. Some legal academics have seen courts as a final line of defense against intellectual property's expansionist political economy,[7] but these cases show courts strengthening copyright's position against obvious infringement-based business models at a time when the political economy has either favored the digital intermediaries over copyright owners or has generally been in equipoise between the two camps. Despite legislative pronouncements that intermediaries have no duty to monitor, judges' opinions often slip into language impliedly suggesting such responsibility.

Part III takes up the emerging plotline of the third act by describing filtering and packet inspection technology – as well as the controversy surrounding ISP actions against BitTorrent. Part IV then explores some recent cases that herald a future less favorable to *mainstream* digital intermediaries. The sentiments that animate these opinions – whether a simple sense of right and wrong or a cold calculus of the most efficient cost-avoider – have traction against a wide range of ISPs, particularly as the filtering of copyrighted works increasingly robust and affordable. Part IV also reviews the wide range of public, private, and mixed initiatives premised on the notion that as

---

6 These are names given to ISPs just among the English-speaking jurisdictions of the Pacific (Australia, New Zealand, Singapore, and the US). *See* APEC-IPEC Preliminary Report on Copyright Exceptions and Limitations at 18.

7 Yochai Benkler, *Through the Looking Glass: Alice and the Constitutional Foundations of the Public Domain,* 66 LAW & CONTEMP. PROB., 173, 197 (2003)

ISPs become increasingly able to detect infringement technologically, they should take up increasing responsibility to combat such infringement.

Part V concludes by looking at how the US knowledge-based standards for maintstream ISP responsibility have, in effect, been taken over by an automated, regulatory system. This can be seen by looking at the actual functioning of the section 512 "notice and takedown" system; I will suggest that it is also the best way to understand Viacom's claims against YouTube, i.e. as an effort to shift the paradigm while remaining *within* the 512 framework. In the case of the former, what was intended as a system of responsibility based on human knowledge has become almost wholly automated. And, despite the protests of some academics, complaints about this system's impact on free expression have been muted, a point that leads to a broader discussion of whether the internet role of ISPs permits a classic 'least cost avoider' approach to responsibility, requires a more specialized policy framework, and/or allows us to tolerate a largely automated system for copyright violations on the internet.

The prospect of ISPs having some responsibility to monitor, filter, and act against unauthorized distribution of copyrighted works strikes some as a "locking down" of the Internet[8] and, as one consumer activist put it, "against digital history."[9] But that is partly the point: "digital history" is a superstructure built on a technological foundation and technology was never going to develop inextricably in one direction. Those who hummed technological determinism when the rhythm sweetly whispered of minimal laws and copyright's death should at least accept that the technological curve may be turning history in another direction.

8 Michael Geist, *The dangers of 'locking down' the Internet*, Toronto Star, January 28, 2008.

9 Statement of French consumer group UFC Que Choisir in reaction to 2007 plan for French ISPs to monitor customers and issue warning messages to customers downloading files illegally. Reuters, *France set to cut Web access for music, film pirates*, Cnet News.com, Nov. 23, 2007.

I. Legislatures shield ISPs from liability

One of the first defining issues of "cyberlaw" was the liability of ISPs for torts committed by non-related persons using the Internet. The problem initially arose more frequently with defamation than with copyright. With early data transfer rates, it was easier to defame than to infringe. "Cyberlaw" was about slander -- and then porn (sometimes as unauthorized copyrighted material) -- before it was about music and warez sites. There were a variety of ways to conceptualize ISP exposure to and responsibility for these information torts. Once it was accepted that ISPs do not themselves "communicate" users' content to the public,[10] ISPs *might* still have broad exposure under theories of secondary liability.[11] ISP exposure might take the form of the strict liability standard applicable to "publishers" or a "distributor" (bookstore) liability standard based on continued distribution after becoming aware of the tortious nature to the information. Or ISPs might be exculpated generally from liability for information torts by their customers – as are the telephone companies, with whom – at the time – the ISPs shared telephone lines as the main means of connectivity.

---

[10] *See* Agreed Statement to Article 8, WIPO Copyright Treaty (WCT) (1996), WIPO Publication No. 227(E) adopted by the WIPO Diplomatic Conference on Certain Copyright and Neighboring Rights Questions in Geneva, on December 20, 1996. Available at http://www.wipo.int/treaties/en/ip/wct/ last visited January 20, 2008 ("It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention."); This statement has been transposed expressly in the law of some jurisdictions. See, e.g. Copyright Ordinance of Hong Kong, § 26(4) ("The mere provision of physical facilities for enabling the making available of copies of works to the public does not of itself constitute an act of making available copies of works to the public."); Canadian Copyright Act, § 2.4(1) (xxx xxx xxx); proposed § 92B(2) of the New Zealand Copyright Act ("xxx xxx xxx). *See also* P. Bernt Hugenholtz, *Caching and Copyright: The Right of Temporary Copying*, 22 EUROPEAN INTELL. PROP. REV. 482, 489 (2000). In the United States, direct liability was found in Playboy Enterprises v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993), but quickly discredited in subsequent cases and commentary.

[11] *See, e.g.* Pamela Samuelson, *Symposium: The Jurisprudence of Justice Stevens: Panel II: Antitrust/Intellectual Property: Generativity of* Sony v. Universal*: The Intellectual Property Legacy of Justice Stevens*, 74 FORDHAM L. REV. 1831, 1872 (2006)("Prior to enactment of the DMCA, there was considerable uncertainty about the copyright liability of Internet service (and access) providers.")

In the US, this issue was first vented in the 1995 New York state case *Stratton Oakmont v. Prodigy,*[12] a dispute concerning Prodigy's moderated computer bulletin boards that were accessible only to paid subscribers. A statement posted on its financial bulletin board by an "unidentified bulletin board user" – one of two million Prodigy users -- claimed that a particular securities offering from investment firm Stratton Oakmont was criminally fraudulent, that Stratton's president committed this fraud, and that Stratton brokers regularly lied.[13] Critical to the fact pattern, Prodigy distinguished itself from other bulletin board hosts by holding "itself out as an online service that exercised editorial control over the content of messages posted on its computer bulletin boards."[14]

The court's analysis starts by distinguishing the liability of publishers from the liability of "distributors such as book stores and libraries [who] may be liable for defamatory statements of others only if they knew or had reason to know of the defamatory statement at issue."[15] Based on how Prodigy had "uniquely arrogated to itself the role of determining what [wa]s proper for its members to post and read on its bulletin boards,"[16] the court determined that Prodigy was the "'publisher' of statements on its 'Money Talk' computer bulletin board for the purposes of Plaintiffs' libel claims."[17] At the same time, the *Stratton Oakmont* court concluded that, generally speaking, most computer bulletin boards should be held only to "distributor" liability

12 Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 N.Y. Misc LEXIS 229, 1995 WL 323710, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. May 24, 1995). Some may consider that the the first U.S. decision in this realm was Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla, 1993). But the reasoning of the *Frena* decision is based on the bulletin board operator having *direct* liability for the infringing images (although the defendant claimed that other users, not he, had loaded the images to his bulletin board). An internet bulletin board operator's *direct* infringement liability for materials posted by users was also the holding in Sega Enterprise v. MAPHIA, No. CIV. A. 93-4262 CW, 1997 WL 337558 (N.D. Cal., 1997). Both these cases conflict with the Agreed Statement in the WCT and precede US ratification of the WCT in 1998.

13 1995 N.Y. Misc LEXIS 229 at 2.

14 1995 N.Y. Misc LEXIS 229 at 3.

15 1995 N.Y. Misc LEXIS 229 at 7.

16 1995 N.Y. Misc LEXIS 229 at 10.

17 1995 N.Y. Misc LEXIS 229 at 1.

standards, i.e. liability when they are aware of the libel and continue the distribution of the libelous material.[18]

The same year as *Stratton Oakmont* the owner of the copyright in various Church of Scientology writings sued another computer bulletin board service over the a posting of the writings by a bulletin board user. (These bulletin boards were, in fact, the first "user generated content" sites.) In *Religious Technology Center v. Netcom*[19] a northern California district court concluded that the case could go forward on contributory liability grounds – that is, liability when there is knowledge and material contribution to the infringement – but barred strict liability on the grounds that such liability "would chill the use of the Internet because every access provider or user would be subject to liability when a user posts an infringing work to a Usenet newsgroup."[20]

Early English and Japanese court decisions adopted a similar middle ground for ISP liability. In the first case in Europe, the 1999 *Godfrey v. Demon* case, an English court used a rough distributor liability standard, concluding that an UK ISP could be liable under English defamation law when it had been advised of the alleged defamation and had not disabled the defamatory material within a reasonable time.[21] In Japan, the 1997 *Nifty Service* decision by the Tokyo district had found that the operator of an electronic forum had an "active obligation to take necessary measures" against the posting of defamatory statements, but this line of reasoning was softened in the subsequent 1999 *Toritsu (Tokyo Metropolitan) University* case, in which the court concluded that network managers should only be liable in exceptional cases where the defamation was obvious and the "reputational damage substantial."

---

18 1995 N.Y. Misc LEXIS 229 at 12-13.

19 907 F. Supp. 1361, 1377 (N.D. Cal. 1995). For a much more exhaustive discussion of the case, see Yen at 1846-1848.

20 The pattern of ruling out vicarious liability, but permitting the case to go forward on possible contributory liability was also the result in another important pre-DMCA case, Marobie-FL Inc. v. National Ass'n of Fire Equip. Distribs., 983 F. Supp. 1167, 1179 (N.D. Ill. 1997).

21 Godfrey v. Demon Internet Ltd., [1999] 4 All E.R. 342 (Queen's Bench Division, March 26, 1999)

These early internet defamation cases provided a context for policy makers pondering the issue of ISP liability in relation to copyright infringement.[22] In these discussion, copyright industries obviously were interested in holding digital intermediaries liable for subscriber infringements, a position largely echoed by the U.S. Government's 1995 "White Paper."[23] On the other hand, digital intermediaries had equally obvious interests in lobbying against liability.[24]

But market economics and technology did point to a choice among the competing proposals. At the time it was widely agreed that there was an easy technological fix for detection of neither defamation nor copyright infringement. Any monitoring or filtering would have to be done by humans. Putting aside the enormous issues of ISPs being placed in the role of private censors, monitoring would be so slow

---

22 For example, when Japanese policymakers first explicitly addressed the question of ISP liability for copyright infringement they expressly turned to the two cases discussed above. INTERIM REPORT BY THE COPYRIGHT COUNCIL OF JAPAN, [FIRST SUB-COMMITTEE – EXPERTS' WORKING GROUP], REGARDING THE ISSUE OF ISP LIABILITY, December 2000 (reporting on 1997 and 1999 Tokyo District Court cases) (unofficial translation on file with author).

23 WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP IN INTELLECTUAL PROPERTY RIGHTS 1-6, 114-24 (1995). The "White Paper," as it was called, was prepared principally under the direction of then Assistant Secretary of Commerce Bruce Lehman. Commentary favoring ISP liability of some form during that period included Jane C. Ginsburg, *Putting Cars on the "Information Superhighway": Authors, Exploiters, and Copyright in Cyberspace*, 95 COLUM. L. REV. 1466, 1492-95 (1995) (mildly supporting the idea of ISP vicarious copyright liability); I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT L. REV. 993, 1042-46 (1994) (advocating strict ISP liability); John Carmichael, Comment, *In Support of the White Paper: Why Online Service Providers Should Not Receive Immunity from Traditional Notions of Vicarious and Contributory Liability for Copyright Infringement*, 16 LOY. L.A. ENT. L.J. 759, 771-85 (1996) (advocating vicarious and contributory ISP liability); Kelly Tickle, Comment, *The Vicarious Liability of Electronic Bulletin Board Operators for the Copyright Infringement Occurring on Their Bulletin Boards*, 80 IOWA L. REV. 391, 416 (1995) (favoring limited ISP liability).

24 In the words of one official who attended the 1996 Diplomatic Conference that created the WCT and WPPT, the Agreed Statement that ISPs do not "communicate" copyrighted materials sent by their subscribers "was the result of heavy pressure and lobbying by the telecoms (who were in Geneva en masse) for this clarification statement as they were extremely concerned over the national application of secondary and contributory liability for copyright infringement, especially in the U.S.." Email in file with the author.

and costly as to be impractical.[25] Thus, in 1995, 1998, or 2000, a jurisdiction that imposed strict liability on ISPs for third party defamation and copyright infringement might drive ISPs either out of business or into highly restricted business models. The combination of policing and/or insurance costs would have required much higher subscriber costs, dampening the promise – then often made by politicians -- of an Internet as ubiquitous as our highways and autobahns.[26] Because the problem – the impracticality of filtering appeared intractable[27] -- convergence toward complete or at least robust liability shields for ISPs seemed likely.[28]

Of the major economies, only the United States adopted the former – a complete shield for tortious materials posted by others – and the U.S. did so for claims of defamation, invasion of privacy, and other *non-intellectual property torts*. The 1996 Communications Decency Act added section 230(c)(1) to Title 47, providing that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[29] As long as the provider of "an interactive computer service" is not responsible "for the creation or development of [the] information" the provider is shielded from liability. This provision has almost uniformly been interpreted as giving ISPs a complete shield when they are not involved in the creation of the information they are hosting, transmitting, caching, etc.[30] The provision, however, expressly exempts intellectual property violations.[31]

---

25 *See, e.g.* Frank Pasquale, *Rankings, Reductionism, and Responsibility* 54 Cleveland State Law Review 115, 121 (2006) (saying of any ISP "[i]t is certainly in no position to review individually all new content on the web.")

26 *See, e.g.* Daniel Seng, *Secondary Liability for Peer to Peer Software Networks – A Singapore Perspective*, paper presented at Fordham/Queen Mary/Singapore IP Academy Seminar, London, November 14, 2005 ("legislatures were quick to revise copyright laws to exempt ISPs from liability. This is presumably driven by national policies to encourage and promote Internet usage and ensure its low-cost accessibility to the masses.")

27 I was one of the people who characterized (I now thinking mistakenly) the problem as intractable. Justin Hughes, *The Internet and the Persistence of Law*, 44 BOSTON COLLEGE LAW REVIEW 359, ___ (2003

28 Michael Geist, *Internet "choke points" put the squeeze on content*, TORONTO GLOBE AND MAIL, July 11, 2002, at B11 (concluding that "the rules for ISPs [are] increasingly settled.")

29 47 U.S.C. §230(c).

30 Zeran v. America Online, Ind., 129 F.3d 327 (4th Cir. 1997) (ISP not liable under §230 for posted statements that portrayed plaintiff has celebrating Oklahoma City bombings, even

But it is the second approach – robust, but limited shielding of ISPs – which became the dominant approach.[32] It is now the system in place for all information torts in the European Union and Japan as well as copyright and trademark infringements in the United States, China, and Singapore. Without reviewing the details of each national law, under this general type of regime, ISPs are shielded from liability for third party content transfers when the following conditions apply:

+ a ***non-control condition*** that the ISP creates or controls
  + **neither** the content of the third party information
  + **nor** who gets the third party information;

+ a ***limited retention condition*** that the ISP does not retain the information for longer than reasonable and necessary;

---

after ISP was alerted and failed to remove postings quickly); Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998) (ISP not liable under §230 for defamatory statement posted by ISP, even where it paid poster for the content and had editorial right to control content); Ben Ezra, Weinstein & Co. v. Am Online, Inc., 206 F.3d 980, 983 (10th Cir. 2000) (ISP not liable under §230 for distribution of inaccurate stock prices); Doe v. America Online, Inc., 783 So. 2d 1010 (Fla. 2001) (ISP not liable under §230 for retransmitting sexually explicit photographs); Barrett v. Rosenthal, 146 P.3d 510 (Cal. 2006) (section 230 creates immunity for republication of defamatory speech even where ISP may have been more than completely passive conduit); Chicago Lawyers' Committee for Civil Rights under Law, Inc. v. Craigslist, Inc., No. 07-CV-01101, 2008 BL 53042=3 (7th Cir., Mar. 14, 2008) (holding that electronic classifieds service Craigslist shielded from liability under the Fair Housing Act for discriminatory housing notices posted by users). *But see* Fair Housing Council of San Fernando Valley v. Roommates.com**,** LLC, 521 F.3d 1157, 1164-65 (9th Cir. 2008) (holding that section 230 does not shield a website which required certain information from users and provided a set of pre-chosen answers for the information which was ultimately displayed publicly, including discriminatory content).

31 47 U.S.C. § 230(e)(2) ("Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property."). There is a circuit conflict as to whether this includes state law IP claims. Compare Universal Commc'n Sys., Inc. v. Lycos, Inc., 478 F.3d 413 (1st Cir. 2007) (finding that state dilution claim was not barred by section 230) with Perfect10, Inc. v. CCBill LLC, 488 F.3d 1102, 1118-19 (9th Cir. 2007) (holding that "intellectual property" as excluded from section 230 immunity means only federal IP rights). Violations of federal criminal statutes and the Electronic Communications Privacy Act of 1986 are also exempted from the section 230 shield.

32 Ronald J. Mann and Seth R. Belzley, *The Promise of Internet Intermediary* Liability, 47 WM. & MARY L. REV. 239, 260-261 (2005) (After describing US limitations on liability, the authors note "[a]lthough the parallels are not perfect, other rjusidcitions seem to be taking a similar approach.")

+ a ***limited knowledge condition*** that the ISP does not know and/or does not have reason to know about the illegal nature of the information (this applies generally to hosting or caching[33]);

+ a ***prompt "take-down" or disablement condition*** characterized as the ISP removing or disabling information when it receives knowledge, notice, and/or proper allegation of a violation of law;[34] and

The last of these can be understood as a requirement of prompt action by the ISP *to eliminate its own knowing role* in the distribution of the allegedly tortuous materials. There is also usually:

+ a *user/**subscriber notification condition*** intended to provide some consumer protection and safeguards for free expression.[35]

This is a very rough, general formulation of the principles embodied in these laws, particularly in the United States' 1998 Digital Millennium Copyright Act ("DMCA")[36] for copyright infringements; the European Union's 2000 Electronic Commerce Directive[37] for information torts generally; Japan's 2001 Provider Liability

---

33 Singapore 193D; Japan Law No. 137 of 2001, articles 2 and 3; New Zealand, section 92C.

34 One of the main distinctions between the E-Commerce Directive and the DMCA is that the latter has elaborate "notification" provisions. The American statute shows a heavy, lobbyist-driven effort to parse a legal "notice" from the conditions of having "knowledge," i.e. a properly executed notice can establish knowledge, but the statute precludes a substantially inadequate notice from establishing that the ISP knows or should know of the infringement. 17 U.S.C. 512 _____. For discussions of the distinction between a 512(c)(3)(A) notice and knowledge standards for secondary liability *see also* Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 GEO. L.J. 1833, 1872-80 (2000); Emily Zarins, *Notice Versus Knowledge Under the DMCA's Safe Harbors*, 92 CAL. L. REV. 257 (2004).

35 In addition, non-EU jurisdictions commonly require that an ISP inform a customer that it is disabling or deleting materials that it has determined to be infringing or been notified to be infringing. United States 17 USC §512; Singapore §193DA(2); New Zealand Bill §92(c)(3); Japan xxx xxx xxx This reflects the concern during the DMCA negotiations that copyright infringement notices would be used to suppress distribution of speech in situations in which there was no probable copyright infringement. In the American law, the ISP subscriber is only required to be informed of the copyright holder's complaint – and the "take down" in a 512(c) hosting situation, not the other 512 sections.

36 17 U.S.C. § 512.

37 *See* E-Commerce Directive, *supra* note ___, arts. 12-14; *see also* draft U.K. Electronic Commerce (EC Directive) Regulations 2002, published _____ 2002, art. 17-19, available at _____. Among EU members, some had already passed statutes or had court decisions limiting ISP liability. Luxembourg's Law of 14 August 2000 limits ISP liability to conditions very similar to the DMCA, but for all bases for liability. *See* Veronique Hoffeld and Sara Delbecque, *Luxembourg*, in DENNIS CAMPBELL, ONLINE SERVICE PROVIDERS:

Limitation Act, also for information torts;[38] the Chinese People's Supreme Court "interpretations" Chinese copyright law in 2000 and 2004[39] as well as subsequent regulations;[40] and Singapore's 2005 amendments to their Copyright Act.

People familiar with the details of these various statutes and regulations might object that different conditions on my list do not apply to all ISPs[41] and that I am glossing over important differences among the laws, of which there are ***many.*** For example, Chinese law, instead of creating a safe harbor for ISPs that ***do not*** know and

---

INTERNATIONAL LAW AND REGULATION (2003), Binder I at Lux-7 [hereinafter CAMPBELL, ONLINE SERVICE PROVIDERS]. In a 2000 case, the Italian Supreme Court held that an ISP would not be held liable for defamation by one of its users absent the requirements of "conspiracy" in the Italian penal code being met. Corte de Cassazione, Decision Number 1141 of October 27, 2000, as reported in Francesco Portolano and Eugenio Prosperetti, *Italy* in CAMPBELL, ONLINE SERVICE PROVIDERS, Binder I at ITA-17-19. A December 2002 Law Commission report in the United Kingdom recommended that, if anything, European law on liability for third party defamations should be moved closer to the United States' section 230 standard, further protecting ISPs. *See* Owen Gibson, *Report backs ISP libel law claims*, THE GUARDIAN, Dec. 18, 2002.

38 JAPAN PROVIDER LIABILITY LIMITATION ACT, passed November 30, 2001 and effective May 27, 2002. The take-down procedures in the Japanese law, however, do not seem very "expeditious."

39 Interpretation by the Supreme People's Court (China) of Several Issues Relating to Adjudication of and Application of Law to Cases of Copyright Disputes on Computer Network, adopted at the 1144th meeting of the Adjudication Commission of the Supreme People's Court, December 21, 2000; Amended at the 1302nd Meeting of the Commission on 23 December 2003 and Entering into Force on 7 January 2004, available at www.cpahkltd.com/Archives.

40 Article 22 of the Regulations on Protection of the Right of Communication Through Information Networks, now provide:

"A network service provider which provides an information storage space to a service recipient, thus enabling the service recipient to make available to the public through information network a work, performance, or sound or video recording, and which meets the following conditions, bears no liability for compensation: ……

"(3) it does not know or has no reasonable grounds to know that the work, performance, or sound or video recording made available by the service recipient is an infringement; ……

"(5) upon receiving a written notification of the right owner, it removes, in accordance with the provisions of these Regulations, the work, performance, or sound or video recording which the right owner believes to be an infringement."

41 For a careful analysis of the American law, see Jennifer M Urban & Laura Quilter, *Efficient Process or « Chilling Effects » ? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act,* 22 SANTA CLARA COMP. & HIGH TECH. L. J. 621 (2006).

do remove infringing material promptly on notice, expressly imposes joint tortfeasor liability on ISPs that ***do not*** remove infringing material expeditiously.[42]
(One can argue about how much of a difference there is between creating safe harbors from (then) uncertain liability or just creating conditions of liability.[43]) In another broad difference, both the DMCA and the E-Commerce Directive have separate provisions applying different conditions to three main ISP functions: transmission, caching, and hosting information materials. The DMCA and Singapore's DMCA-inspired law also extend their safe harbor concepts to search engines;[44] the EU Directive does not.

Some of the differences drawn among different types of ISPs rest on technological or business model assumptions. The user/subscriber notification principle exists only in some places in some national law, typically where there would be an expectation of a contractual relationship between the ISP and the user (so that the ISP would have the means to notify the user). In the DMCA and E-Commerce Directive the knowledge standard was not included with transmission ISPs because it was generally believed that they would not have such knowledge – an assumption that may have turned out to be more technologically short-lived than most. But one important assumption that has seemed to be correct and enduring is that conditioning

---

42 INTERPRETATION BY THE SUPREME PEOPLE'S COURT OF SEVERAL ISSUES RELATING TO ADJUDICATION OF AND APPLICATION OF LAW TO CASES OF COPYRIGHT DISPUTES ON COMPUTER NETWORK, Adopted at the 1144th meeting of the Adjudication Commission of the Supreme People's Court, December 21, 2000, available in English at www.cpahkltd.com/Archives.

43 The DMCA has been criticized for its "failure to clarify the underlying law." Alfred C. Yen, *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability, and the First Amendment*, 88 Geo. L. J. 1833, 1838 (2000) [hereinafter Yen, *ISP Liability*] But after ten years, it may be that the varied approach of the DMCA and Chinese law is a distinction without a difference. ISPs abiding by the DMCA provisions has, as one would have expected, dampened case law developing the underlying liability. *Id.* at 1888. But if such a case ever arises, surely the 512 provisions will have some gravitational force in guiding a court to impose liability on an ISP who wandered too far outside the safe harbor. Professor Yen reasoned that "if Congress knows the desired result already, it should codify that result," *Id.* at 1891, a conclusion that is quite sensible except for one fact: no other part of third party liability in copyright is codified. And overall codification of third party liability in copyright? That's sounds like a lobbyists dream.

44 17 U.S.C. § 512 (d).

liability on knowledge has given ISPs a strong incentive to reduce or eliminate monitoring – distancing the ISPs from any role as private censors.

These statutory and regulatory systems have worked to varying degrees. The American law has been the subject to the most scrutiny, perhaps simply because of the size and prolixity of the American legal and law academic communities. While recognized to be "in some ways, an astounding success."[45] the DMCA section 512 liability limitations have been frequently critiqued by academics, concerned that the provisions would damage free expression on the Internet.[46] Since 1998, there have been a handful of high-profile examples of unquestionable misuses of the statute, some centered on core free expression concerns (such as postings about voting machines in the 2004 election[47] and Obama/McCain debates in the 2008 election).

A few studies have tried to verify these concerns by looking systematically at actual take-down notices. But these efforts have suffered from having too small (and potentially skewed) dataset. This is not the fault of the researchers – ISPs and content providers generally do not make public the take-down notices. The dataset readily available for study is a voluntarily-assembled compendium of take down notices hosted at ChillingEffects.org.[48] The Chilling Effects Clearinghouse provides internet users with valuable information (on defamation, copyright, and trademark) as well as bringing light to – and hopefully ridicule on – inappropriate, egregious, and/or overreaching take-down notices. But its database of less than 2,500 cease and desist letters (many of which are **not** DMCA take-down notices) provides too small a set to

---

45 Steven Seidenberg, *Copyright in the Age of YouTube*, ABA JOURNAL, February 2009 at 46, 48.

46 *See, e.g.* Yen, *ISP Liability, supra* note __ at 1838 (". . . the DMCA actually exacerbates conflicts between copyright and the First Amendment because it gives ISPs incentives to remove speech . . . from the Internet even though no copyright infringement has been established.")

47 Online Policy Group v. Diebold, Inc., 337 F. Supp. 2d 1195 (N.D. Cal. 2004). The Diebold company tried to use DMCA takedown notices to stop dissemination of internal emails showing problems with its electronic voting machines. As the *Diebold* court noted that "it is hard to imagine a subject the discussion of which could be more in the public interest." *Id.* at 1203.

48 The website was founded by Wendy Seltzer and is now a joint project of the Electronic Frontier Foundation and law clinics at seven law schools.

make any valid inferences about the effects of the DMCA take-down system on free expression.

For example, the 2005 "Will Fair Use Survive" report by Marjorie Heins and Tricia Beckle looked at the 263 take down notices for 2004 in the Chilling Effects database.[49] According to the two researchers "more than half of the 2004 letters did seem to state valid claims for copyright or trademark infringement,"[50] but Heins and Beckle nonetheless concluded that the take down notice system produced "significant suppression of criticism, commentary, or other likely fair and legal uses of copyright and trademark-protected works."[51] In another study, Jennifer Urban and Laura Quilter carefully scrutinized 876 entries submitted to the Chilling Effects database through August 2005,[52] finding a number of things, both predictable and unexpected.[53] They

---

[49] MARJORIE HEINS & TRICIA BECKLES, WILL FAIR USE SURVIVE? FREE EXPRESSION IN THE AGE OF COPYRIGHT CONTROL (2005), available at http://www.fepproject.org/policyreports/fairuseflyer.html. The only ISP that systematically releases – or *says* it systematically releases -- the take down notices it receives to the Chilling Effects website is Google. Thus, of the 263 cease and desist notices that this project looked at, 245 came from Google. *Id.* at 29.

[50] *Id.* at 36.

[51] *Id.* Because the focus of this project was free expression, the researchers properly focused on trademark claims too. But this makes it harder to judge the adverse impact *copyright laws* may be having. For example, of the seven examples of "weak IP claims" that the study describes, ALL are trademark claims (and so of them are weak indeed!). *Id.* at 33. There is no statutory take down system for trademark infringements, raising another interesting question: the degree to which customary practices have developed among trademark holders and ISPs parallel to the section 512 provisions – and whether these practices are occurring mainly as a function of background liability rules or mainly from imitation of section 512.

[52] Jennifer M Urban & Laura Quilter, *Efficient Process or « Chilling Effects » ? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act,* 22 SANTA CLARA COMP. & HIGH TECH. L. J. 621 (2006). As Urban and Quilter point out, that does not mean they will have covered all takedown notices dated before August 2005 since people may submit takedown notices to the Chilling Effects database years after the takedown notices originally issued.

[53] Among the observations that seem to me predictable or unsurprising are the following:

[a] That 68 of the 876 takedown notices were issued to ISPs that qualify as transmission ISPs, although, under the statute, they are not proper recipients of a 512(c) takedown notice. *Id.* at 644. As Urban and Quilter recognize, this seems to be copyright holders using the 512(c) notice system to establish a record of repeat infringers – perhaps triggering ISP obligations under _____ -- "where complaints about an alleged infringer might convince the OSP to terminate the alleged infringer's service" *Id.* at 651. To me, that's an unsurprising result of the statute's construction and does show "that the copyright industry's concerns about piracy are currently not well-addressed by the notice and take-down process." *Id.* at 652.

[b] that a small percentage – 4.2% (37 of 876) were directed at noncopyrightable subject matter. *Id.* at 668-669. But given that some of the things Urban and Quilter properly code as

too concluded that there was "unfortunately high incidence of questionable use of the process"[54] and a "continuous and perhaps unquantifiable effect on public discourse."[55]

Given that issues like the merit of a copyright claim or a fair use defense can be notoriously difficult, both these studies appear to have been careful and methodical – and, therefore, very valuable. (Urban and Quilter published much more detailed information, parsing the dataset different ways). But as the authors of these studies recognize, the real problem is the very small size of the sample – and that most of the takedown notices are supplied by one party, Google.[56] There are estimates that the RIAA and the MPAA themselves send out upwards of 50,000 take-down notices a year.[57] If we assume that there have been between 250,000 and 500,000 take down

---

non-copyrightable subject matter have only recently been litigated to that conclusion (prices) or are still grey zones (forms or straightforward product photographs), not all these notices may be abusive.

[c] that a larger percentage – 22% (193 of 876) included non-copyright claims [with or without a copyright claim] such as unfair competition, trademark infringement, or privacy claims. *Id.* at 678. It's no surprise that the DMCA take-down would be taken by private parties as a model for their conduct in other areas. *See also* Mark Lemley, *Rationalizing Internet Safe Harbors*, 6 J. Telecomm. & High Tech. L. 101, 108 (2007) (author reporting "a number of intermediaries that treat any content-based complaints they receive under the DMCA, whether or not those complaints involve copyrights).

Among the observations that seem to me unexpected:

[a] that were was no significant use of 512(c) and 512(d) takedown notices by movie and music industries. *Id.* at 651. This might reflect that the data set comes from before August 2005, i.e. before the rise of hosting sites like YouTube and social networking sites. Or it might just tell us that this dataset is skewed;

[b] that the 512(d) notices "appear to be used in some instances as a new weapon in the search-rank wars" *Id.* at 684. That certainly was a non-obvious result of the 512(d) provision.

54 *Id.* at 681.

55 *Id.* at 687.

56 84% of the takedown notices studied by Urban and Quilter were from Google. Urban & Quilter, *supra* note __ at 642. At a minimum, since most of the takedown notices that Google receives are for 512(d) "information location tool" services, any study of the dataset is skewed toward the kind of notices sent under 512(d). According to Urban and Quilter, 59% of the takedown notices in their study were strictly under 512(d). *Id.* at 644.

57 Urban and Quilter, *supra* note __ at 651-652 ("Our data do not reflect the very high numbers in the tens of thousands annually) of notices received by larger OSPs from the content industry . . .") and citing confidential interviews "which revealed that larger ISPs received tens-of-thousands of notices – largely 512(a) complaints – in a year." *Id.* at 684. Within a short time after the DMCA's passage, Yahoo was reporting receiving several thousand take down notices each quarter. Greg Wrenn, Associate General Counsel for Yahoo!, Inc., reported similarly high volumes, of several thousand notices each calendar quarter. A Look Back at the Notice-Takedown Provisions of the U.S. Digital Millennium

notices since the law's inception – "hundreds of thousands" according to one ABA journalist[58] -- then the researchers have only identified a very small amount of adverse impact on speech.

But can we nonetheless infer things from this small sample? Probably not. Because of the dataset's skewed nature – voluntary (perhaps motivated) submissions, mainly from one entity and unquestionably concentrated on ISPs to which the statutory take-down system does not technically apply – it would be irresponsible as policymakers to extrapolate from the percentages found to the full realm of take-down notices. The take-down system's "unquantifiable effect on public discourse" remains unquantifiable – potentially significant, potentially miniscule.[59] We just do not know.

Meanwhile, across the Atlantic, a simpler research project resulted in some praise for the American's notice and takedown system. [DESCRIPTION OF THE MULTATULI PROJECT]

Interestingly, this "Act 1" wave of legislative reform continues to lapse over national laws. One of the principle ways this is happening is through free trade agreements (FTAs) with the United States. Singapore's 2005 copyright law amendments – following its FTA with the US in 2003 -- largely repeated the US section 512 system. As early as 1992, Australia immunized "internet content hosts" and "internet service providers" from both civil and criminal liability for third party

---

Copyright Act One Year After Enactment, WIPO Workshop on Service Provider Liability, Dec. 1, 1999.

58 Seidenberg, *supra* note __ at 48.

59 Similarly, the fact that so few counter-notifications are filed can taken as evidence that the DMCA provisions are too complicated and copyright law too daunting OR as evidence that the take down notices identified unquestionably infringing material and the sources of the material (wisely) chose not to remain silent. Each of explanations is probably right some of the time and we just don't know the percentages between them. The combination of how the DMCA was created and its substantive provisions places makes it "legitimate censorship" in the analysis of Derek Bambauer. *See passim* Derek E. Bambauer, *Guilding the Censor's Scissors: Assessing Internet Filtering* manuscript available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1143582. Bambauer comments that the 'filtering' caused by the DMCA "is not mandated and emerged from established, particupatory public regulation process." *Id.* at 25.

information torts -- except copyright violations,[60] -- when they we "not aware of the nature of the content."[61] More recently Australian law has also enacted DMCA-like safe harbors for copyright infringement as a result of the Australia-US Free Trade Agreement (AUS FTA). Although the AUS FTA speaks in broad terms about ISP safe harbors,[62] the Australian government passed amendments to the 1968 Copyright Act making the safe harbors available only to "carriage service providers," i.e. companies that provide internet *access*.[63] As of late 2007, Chile, New Zealand, and Taiwan (Chinese Taipei) all had pending legislation to introduce these sorts of limitations on ISP liability into their copyright statutes.[64] Most, perhaps almost all, of this reform can be traced back to countries entering into or at least negotiating FTAs with the United States.

Promulgation of ISP liability limitations through FTAs warrants our attention for two reasons, First, as a mechanism it may speak of how bureaucrats and lobbyists get locked into one policy compromise and continue to promulgate that compromise despite changing circumstances. Second, it has been widely observed that the US (and EU) bilateral FTAs have been a way for these developed economies to force increased "TRIPS+" standards on developing countries, but it is worth noting that these DMCA-inspired limitations on ISP liability in FTAs with the US are a small example of bilateral agreements producing IP limits.

60 Clause 91 limits liability only in relation to causes of action arising under common law, equity, and the statutory laws of Australian states and territories. It, therefore, does not limit ISP liability in relation to any Australian federal causes of action which includes copyright.
61 Schedule 5 of the Australian Broadcasting Services Act of 1992 provides that [MORE]
62 Article 17.11.29 of the Australia-United States Free Trade Agreement.
63 Copyright Act 1968, s. 116AA
64 APEC-IPEC Preliminary Report on Copyright Exceptions and Limitations at 16.

II. Judges move against P2P and other infringement-based internet business models

While legislators and policy experts were focused on mainstream ISPs like AT&T. France Telecom, and Yahoo, a new generation of developers and companies began providing an additional, unanticipated layer of internet services – "Peer to Peer" systems. While legislators formulated limits on ISP liability for infringements by users, courts swiftly and consistently imposed liability on peer to peer ISPs for infringements by users. In all these cases, courts clearly understood that the P2P purveyors were engaged in infringement-based business models – and, more recently, Chinese courts have moved swiftly to impose liability on non-P2P websites that also seem to be infringement-based business models.

In peer to peer (P2P) systems the content being copied and transmitted across the internet is stored on and transmitted from individual user's personal computers – the "peers" – instead of larger server computers attached to the internet 24/7. With a P2P system, the user downloads the particular P2P software package to her computer; the software then typically sets up a "shared" media directory. The software allows the user to make inquiries as to what files are available from the shared media directories on other personal computers currently online that use that particular P2P system. How these queries are handled is the principle difference between the Napster, Morpheus, and FastTrack technologies explained below. In each of these systems, once user A has identified a desirable music file on user B's computer, the file is copied from user B's computer and transmitted directly to user A's computer; the file transmission is from a "peer" computer to another "peer" computer without going through a host server. The BitTorrent technology represents a new generation of P2P in the sense that it offers a new method of copying and distributing the media files across the network of users' computers – a method more efficient for large files, like feature films.

There is little question that the use of such P2P systems to distribute copyrighted works without authorization constitutes infringement. Even if the

downloading of a music file is permissible under a jurisdiction's fair use or private copying doctrines,[65] the making files available with downloading by others has been found – almost uniformly – to constitute infringement by the uploader of rights of distribution, transmission, communication, or making available to the public.[66] This is true even in the United States where controversy broke out in 2008 as to whether making files available without proof of downloading by anyone else constitutes "distribution" under section 106.

Enforcing copyright against P2P systems has meant both suing end users of the systems as well as the developers, distributors, and operators of the P2P networks. In 2003, music companies began filing actions against P2P end users in the US.[67] Even the public interest groups that had (half-heartedly) suggested "targeted lawsuits" against large-scale infringers[68] were probably dazed at the large numbers of suits against individuals that the music companies pursued. The music industry no longer publishes figures on the total number of law suit globally, but they are at or above the 100,000 range – just based on the actions in the US and EU.[69] In the US, these lawsuits typically settled in the 3-5,000 dollar range with reports indicating higher

---

65 For example, downloading was considered legal in the Netherlands under an interpretation of Dutch copyright law issued by the Ministry of Justice until a court in the The Hague ruled that the "explanation by the Minister and Government , which concludes that a private copy from an illegal source should be considered to be legal is violated [the law]." Tom Sanders, *Dutch court rules against law that allowed file downloading*, PCWorld, 27 June 2008, available at www.pcworld.idg.com.au/index.php/id;1262747976;fr;;fpid;;pf;1

66 A 2005 brochure an educational campaign organized by the record companies' international trade association states "[d]ownloading music from p2p is illegal in most countries, but people who 'share' or 'upload' music on the Internet, particularly if they upload a lot, run a greater risk of being sued or prosecuted." Childnet/Pro-Music, *Young People, Music & the Internet* (2005) (On file with the author).

67 See Amy Harmon, *Recording Industry Goes After Students Over Music Sharing*, N.Y. TIMES, Apr. 23, 2003, at A1. *See generally* Justin Hughes, *On the Logic of Suing One's Customers and the Dilemma of Infringement-Based Business Models,* 23 CARDOZO ARTS & ENT. L. J. 723 (2005).

68 Declan McCullagh, *End of an era for file-sharing chic?,* Cnet News.com, September 9, 2003 (quoting Electronic Frontier Foundation spokesperson Fred von Lohmann as calling for "a few targeted lawsuits" in April 2002 and Public Knowledge president Gigi Sohn recommending "[a]n industry-initiated lawsuit against a large-scale infringer" in September 2002).

69 The RIAA confirms 30,000 law suits in the United States and there are unofficial reports of 70,000 lawsuits in Germany alone. It is reasonable to think these two together are the lion's share of actions, but [MORE DETAILS] (based on RIAA correspondence with the author, October 27, 2008).

average settlements later[70] and the Electronic Frontier Foundation preferring to cite a settlement range going up to $11,000. In December 2008, the recording industry announced a cease-fire in these lawsuits against end users based on an agreement with major ISPs on identifying and warning downloaders. As discussed in Part IV, the ambiguities surrounding this cease-fire speak to the changing position of ISPs in the copyright enforcement terrain.

Quite separate from the end user lawsuits, the music industry began its litigation campaign against the developers, distributors, and operators of the P2P networks in 2000. Since then, courts in the United States, Japan, Australia, Korea, Germany, the Netherlands, and Norway have all confronted infringement through P2P systems. Viewed as a suite of cases, there are both striking commonalities and striking differences. First, all these courts seemed relatively untroubled by arguments that the P2P system should be shielded from liability on the same rationale as mainstream ISPs. More importantly, although courts have relied on different theories of liability, all but one have arrived at the same result: P2P developers, distributors, and operators have been found liable for copyright infringement by P2P users. In Japan, a developer of P2P software was found *criminally* liable for user infringement in December 2006, followed by 2008 convictions of P2P hub operators in the US, Finland, and Iceland.[71]

This is not to say that every jurisdiction with a sophisticated copyright law would necessarily impose secondary liability on the P2P systems and purveyors we have seen to date. In the UK and Singapore, there is precedent strongly suggesting

---

[70] A 2005 pro-music industry pamphlet targeted toward UK and European audiences says "On average, people who have settled out of court have had to pay thousands of euros." Childnet/Pro-Music, *Young People, Music & the Internet* (2005) (On file with the author).

[71] In the US, Daniel Dove was convicted and sentenced to eighteen (18) months imprisonment for his role as a "high level member of an Internet piracy organization" using BitTorrent. United States v. Dove, 585 F. Supp. 2d 865 (W.D. Va. 2008); United States v. Daniel Dove, 2008 U.S. Dist. LEXIS 65025 (W.D. Va. 2008). The Dove prosecution was part of a Department of Justice operation ("Operation D-Elite") which also resulted in at least seven other guilty pleas by participants in that BitTorrent system. Grant Gross, *Jury Convicts Web Site Operator in P2P Case,* N.Y. TIMES, June 27, 2009. *See also* Finreactor case, Finnish Court of Appeals, June 2008 (operators of BitTorrent index site held criminally liable for aiding copyright infringements); DC Hub case, Rekyavik District Court, March 2008 (operator of DirectConnect hub held criminally liable for abetting copyright infringements).

that P2P systems to be cleared of any responsibility.[72] But together these cases constitute the second act of the development of general ISP liability for a simple reason: what courts were really doing was imposing liability on internet business models that were blatantly based on copyright infringement. That is pounded home in the US Supreme Court's *Grokster* decision, in the reasoning of Japanese judges in their P2P cases, in the Australian *Kazaa* decision, and in the wave of Chinese court decisions in 2007-2008 that have imposed financial liability on non-P2P websites.

A. United States - A&M Records v. Napster, Inc. (2001)[73] and In re. Aimster Litigation (2003)[74]

As has happened with much of "internet law" American judges were the first to wade into the thicket of P2P disputes. So much has already been written about the three main litigations – *Napster* (2001), *Aimster* (2003), and *Grokster* (2005)[75] – that this

---

72 In the United Kingdom secondary liability takes the form of liability for "authorizing" the copyright infringement, but courts have construed this idea of "authorization" narrowly. CBS Songs Ltd. v. Amstrad Consumer Electronic plc, [1988] AC 1013 (defendant's advertising that its copying devices could be used to reproduce copyrighted material was not authorization); CBS Inc. v. Ames Records & Tapes Ltd, [1982] Ch 91, 106 ("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."). UK copyright law has provisions establishing different, additional forms of secondary liability. The most relevant of these may be section 24(2) of the UK Copyright, Design, and Patents Act 1988 establishing secondary liability when a person transmits a work via "a telecommunications system (otherwise than by communication to the public)" [NEEDS FURTHER RESEARCH] Singapore: Ong Seow Pheng v. Lotus Development [CITATION]. *See also* Daniel Seng, *Secondary Liability for Peer to Peer Software Networks – A Singapore Perspective*, paper presented at Fordham/Queen Mary/Singapore IP Academy Seminar, London, November 14, 2005 (concluding that analysis in *Ong Seow Pheng* case means that "a developer of peer-to-peer software such as Grokster or Kazaa, cannot be found liable under Singapore copyright law.")

73 239 F.3d 1004, 2001 U.S. App. LEXIS 5446 (9th Cir. 2001)

74 334 F.3d 643; 2003 U.S. App. LEXIS 13229 (7th Cir. 2003)

75 *See, e.g.* Stacey L. Dogan, *Is Napster a VCR? The Implications of Sony for Napster and Other Internet Technologies*, 52 HASTINGS L.J. 939 (2001); Alfred C. Yen, *A Preliminary Economic Analysis of Napster: Internet Technology, Copyright Liability, and the Possibility of Coasean Bargaining,* 26 DAYTON L. REV. 247 (2001); Raymond Shih Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U. Chi. L. Rev. 263 (2002); Jesse M. Feder, *Is Betamax Obsolete?: Sony Corp. of America v. Universal City Studios in the Age of Napster,* 37 CREIGHTON L. REV. 859 (2004); Raymond Shih Ray Ku, *Grokking Grokster,* 2005 WIS. L. REV. 1217; Pamela Samuelson, *Three Reactions to MGM v. Grokster,* 13 MICH. TELECOMM. TECH. L. REV. 177 (2006); Alfred C. Yen, Third-Party Copyright Liability After Grokster, 91 MINN. L. REV. 184 (2006); Anuj Desai, *Big Entertainment Needs a Sequel to the Highly Anticipated Flop: MGM v. Grokster,* 41 GA. L. REV. 579 (2007); Jane C. Ginsburg, *Separating the Sony Sheep From the*

discussion will only sketch out the important facts in each case and the basic elements of each court's imposition of liability.

The two traditional theories of secondary liability in American copyright law – contributory and vicarious liability -- were developed by courts[76] and later ambiguously embraced by Congress. Under the first form of secondary liability, a party can be a "contributory infringer" if that party knowingly causes or materially contributes to the infringing conduct of another.[77] In the 1982 *Sony Corp. v. Universal City Studios* decision[78] the Supreme Court imposed a significant limitation on contributory liability by importing into copyright law the "staple article of commerce" doctrine from patent law. Despite evidence that Sony-manufactured video tape recorders (VCRs) were being used to infringe plaintiffs' television shows, the majority in *Sony* concluded that the requisite level of knowledge for contributory liability could not be imputed to the VCR manufacturer and retailers where they made and sold a "staple article of commerce" capable of both infringing and "substantial noninfringing uses."[79] In contrast, vicarious liability – which is not limited by the *Sony* staple article of commerce doctrine -- arises when the party has the right and ability to supervise another person's infringing activities and the party has a direct financial interest in those activities.[80] In a 1988 case, Judge Gerard Goettel provided an elegant summary of the two routes for secondary liability under American copyright law: "[t]hus, just as benefit and control are the signposts of vicarious liability, so are knowledge and participation the touchstones of contributory infringement."[81]

Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs, 50 ARIZ. L. REV. 577 (2008).

76 Kalem Co. v. Harper Brothers, 222 U.S. 55 (1911)(); Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159 (2d Cir. 1971)()

77 Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971) ("one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a 'contributory' infringer").

78 Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 78 L. Ed. 2d 574, 104 S. Ct. 774 (1984).

79 *Id.* at 442

80 Shapiro, Bernstein & Co. v. H.L. Green Co., Inc., 316 F.2d 304 (2d Cir. 1963); Pinkham v. Sara Lee Corp., 983 F.2d 824 (8th Cir. 1992). *See also* Polygram Int'l Publ'g, Inc. v. Nevada/TIG, Inc., 855 F. Supp. 1314, 1325-26 (D. Mass. 1994).

81 Demetriades v. Kaufmann, 690 F. Supp. 289, 293 (S.D.N.Y. 1988).

Shawn Fanning's Napster software was the first generation of P2P software, allowing Napster users to exchange information about what MP3 files were available on their PCs through a central server. By all accounts, tens or hundreds of millions of unauthorized music files were reproduced and distributed through the internet with Napster providing what was essentially an "information location" service. Napster contended that its users' activities fell under section 107 fair use, but both trial and appellate courts concluded that the unauthorized downloading by most Napster users would not qualify as fair use.[82] At the same time, it was clear that a certain amount of the downloading by Napster users was *authorized* and that the Napster system "capacities" included non-infringing uses.[83] This set the stage for Napster to assert the *Sony* "staple article of commerce" defense when it was sued by the major record labels.

Relying on a central server that was under Napster's control ensured that Napster's leadership *could* know about copyright infringements, but much more importantly, the evidentiary record in the case established that Napster ***did*** have such actual knowledge.[84] Following the *Sony* decision, the Ninth Circuit drew "a clear distinction between the architecture of the Napster system and Napster's conduct in relation to the operational capacity of the system." Recognizing that the *Sony* rule was only a limitation on imputed knowledge (in the context of knowledge as a necessary condition for contributory liability), the Court concluded that *Sony* could not shield a defendant who had *actual knowledge* of infringements *as it was facilitating them.* Napster lost, its assets subsequently sold and reconstituted as a legitimate music business (by then, its main asset being the Napster name).

The *Napster* decision was scrutinized carefully by lawyers, technologists, and at least a few entrepreneurs – including one Johnny Deep. Like Napster, Johnny Deep's "Aimster" service used a central server to process P2P user queries on music files

82 239 F.3d at 1019 ("We find no error in the district court's determination that plaintiffs will likely succeed in establishing that Napster users do not have a fair use defense.")

83 The Court of Appeals criticized the district court for "improperly confin[ing] the use analysis to current uses, ignoring the system's capabilities" and for "plac[ing] undue weight on the proportion of current infringing use as compared to current and future noninfringing use." 239 F.3d at 1021.

84 239 F.3d at 1020, n. 5.

available from other users' PCs. But unlike Napster, the Aimster system encrypted user communications so that "the encryption feature of Aimster's service prevented Deep from knowing what songs were being copied by the users of his system."[85] In other words, Mr. Deep designed his system to deny himself the actual knowledge that apparently had been Napster's undoing. Aimster also provided its users with tutorials that instructed people on the downloading of music files. While Napster was shut down before having learned how to "monetize" their user base, Deep provided a "Club Aimster" premium service that allowed its members "for a fee of $4.95 a month to download with a single click the music most often shared by Aimster users."

With only the *Sony* and *Napster* decisions as guideposts, Judge Posner's decision in *Aimster* is remarkable for how much he throws into the mix, trying to develop and reshape the contours of indirect liability in copyright. First, Posner interpreted the *Sony* staple article of commerce doctrine more narrowly than the words facially suggest:

> **We also do not buy Aimster's argument that . . . all Aimster has to show in order to escape liability for contributory infringement is that its file-sharing system *could* be used in noninfringing ways, which obviously it could be. Were that the law, the seller of a product or service used *solely* to facilitate copyright infringement, though it was capable in principle of noninfringing uses, would be immune from liability for contributory infringement.[86]**

Posner then expressly interprets substantial non-infringing uses through a cost/benefit analysis, suggesting an approach more akin to what the district court judge had done – and the appellate court had criticized- in *Napster*. For Posner, neither theoretical non-infringing uses nor a pittance of actual non-infringing uses will save a P2P system if the system is used principally for copyright infringement. *Once* "substantial non-infringing uses, present or prospective, are demonstrated," Posner tells us that "some estimate of the respective magnitudes of these [two kinds of] uses is necessary for a finding of

---

85 334 F.3d at 650.

86 334 F.3d at 651. Arguably, this pushes back toward patent law's "suitable for substantial non-infringing uses" test. The patent standard provides a defensive shield only "where non-infringing uses are common," D.O.C.C. v. Sprintech, Inc., 36 U.S.P.Q.2d 1145, 1155 (S.D.N.Y. 1994), and "a theoretical capability [for non-infringing use] does not suffice," Alcon Laboratories, Inc. v. Allergan, 17 U.S.P.Q.2d 1365, 1369 (N.D. Tex. 1990).

contributory infringement,"[87] suggesting that a staple article of commerce defense will not prevail unless the non-infringing uses reach some *relative* measure against the infringing activities.

Of course, an *ex post* cost/benefit analysis of uses was not the thrust of Aimster's defense. And it surely would be a technologist's nightmare for a liability test. Deep had based his defense – and Aimster's design -- on *some* substantial non-infringing uses being self-evident so that he would escape liability through his lack of knowledge and the *Sony* axiom that "constructive knowledge" of infringing uses is not enough for contributory infringement.[88] To avoid that result, Judge Posner interpreted Deep's encryption strategy as "willful blindness" and then (a) deftly equated that willful blindness with *knowledge* and (b) went to far as to say that it was evidence of *criminal intent*.[89] By this reasoning, Posner concluded that Deep could not avoid liability "by using encryption software to prevent himself from learning what surely he strongly suspects to be the case: that the users of his service—maybe *all* the users of his service—are copyright infringers." Recognizing that this conclusion concerning system design and willful blindness could have broad ramifications, Posner distinguished Aimster's design from non-incriminating uses of encryption in a way that implicitly turned on Deep's initial epistemic state (a suspicion of widespread infringement) and his initial intent (not to learn what was happening)[90] In this way, a double layering of intent pulls Deep and Aimster outside the protection of *Sony* through an "actual knowledge" equivalent – willful blindness.[91] Carefully parsing the

---

87 *Aimster*, 334 F.3d at 649-50.

> What is true is that when a supplier is offering a product or service that has noninfringing as well as infringing uses, some estimate of the respective magnitudes of these uses is necessary for a finding of contributory infringement. The Court's action in striking the cost-benefit trade-off in favor of Sony came to seem prescient when it later turned out that the principal use of video recorders was to allow people to watch at home movies that they bought or rented rather than to tape television programs.

88 *Sony*, 464 U.S. at 439.

89 334 F.3d at 650

90 334 F.3d at 650-651 ("Our point is only that a service provider that would otherwise be a contributory infringer does not obtain immunity by using encryption to shield itself from actual knowledge of the unlawful purposes for which the service is being used.").

91 It is not completely clear whether it is *willful blindness equals actual knowledge* or intent that

Aimster decision, one realizes that the whole edifice that Posner constructs really does rely on Deep's initial intent, making the *Aimster* opinion a suitable, if somewhat opaque, antecedent to the Supreme Court's decision two years later in *MGM v. Grokster*.

[Next sections excerpted – contact the author for more recent version]

---

robs Aimster of its *Sony* shield. Posner also discusses Aimster's "invitation to infringe" as distinguishing Aimster from Sony, but does not directly connect that "invitation" to intent. *Id.* at 651.

> In explaining how to use the Aimster software, the tutorial gives as its *only* examples of file sharing the sharing of copyrighted music, including copyrighted music that the recording industry had notified Aimster was being infringed by Aimster's users. The tutorial is the invitation to infringement that the Supreme Court found was missing in *Sony*.

Posner says that the Ninth Circuit erred in "in suggesting that actual knowledge of specific infringing uses is a sufficient condition for deeming a facilitator a contributory infringer." *Id.* at 649 (suggesting that willful blindness equals actual knowledge would not be enough to bring *Aimster* outside *Sony* in Posner's mind).

C. The Japanese recognize inducement first -- The File Rogue (2003)

Just a few months before the U.S. Supreme Court issued its *Grokster* decision, the High Court of Tokyo had already reached the "inducement" reasoning in Japan's first case against a P2P developer or operator, the *File Rogue* case.[92] The discussion here will elaborate a little more on these decisions because they have rarely been discussed in English-language legal literature.

In most respects, the File Rogue fact pattern appears to be very similar to the Napster case. Through a server in Canada, the defendant provided a free, Japanese language-only file sharing service named "File Rogue." As with Napster, the File Rogue software created a designated folder for sharing and information about files in this folder -- file name, folder name, file size, user name, IP address and port number -- was automatically transmitted to the File Rogue server.[93] As with Napster, the files were exchanged directly between the users and the central server only had the function to make the files automatically searchable, visible and exchangeable. Nineteen record companies operating in Japan brought suit against MMO Japan, the corporate provider of File Rogue, and the Tokyo District Court issued a final judgment against MMO on December 17, 2003.[94] MMO appealed and the High Court of Tokyo affirmed the lower court's decision on March 31, 2005.

On the question of primary infringement, the district court concluded – and the appellate court affirmed – that File Rogue users infringed plaintiffs' neighboring rights of reproduction and of making works "transmissible" under Article 92bis (1) of

---

[92] Tokyo District Court Heisei 14(Wa)4249 (2003); High Court of Tokyo Heisei 16(Ne)446 (2005). English quotations come from "File Rogue Case" (Kazuo Makino, trans.) in KAZUO MAKINO, CASEBOOK OF INTELLECTUAL PROPERTY RIGHTS (2) 15 (Japan Patent Office, 2005) (translating and summarizing trial court interlocutory order) and Shinji Niioka and Justin Hughes, *The File Rogue Case* (translation and summary manuscript on file with the author) (summarizing trial and appellate decisions) [hereinafter Niioka and Hughes].

[93] Niioka and Hughes, *supra* note __ at 2.

[94] Makino, *supra* note _ at 218.

the Japanese Copyright Act.[95] The court reasoned that the personal use exception pursuant to Articles 30(1) and 102(1) of the Japanese Copyright Act[96] was not applicable because the users intended – from the beginning of their activities -- to make the files publicly available.

On the question of MMO's secondary liability for the file sharing, the trial court sought to "assess[]the overall situation" identifying three pertinent factors: "(i) the content and nature of MMO's conduct, (ii) the degree of MMO's control/supervision over the users' conduct to make works transmissible, and (iii) MMO's profits through its conduct."[97] Concerning the "content and nature of the service," the trial court had noted that "96.7 % of the file information on MMO's server were information on marketed records and neither consent nor waiver were given by copyright owners. [T]herefore, it was obvious that most of the mp3 files were illegal reproductions." Notice that while the juridical tools are different the facts the judge focuses upon are the same that would concern a judge guided by *Sony*, *Napster,* and *Aimster*. The high percentage of obvious infringements indicates both knowledge and a lack of substantial non-infringing uses, at least as Judge Posner would analyze it.

While agreeing with the three criteria announced by the trial judge, the Tokyo High Court used the first and second criteria to emphasize the defendant's knowledge of how its P2P system was being used:

> **Moreover, MMO knew of the problems of Napster before it started its Service since it was well-known in Japan […], and on November 1, 2001, there was a**

---

[95] Article 92bis (1) of the Japanese Copyright Act provides that "[p]erformers shall have the exclusive right to make their performances transmissible." COPYRIGHT RESEARCH & INFORMATION CENTER, COPYRIGHT LAW OF JAPAN 86 (Yukifusa Oyama et al. trans., 1999). Makino, *supra* note _ at 216.

[96] Art. 30 (1) of the Japanese Copyright Act provides that "[I]t shall be permissible for a user to reproduce by himself a work forming the subject matter of copyright . . . for the purposes of his personal use, family use or other similar uses within a limited circle (hereinafter referred to as 'private use')" COPYRIGHT RESEARCH & INFORMATION CENTER, COPYRIGHT LAW OF JAPAN 86 (Yukifusa Oyama et al. trans., 1999). Article 30(1) then exempts from "private use" photocopying on public photocopiers, rt. 30(1)(i), and copies made via circumvention of technological protection measures, Art. 30(1)(ii). The former is subject to an equitable remuneration system under Japanese law.

[97] Niioka and Hughes, *supra* note ___ at 3; Makino, *supra* note _ at 216.

> **television broadcast in which MMO's president commented on JASRAC's statement 'legal steps against copyright infringements must be considered' with 'we are only providing a forum to freely exchange files and how users use this forum, it is not within our responsibility.' Therefore, MMO knew (*ninshiki*) and expected (*yosou*) that there would be problems with copyright infringements.**[98]

One sees in this excerpt, again, familiar themes: the P2P provider echoes a substantial non-infringing uses argument and the court counters this with a finding of sufficiently specific knowledge. The *Rogue* File courts also focus on the core of vicarious liability, concluding that defendant MMO had the ability to "screen file exchanges" through its central server (just as the original Napster had) and both courts reasoned that while MMO had yet to make a profit, the profit incentive drove MMO, in the trial court's words, to "to increase the number of music file information and file exchanges."

But it is the appellate court's overall analysis that warrants most of our attention:

> **"[…this case] is not a situation where illegal use of the Service simply occurred; considering the nature of the Service, [MMO] induced with a specific and realistic probability (*gutaiteki katsu genjitsutekina gaizenseiwo motte […] jakkisuru*) a specific kind of copyright infringement. MMO provided its Service although it expected (*yosou*) such infringements, and it also had control over those conducts. If MMO received commercial profit from such controllable conducts, it is self-understood that it is held liable and to be considered as a main factor (*shutai*) to such infringements."**[99]

In other words, the Tokyo High Court assumed that an actor who acts *with the expectation of a likely outcome* actually *intends* that *outcome* – an alloying of knowledge, expectation, and intention that is also found in the American Restatement of Torts. The resulting test of "inducing with a specific and realistic probability a specific kind of copyright infringement" is certainly one that could be applied to all three of the American cases – as well as the Kazaa case in Australia and the Chinese cases discussed below.

[Next sections excerpted – contact the author for more recent version]

---

98 Niioka and Hughes, *supra* note ___ at 4.
99 Niioka and Hughes, *supra* note ___ at 3.

F. Chinese courts attack infringement-based internet business models 2007-2008

The Chinese courts are the most recent to enter the fray – and have done so with a splash. Article 22 of the current Regulations on the Protection of the Right of Communication through Information Networks (the Regulations) provides an ISP *could* be jointly liable for copyright infringements by its users *unless* the ISP "does not know or has no reasonable grounds to know that the work, performance, or sound or video recording made available by the service recipient is an infringement." Article 23 of the Regulations reinforces this.[100] The courts have applied these provisions stringently, finding both search engines and UGC sites liable for copyright infringement *when they set up their business model in such a way that infringement seems to be promoted.*

The search engine case the 2007 *Go East Entertainment v. Beijing Alibaba Information and Technology* decision from the Court of Appeals in the Haidan district of Beijing.[101] Alibaba is the company that runs Yahoo's "Music Box" music search service in China. The Yahoo China/Alibaba service ("Alibaba") had characteristics of a conventional search engine, but with functionality specially suited for locating and downloading music. (This section is written in the past tense but the author does not know if the service was shuttered or significantly reconfigured following the judgment.)

---

[100] Article 23 provides "A searching or linking service provider shall not bear liability if it cuts off the links to any infringing work, performance or audio/video recording as soon as it receives a notice of infringement sent by the copyright owner. However, if it knows or should know that the linked work, performance or audio/video recording is infringing, it should bear liability for joint tort."

[101] Go East Entertainment Company Limited v. Beijing Alibaba Information and Technology Co., Ltd., Beijing Higher People's Court, Civil Judgment, (2007) Gaominzhongzi No. 1191, Judgment of Dec. 20, 2007, affirming Go East Entertainment Company Limited v. Beijing Alibaba Information and Technology Co., Ltd., Beijing No. 2 Intermediate People's Court, Civil Judgment, (2007) erzhongminchuzi No. 02627, Judgment of April 24, 2007. [Translations on file with the author and forthcoming in Cardozo Arts & Entertainment Law Journal.]

When a user conducted a search for a song on the Alibaba service – let's say "Yan Yuan" by Wilfred Lau – Alibaba gave the user search results with "try listening" or download options. The user could exercise either option without leaving the Alibaba website[102] – quite useful for keeping advertising eyeballs. Instead of just responding to search requests, Alibaba also categorized and classified links by "various styles, popularity of the tracks, gender of the artist, etc";[103] indeed, the user "entering the search page of Yahoo music finds 18 columns of classifications" ranging from a search lyrics function to "All Female Artists" to "Hot New Track Rank."[104] In addition, the service gave the user functionality to create one's own album with downloads, create one's own rankings of music, and make all these "public" so "that the information would be seen by other network users."[105]

Needless to say, Alibaba quickly came under the scrutiny of both international and Chinese copyright owners.[106] The factual record in the case has various nuggets of interest. When Go East, a Hong Kong record label with a variety of Chinese artists, sent Alibaba a list of its protected sound recordings and correlated infringing URLs, Go East asked that *all* links to the songs be removed, not just the identified URLs. Go East sought this action on the grounds that no sites or downloads that Alibaba was indexing were authorized.[107] But Alibaba replied that "only the URL addresses provided in the Notice would be removed."[108] The back and forth between the two

---

102 *Id.* at 2.
103 *Id.* at 3.
104 *Id.* at 10.
105 *Id.*
106 In the pre-litigation back and forth, Alibaba advised the representatives of foreign record companies, the International Federation of Phonogram Industries (IFPI) that Alibaba was in the process of installing filters to prevent non-Chinese IP addresses from using the service "and to screen out the non-Chinese search results." *Id.* at 3. To the degree that was actually Alibaba's plan, it shows an interesting attempt to continue its free-riding operations, seeking to placate international copyright owners while allowing local artists to continue to be "shared." This plan was frustrated when Alibaba was sued by Go East, holding extensive rights in Chinese sound recordings.
107 *Id.* at 3.
108 *Id.*

sides on this issue[109] obviously mirrors one of the key bones of contention between Viacom and YouTube.

The trial court held that Alibaba's service did not "constitute reproduction or network distribution of the sound recordings at issue,"[110] but found that Go East's "notice" to Alibaba was proper ("justifiable") and had made Alibaba "aware that the search results through its music search service contain sound recordings that infringe Go East's producer rights."[111] On that basis, the trial court held Alibaba jointly liable for the infringements and awarded Go East damages and costs of 21,400 RMB ($3,130). On appeal, the Beijing Higher People's Court affirmed both trial court conclusions. The appellate court held that Alibaba was not a direct infringer -- applying both what Americans would call the "server" test and a user experience test[112] -- but the appellate panel also held that Alibaba was jointly liable for the infringement because it knew or should have known was happening through its search service.

After setting out the standard of liability in Article 23 of the Regulations on [Protection of the Dissemination Right through Information Network], the appellate court said that even if "the rights owners did not sent our Notices meeting the requirements" of the Regulation, "the internet service provider shall still bear infringement liability if it knows or ought to have known about the infringement, but continues to provide search and linking services." The court added that "subjective fault" was necessary for joint liability, describing the standards as follows:

---

109 *Id.* at 12 (After Go East asked that *all* links to the songs deleted, "Alibabe Company sent a letter to the attorney of Go East HK and claimed that they could only delete the relevant links whose URL addresses were listed in the Letter. On 3 and 10 August 2006, the attorney for Go East HK sent letters to Alibaba Company twice, emphasizing that all the links related to the tracks involved in the case on the Yahoo China website were infringing and requesting to delete not only the specific links with URL addresses listed, but also all the searching results related to all the works mentioned in the Letter.")

110 *Id.* at 4.

111 *Id.* at 5.

112 *Id.* at 14 ("the aforesaid service of Alibabaa Company still belongs to search and linking services and it does not reproduce or distribute to the public the alleged infringing sound recordings from its services, while its service pattern would not mislead network users to believe that they sound recordings at issue are sourced from the Yahoo China website.")

> **To judge whether the party has subjective fault or not, it should be considered whether the party is able to and should foresee the native results that will be caused by its act, based on the competence and extent of the party's foresight [foreseeability], as well as considering the average level of foresight, professional conduct, and so on.**[113]

By this standard, the court had no problem in concluding that Alibaba was jointly liable for the infringements, not because of the notices it received from Go East, but from Alibaba's own business model:

> **Obviously, Alibaba Company, of its own volition, collects, organizes, and categorizes relevant music information, and sets up corresponding classifications according to various criteria. As a search engine provider, Alibaba Company carries out a music search business, providing professional music search services to users and gaining profit from such activities; its website belongs to specialized music websites. With all the above concerns, according to the criteria to judge subjective fault, Alibaba Company should have known and is able to know the legal status of the sound recordings searched and linked by it. Especially after Go East had notified Alibaba Company several times in writing the various sorts of music search services provided on its Yahoo China website in respect of the sound recordings at issue were all infringing, and requested Alibaba Company to remove the links, Alibaba should have paid even more attention to the legal status of the sound recordings [of plaintiff's music] and taken relevant measures. But Alibaba Company only deleted the links for which Go East provided specific URL addresses and left untouched other search links in relation to the sound recordings at issue. It is obvious that Alibaba Company has neglected its due diligence and indulged the infringement; it should be concluded that Yahoo China has subjective fault.**[114]

The court concluded that "Alibaba in fact has participated in and assisted the linked third party websites to carry out infringement, has obvious subjective fault, . . . and shall bear legal responsibility for the infringements."[115]

The Chinese courts have also handled a wave of cases against UGC sites in which the UGC sites, like Alibaba, arranged their business model in ways that showed a clear intent to exploit the presence of unauthorized uploads. The 2007 *Zhongkai Co. v. Poco.com* decision concerned Poco.com, a popular UGC sit hosting many feature films; the plaintiff's had its theatrical release in Hong Kong min November 2005 and

---

113 *Id.* at 15.
114 *Id.* at 15-16.
115 *Id.* at 16.

appeared almost immediately on Poco.com.[116] The Shanghai trial court concluded that the website knew that it was hosting many recently-released feature films and that it *should have known* these films were infringing because "[i]t is common sense that the copyright owner was unlikely to license others to transmit the movie via Internet free of charge, so obviously the movie was uploaded without license." Perhaps critical to the defendant's liability was that it had created an area of its UGC website called the "movie exchange zone"; the court held that in taking this approach to attract users – to give it more advertising income – "the defendant had a duty to review the legality of movies uploaded onto the 'movie exchange zone'; the defendant turned a blind eye to the obvious infringing activities of its users and should be liable." In 2008, the Shanghai High Court affirmed the ruling that Poco.com "must have known or at least should have known" that the plaintiff's movie had not been authorized for distribution on the site.

[Next sections excerpted – contact the author for more recent version]

[116] Zhongkai Co. v. Poco.com, Shanghai No.1 Intermediate Court(2007) [full citation to come]

III. New curve of technology?

Internet service providers all over the world remain understandably firm – at least in their public statements -- that "they should not be responsible for policing their users."[117] But ISPs were never absolved of responsibility for their users – completely and come what may technologically. In the 1995 *Netcom* case, the district court refused to grant the ISPs motion for summary judgment on contributory liability, concluding it would be fair to hold Netcom liable when it knew about infringements and was 'able to take simple measures to prevent further damage to plaintiff's copyrighted works";[118] Japanese law expressly premises ISP potential ISP liability on it being "technically possible to take measures to prevent transmission of the [infringing] information";[119] and, unnoticed by many, in 2007 the Ninth Circuit reiterated the *Netcom* test of liability when "simple measures" to prevent infringement are available. Although outside the scope of this paper, laws – in Japan, the US, China, and elsewhere -- requiring ISPs to turn over information on subscribers alleged to infringe copyright are another form of ISP "responsibility."

The problem for the ISPs is that we are now entering a period when technological measures – filters – look better, cheaper, and increasingly effective. As Ronald Mann and Seth Belzley note, "[a]s monitoring becomes cheaper, it ineluctably becomes relatively more desirable to rely on such monitoring as the least expensive way to eradicate undesirable activity."[120] Moreover, some ISPs are already using these monitoring capacities to their own ends. All this tempts courts and legislature, prodded by music and audiovisual companies, to demand increased participation by

---

[117] Asher Moses, *Music industry has Aussie pirates in the crosshairs*, SYDNEY MORNING HERALD, October 8, 2007 (describing the position of Australian ISPs).

[118] 907 F. Supp. at 1375.

[119] Article 3 of the Japan – Provider Liability Limitation Act of November 30, 2001.

[120] Mann & Belzley, *supra* note __ at 268 ("[A]dvances in information technology make it increasingly cost effective for intermediaries to monitor more closely the activities of those who use their networks. As s monitoring becomes cheaper, it ineluctably becomes relatively more desirable to rely on such monitoring as the least expensive way to eradicate undesirable activity.") It should be noted that Mann and Belzley are very clear that controlling copyright infringement is not the focus of their paper and they express doubts about focusing on P2P systems for regulation.

ISPs in the overall mix of copyright enforcement. Before turning to those debates in the courts and legislatures, let us consider here how the technology is changing – first through a discussion of host site filtering technology, then the technology of "deep packet inspection," and the initial skirmish in the net neutrality debate. The discussion in Part IV then turns to some of the disparate ways in which greater responsibility is being imposed – or trying to be imposed -- on ISPs.

A. How technology shifted 2002-2008: filtering technologies

At the time of the *Netcom* and *Napster* litigations, the only filtering system the courts discussed was "key word" filtering – that is, filtering by the title or artist name attached to the music file. This is a simple search for alphanumeric strings in the metadata associated with the music file – a search for <radiohead>, <bowie>, <shut up and drive> or, more improbably, <appalachian spring>. Key word filtering remains a useful technique, particularly when it also catches obvious misspellings, either errors or intentional efforts to keep an alphanumeric string legible to humans while avoiding automated detection (like naming a file as "b0w1e – 1et5 d4nce"). Detection of keyword misspellings is a cat-and-mouse game, but a game of fairly limited range since the title and artist information must remain identifiable to the average human using a P2P system. Because of this constraint, keyword filters remain useful for any ISP that receives title and artist metadata attached to a file (such as a hosting site or an information location tool).

But filtering technology has evolved rapidly beyond key word searching – and presumably will continue to evolve. Since 2001, there has been significant development in three broad areas of filtering technology that make keyword filters seem primitive (a) "hash" value filters, (b) audio fingerprinting, and (c) video fingerprinting. It is worth reviewing these technologies briefly.

Every digital file has a "hash" number representing characteristics of the file; when a file is copied perfectly, the new copy retains the same hash number. When a file is modestly changed – a 4:36 minute music track is copied as a 4:27 minute track, the hash number changes. Thus, hash number filtering will capture a substantial

amount of unauthorized reproduction as that reproduction has been done to date. The UGC website Veoh apparently has used has filters in conjunction with DMCA take-down notices, i.e. once it receives a take-down notice concerning one video upload, it make a hash value measurement of the allegedly infringing video and refuses future attempts to upload videos with matching hash values. But because it would be easy to constantly change the file hash numbers of a digital file (music or video) through an automated process, hash filtering, by itself, could be easily frustrated.[121]

In contrast to a hash, an "audio fingerprint" technique measures the actual sound pattern produced by a digital file: this type of filtering "analyze[s] the shape of the spectrum represented by a digital audio file." To be most useful, an audio fingerprint will not be for the entire track, but for key passages of a music track. This allows the audio fingerprint to match against the music file even when [a] the beginning or end of the file is changed (producing a new hash number) or [b] portions of the track are substantially remixed. In other words, for a 5:20 minute, it would be better to have 2-3 fingerprints of 20 second portions of the track than worry about storing and matching against the entire 5:20 minutes. Of course, the smaller the portions of a track that you are using for matches, the greater the likelihood that some fair uses will be mis-identified as infringing. Over a dozen different audio (or acoustic) fingerprinting technologies have been made public, including systems from Audible Magic, SNOCAP, the Fraunhofer Society, and Gracenote.

Video fingerprint technology similarly seeks to recognize a limited visual pattern that would be integral to an audiovisual work. One method is to match a series of frames – using X number of "snapshot" frames from a key sequence of a audiovisual work.[122] Of course, audiovisual works can also be recognized by their *audio* fingerprint. In early 2007, ahead of its own development of proprietary video filtering

---

121 Of course, any such process attached to a P2P system would surely manifest intent to infringe because there are no obvious reasons to want to change hash numbers on these files *except* to avoid filtering system matches

122 One Google employee described their "YouTube Video ID" software as involving 50 PowerPoint pages of differential equations. Elise Ackerman, *Google releases video filtering system*, SAN JOSE MERCURY NEWS, October 15, 2007.

technology, Google was making limited use of Audible Magic's audio fingerprinting filter.[123] Although parties still argue about cost issues, it is clear that these filtering systems are more economically and technologically viable than they were in 2000 or 2002. In the *Scarlet* case discussed below the court accepted evidence that it would cost a medium-sized ISP approximately $.50 - .75 a month per subscriber to install effectively filtering technology [MORE].

Each of these filtering systems requires one to begin with a databases of protected works to be compared against materials being made available by end users, i.e., one needs a database of the relevant metadata (titles, artists), hash values, audio fingerprints or visual fingerprints. Creation and control of such databases has been a recurring bone of contention when filtering is being discussed.[124] One obvious answer would be a model in which the database is maintained by a trusted intermediary. The music and audiovisual industries already rely on trusted intermediaries for the manufacture of CDs and DVDs as well as the making and distribution of film prints for cinema projection – all this requires giving control of the "master" to third parties. A trusted intermediary that controlled the database and ran the filters in conjunction with the ISP surely should be acceptable to these content providers.

---

123 Kenneth Li and Eric Auchard, *YouTube to test video ID with Time Warner and Disney*, REUTERS, June 12, 2007, 10:28am, reported in Yahoo! UK & Ireland ("YouTube officiails said they have quietly been testing ways to help identify the audio tracks of video clips with major labels using technology from privately held Audible Magic as early as the first two months of 2007"); Elise Ackerman, *Google releases video filtering system*, SAN JOSE MERCURY NEWS, October 15, 2007.

124 [KAZAA case]. Metro-Goldwyn-Mayer Studios v. Grokster, Order Granting in Part Plaintiff's Motion for a Permanent Injunction, October 16, 2007 at 5 ("Plaintiffs have reportedly refused to turn over a list of artists that they want filtered."). See also Elise Ackerman, *Google releases video filtering system*, SAN JOSE MERCURY NEWS, October 15, 2007 ("Google needs copyright owners to submit copies of their materials to the Google database. 'We need their cooperation,' he said," referring to David King, a Google product manager. But it is unclear whether copyright owners will be willing to turn over decades of programming to Google.") In what looks like a coordinated corporate message, here days later on the launch of a local, Chinese language YouTube site for the Taiwan market, the "co-founder" of thhe YouTube Taiwan site, Steve Chen, said "[w]e need to work with content providers to collect a database (of video clips)." Associated Press, *Google's YouTube launches Taiwan video-sharing site*, in SAN JOSE MERCURY NEWS, October 18, 2007.

It should be clear that the most robust filtering system will employ more than one of these techniques and use multiple filters dynamically. For example, positive matches to an initial database of keyword metadata can be measured to generate new audio fingerprints values to be added to a database for the audio fingerprint filtering; positive audio fingerprint matches from that process can be used to generate new hash values to filter (as the music file changes slightly in size); positive audio fingerprint and hash value matches can, in turn, be used to generate new keyword metadata entries to filter (as a file labeled "Blondie" reappears in the system under the label "bl0ndie," then "bl0nd1e," etc.). An example of such an integrated filtering approach is discussed in the 2007 trial court opinion in the *Grokster* litigation. StreamCast initially developed its own metadata filter by using artist information from the RIAA website as well as Billboard top 40 lists; it then used matches from that metadata to build up a set of hash values for filtering.[125]

Different configurations of filters along this general description can be used by web host ISPs (who can filter files loaded up to websites or social networking pages or UGC services), cache ISPs, and information location ISPs. These filters are evolving technology that an ISP could deploy, but the ISPs have no obvious self-interest in doing do. This contrasts with packet inspection technology, a controversial filtering technology that is relevant to transmission ISPs (but, as we will see, is not the only way that transmission ISPs can filter).

B. How technology shifted 2002-2008: packet inspection and the debate about network neutrality

The amazing adoption rate of the Internet in the 1990s and early 2000s was possible because all the hardware had been "pre-positioned" – almost everyone had telephone and/or cable services and tens of millions had personal computers. All that remained was to distribute a method for the computers to talk to one another through

[125] Metro-Goldwyn-Mayer Studios v. Grokster, Order Granting in Part Plaintiff's Motion for a Permanent Injunction, October 16, 2007 at 6. ("Using each artist name as a search term keyword, the batch process scan the P2P networks accessed by Morpheus users and save all audio and visual hash values obtained from the search results. The hash values are then stored on a hash database server that StreamCast created and maintains." *Quoting* the declaration of Michael Weiss, StreamCast CEO.)

the telephone and cable lines. That method, the Transmission Control Protocol/Internet Protocol (TCP/IP), breaks data flows into "packets" as if a novel were transported by ripping it into individual pages and sending each page in its own envelope through the postal system, complete with directions on how to reassemble the novel at the recipient's end.

Packets vary in length, although the "typical" packet length has been placed at 1-1.5 kilobytes. Most packets are divided into three parts: the header, the payload, and the trailer (or footer). If the substantive data is the packet's "payload," then -- to follow the missile metaphor -- the header serves as the navigational and targetting controls. The header contains the instructions for handling the data, including: + originating address, + length of the packet, + synchronization information, and + destination address. The header must provide the relevant information for the packet's proper place in the reassembly of the larger transmission; it may also have information on the protocol of the packet, i.e. email text, html webpage, flash file, etc. It also Just as there is no fixed length for a packet, there is no fixed length for the header within the packet.[126]

Literally speaking, packet inspection technology is definitional to the Internet – the content of a packet's header must be "inspected" for the packet and its data payload to be properly routed. Early "packet sniffing" technology have been free-standing programs to look at the header information *for purposes other than routing.* A spam filter that stops packets from particular sources is inspecting packets; [MORE ON SPAM FILTERS, FIREWALLS]. [127] These technologies are called "shallow packet inspection."

---

126 MORE ON HEADER SIZE -- Header information could range from 14 bytes (an Ethernet packet) to 44 bytes (a UDP/IP packet)

127 [CITE] [CITE] *See also* Rob Frieden, *Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers*, working paper at n. 29 ("New technologies will enable ISPs to operate non-neutral networks in the sense that ISPs will have the capability to examine traffic and assign particular streams to different tiers of service. Traffic examination of this sort does not examine the content, contained in the "payload" of packets. Accordingly an ISP would not know whether a particular bit stream contains obscene or defamatory content. However, examining packet "headers" would enable the ISP to determine what use, copying and retransmission rights

In contrast, "deep packet inspection" (DPI) looks at the payload of the packet. The technology is evolving in how *much* of the payload can be looked at and how much can be *learned* in real time. Notice I put "look" and "learn" in italics because we should remember that these are anthropomorphic attributions to our machines. Humans might look and learn at a latter report, but they cannot do these activities in "wire speed," i.e. internet transmission real time. Some characteristics of a packet can be detected easily by DPI – for example, a packet of ASCII content has a particular signature and is easily recognized;[128] JPEG and MPEG files are block-encoded, so one might "see" the block structure of the packets.[129] DPI can *often* learn sufficient information about the payload of a packet to match it against a database, such as whether to identify an email word ("Pentagon") or determine the application or format to which a packet belongs.

In our present technological range – that is, barring a paradign shift -- packets of compressed data are harder to analyze in wire time because a side-effect of compression is that each bit becomes more unpredictable.[130] Because mp3 is a compressed data format, its positive detection through DPI should be more difficult than, say, ASCII.[131] If the packet is part of an encrypted data stream, then analysis at the router may be effectively impossible, except, perhaps, to determine that the packet is encrypted. But just that determination could, for example, allow one to permit a stream of encrypted packets sufficient for a consumer to send a password or a vendor to send a bank account statement, while refusing any data stream long enough to be a feature film. Also determination that a payload is encrypted along with header

---

recipients have for the traffic managed by the ISP.") available at http://www.personal.psu.edu/rmf5/Net%20Neutrality%20and%20IPR.htm#_ftnref19

[128] Each ASCII character is 8 bits, which means that there could only be 256 8 bit combinations DPI needs to detect in order to "see" an ASCII packet. In fact, there are only 128 ASCII characters, of which 94 are printable – and therefore would tend to dominate payload content.

[129] My thanks to Michael Kass, Senior Scientist at Pixar, for this point.

[130] If a bit in a data stream is predictable in the sense that it fits into a larger pattern, then there is redundancy in the data stream, which means that a better compression method can make it shorter. In short, the better compressed data is, the more it looks like random noise.

[131] [MORE RESEARCH NEEDED ON DATA COMPRESSION RATE OF MP3 VERSUS, SAY, COMPRESSION RATE OF GZIP.]

information that the packet comes from a known source of unauthorized materials or illegal materials (such as child pornography) might be used as the basis to block the packet. Of course, this is all about detection of the packets constituting the *delivery*. Routers could become smart enough to detect the *requests* and then watch what is sent in reply, i.e. the router "sees" a file transfer request with ".mp3" in the name and waits for the reply.

What most distinguishes packet inspection (both shallow and deep) from the filters discussed above is not technology, but that the development and deployment of packet inspection technology is intimately related to evolving business modes for ISPs (and perhaps national security). There are a variety of *rational* business reasons for an ISP to want to discriminate among different sorts of packets; it is useful to parse these reasons to see which are objectionable – and which ones will simply be objected to.

Probably the least objectionable reason is that discrimination among different kinds of packets may be desirable when some applications are both "latency-sensitive" and seen as "premium services" -- such as voice over IP (VoIP),[132] interactive gaming, or video streaming.[133] For these sorts of applications, TCP/IP's vanilla-plain 'first come, first served' and 'best efforts' protocols will be inadequate in any environment

---

132 For technical background on how VoIP works *see* Intel, White Paper, *IP Telephony Basics*,available at: http://www.intel.com/network/csp/resources/white_papers/4070web.htm; Susan Spradley and Alan Stoddard, Tutorial on Technical Challenges Associated with the Evolution to VoIP, Power Point Presentation, available at: http://www.fcc.gov/oet/tutorial/9-22-03_voipfinal_ slides_only.ppt.

133 Cisco's explanation is useful: "Cisco® Service Control technology offers service providers the ability to classify application traffic and identify subscribers while prioritizing and optimizing network resources. Using stateful deep packet inspection, operators can optimize traffic on their networks, thereby increasing efficient use of network resources, reducing costs, and maximizing capital investment. State-of-the-art bandwidth management can be applied to network traffic on a global, subscriber, or individual flow-level hierarchy, helping ensure that operators can better manage network resource distribution." Cisco, Optimizing Application Traffic With Cisco Service Control Technology, available at http://www.cisco.com/en/US/prod/collateral/ps7045/ps6129/ps6133/ps6150/prod_brochure0900aecd80241955.html

where demand reaches (or nears) system capacity.[134] Second, packet discriminiation could allow an ISP to "tier" its services, charging large entities like eBay, Amazon, and Google for better access to ISP customers. For ISPs, this "two-sided" business model could make good sense; it is the same idea as cable television that charges consumers for access to channels ***and*** charges advertisers for access to customers. Obviously this prospect has meant that packet discrimination has come under a barrage of criticism from large internet companies who might be asked to pay for better access to consumers. But on that particular point, unless you have a lot of relevant stock options it is hard to be impassioned over whether Google or AT&T makes more profit.

Policy makers can be concerned about packet discrimination for more general reasons having to do with competition, technological development, free expression, and privacy. On possibility – related to the concerns of both Google and content providers – is that packet discrimination could allow the ISP to give the content of affiliates – "native" packets -- an advantage in speed and reliability of delivery to customers.[135] This raises genuine competition law concerns. Another meaningful

---

134 *See* Christopher Yoo, *Beyond Network Neutrality*, 19 HARV. J.L. & TECH. 1, 8 (2005). ("TCP/IP routes packets anonymously on a 'first come, first served' and 'best efforts' basis. Thus, it is poorly suited to applications that are less tolerant of variations in throughput rates, such as streaming media and VoIP, and is biased against network-based security features that protect e-commerce and ward off viruses and spam."); Edward W. Felten, *Nuts And Bolts Of Network Neutrality*, Practicing Law Institute, 24th Annual Institute on Telecommunications Policy & Regulation, 887 PLI/PAT 317, 326 (Dec. 2006) ("When you browse the Web, for example, you generate little or no traffic while you're reading a page, but there is a burst of traffic when your browser needs to fetch a new page from a server. If a network provider is using minimal delay discrimination, and the high-priority traffic is bursty, then low-priority traffic will usually sail through the network with little delay, but will experience noticeable delay whenever there is a burst of high-priority traffic. The technical term for this kind of on-again, off-again delay is 'jitter.'")

135 A criticism implicit in the comment of Marvin Ammori, general counsel of a party fighting Comcast on this issue: "Theyre blocking an innovative application that could be a competitor to cable TV." Associated Press, *Consumer groups ask FCC to fine Comcast, end data discrimination,* Siliconvalley.com, November 1, 2007, available at www.siliconvalley.com/news/ci_7340877?nclick_check=1. *See also* Stephen Lawson, *FCC Net Neutrality hearing Draws Diverse Views*, IDG News Service, April 17, 2008, available at www.pcworld.com/businesscenter/article/144791/fcc_net-neutrality_hearing_draws_diverse_views.html (Michele Combs of Christian Coalition of America expressing concern that Comcast would "block online programming from her organization in favor of its own Christian-oriented channel.")

concern is that any form of packet discrimination could be detrimental to new, as-yet-unknown applications and start-up companies.[136] Finally, critics can be concerned that packet inspection may compromise user privacy and/or may lead to content-based discriminations against some forms of communication.[137]

All of this has prompted a volte-face among a wide range of lobbyists and commentators who historically opposed government intervention in the internet and now urge new regulation to guarantee "network neutrality."[138] Beyond the debate on Capitol Hill and in the popular press, the academic legal literature on the broad topic of network neutrality is already extensive.[139] Our concern is much narrower: the prospect of transmission ISPs distinguishing among different kinds of transmissions inevitably reopens the issue of the proper role of ISPs in monitoring and blocking

---

Michael Geist, *The dangers of 'locking down' the Internet*, *supra* note __ . ("[T]he recent move toward a two-tiered Internet – one in which the ISPs themselves dream of distinguishing between different content as a new revenue source – revived the notion that ISPs could be called upon to play a more active role in monitoring and blocking content.")

136 [CITE TO TESTIMONY OF JUSTINE BATEMAN, SENATE COMMERCE COMMITTEE, APRIL 21, 2008]

137 [CITE TO TESTIMONY OF PATRIC VERRONE OF WRITERS GUILD, SENATE COMMERCE COMMITTEE, APRIL 21, 2008]

138 [EXAMPLE] [EXAMPLE] Larry Lessig recently described regulation mandating network neutrality as a "conservative" response in the sense that "[b]efore we allow [the internet] to change, the burden should be on those who would change its architecture" to justify the change. Stephen Lawson, *FCC Net Neutrality hearing Draws Diverse Views*, IDG News Service, April 17, 2008, available at www.pcworld.com/businesscenter/article/144791/fcc_net-neutrality_hearing_draws_diverse_views.html.

139 *See, e.g.* Christopher S. Yoo, *Would Mandating Broadband Network Neutrality Help or Hurt Competition? A Comment on the End-to-End Debate*, 3 J. ON TELECOMM. & HIGH TECH. L. 23 (2004); J. Gregory Sidak, *A Consumer-Welfare Approach to Network Neutrality Regulation of the Internet*, 2 J. COMP. L. & ECON. No. 3, 349 (2006); Christopher S. Yoo, *Network Neutrality and the Economics of Congestion*, 94 GEO. L.J. 1847 (2006); Thomas W. Hazlett, *Neutering the net*, FINANCIAL TIMES, FT.com Online, posted March 20, 2006; available at: http://news.ft.com/cms/s/392ad708-b837-11da-bfc5-0000779e2340.html; *See* Jeff Chester, *The End of the Internet?*, THE NATION (posted Feb. 1, 2006); available at: www.thenation.com/doc/20060213/chester; Tim Wu, *Why You Should Care About Network Neutrality, The Future of the Internet Depends on it!,* Slate (May 1, 2006); available at: http://www.slate.com/id/2140850/; Brett Frischmann & Barbara van Schewick, *Yoo's Frame and What It Ignores: Network Neutrality and the Economics of an Information Superhighway*, 47 JURIMETRICS J. (forthcoming 2007); Barbara van Schewick, *Towards an Economic Framework for Network Neutrality Regulation*, 5 J. ON TELECOMM. & HIGH TECH. L. (forthcoming 2007); *See, e.g.* Trevor R. Roycroft, *Economic Analysis and Network Neutrality: Separating Empirical Facts From Theoretical Fiction* (June 2006); available at: http://www.freepress.net/docs/roycroft_study.pdf.

copyright infringements. Indeed, the first full-fledged battle in the network neutrality debate has involved *de facto* copyright enforcement.

In 2007, Comcast, one of the largest providers of internet access in the U.S, was found to be slowing down BitTorrent packets.[140] While some of these BitTorrent packets may be authorized distributions of copyrighted materials, BitTorrent is typically used to distribute large audiovisual files without authorization. It quickly became apparent that slowing down BitTorrent packets seems to be a common practice among ISPs in several countries.[141] These revelations triggered both lawsuits[142] and hearings by regulators in both the US and Canada,[143] not to mention political jockeying by regulators and legislators with one another.[144]

---

[140] Peter Svensson, *Comcast actively hinders subscribers file-sharing traffic, AP testing shows*, Associated Press, 12:58 pm October 19, 2007; *Comcast Acknowledges Delaying Some Internet Traffic*, NBC10.com, 8:31 pm EDT October 23, 2007, available at www.nbc10.com/print/14408077/detail.html (In wake of Associated Press study showing slowing of BitTorrent packets, Comcast admits to "several network management technologies that . . . delay – not block – some peer-to-peer traffic.")

[141] Associated Press, Peter Svensson, *Study: Cox, Comcast Net subscribers blocked*, May 15, 2008 (describing German study that found "conclusive" signs of interference at Comcast, Cox, and Singapore ISP StarHub with "signs of interference" at seven other US ISPs), available at http://www.usatoday.com/tech/products/services/2008-05-15-cox-comcast-blocks_N.htm; Peter Nowak, *Cogeco ranks poorly in internet interference report*, CBC NEWS, April 22, 2008 (reporting that company that distributes works through BitTorrent found probable, intentional slowing of these packets by US ISPs Comcast, Bellsouth/AT&T, and Cablevision, as well as Canadian ISPs Cogeco, Rogers Communications, and TekSavvy Solutions among others), available at www.cbc.ca/technology/2008/04/22/tech-vuze.html; Naomi Hamilton, *Top broadband ISPs deny P2P shaping,* Computerworld (Australia), June 29, 2007 (reporting that smaller Australian ISPs admitted to controlling P2P traffic and Australian #2 ISP Optus admitted to such capacity and was opaque about actual practices), available at www.computerworld.com.au/articles/120945/top_broadband_isps_deny_p2p_shaping.html.

[142] Ryan Singel, *Comcast Sued Over BitTorrent Bloacking – UPDATED,* WIRED Blog Network, November 14, 2007 (suit filed in California state court), available at http://blog.wired.com/27bstroke6/2007/11/comcast-sued-ov.html; Complaint on file with author; Peter Nowak, *Bell sued for throttling internet speeds*, CBC News, June 2, 2008 (Quebec watchdog group L'Union des consommateurs files lawsuit in Quebec Superior Court that Bell Canada misrepresents its service because of undisclosed slowing of BitTorrent packets), available at http://www.cbc.ca/technology/story/2008/06/02/tech-quebec.html?ref=rss.

[143] [CITE] [CITE] Stephen Lawson, *FCC Net Neutrality hearing Draws Diverse Views*, IDG News Service, April 17, 2008, available at www.pcworld.com/businesscenter/article/144791/fcc_net-neutrality_hearing_draws_diverse_views.html. (describing FCC hearing at Stanford Law School on April 2008).

[144] Like the "broacast flag" debate, the network neutrality debate appeared to be one in which the FCC and some members of Congress competed for lobbyist attention. To the degree that

The widespread decision to slow BitTorrent and other P2P applications provoked a few rumblings of a conspiracy between ISPs and content owners, but the alignment of the two camps' interests seems coincidental. The problem ISPs are addressing is one of their own creation: by offering unlimited internet access for a flat monthly fee,[145] ISPs invite some people to use disproportionate amounts of network resources for (arguably) inefficient purposes. And as P2P applications have gained popularity, they have increasingly sucked up broadband capacity and strained the system.[146] Slowing P2P packets is, from the ISP's business perspective, a sensible way of "managing its network to keep file-sharing traffic from swallowing too much bandwidth and the affecting the Internet speeds of other subscribers."[147] And although there was considerable outcry from internet activists, there were also indications that subscribers who see the internet as a service, not a cause, support the idea of degrading service to extra heavy users in order to ensure normal speeds and accessibility to most customers.[148]

---

the FCC can itself handle the problem, that removes a hot issue – and lobbyists attention – from the Congressional plate. *See, e.g.* Associated Press, *FCC chief says new network neutrality laws not needed*, April 22, 2008, available at www.siliconvalley.com/news/ci_9011164_check=1.

145 Billing by the hour for dial-up connection time was common until AOL introduced its flat-rate, unlimited usage plan plan in 1996. Peter Svensson, *Time Warner Cable tries metering Internet use,* Associated Press, 5:37 pm June 2, 2008, available at http://www.usatoday.com/tech/products/2008-06-02-471239511_x.htm [hereinafter *Time Warner tries metering*];

146 *Id.* (Time Warner reporting that 5% of the company's subscribers take up half the capacity on its local cable lines and that other ISPs experience same problem),\; Michael Calore, Wired (August 30, 2007) ("ISPs say the looming growth of true peer-to-peer applications threatens to overwhelm them"); The Economist, Technology Quarterly (June 7, 2007) (p2P applications may overload current network infrastructure).

147 Peter Svensson, *Comcast actively hinders subscribers file-sharing traffic, AP testing shows*, Associated Press, 12:58 pm October 19, 2007.

148 Daniel Roth, *The Dark Lord of Broadband*, WIRED 54, ___, February 2009 (reporting that consumer focus groups favored clamping down on subscribers who overuse ISP resources so as to slow Internet to other subscribers). Or, as one Australian ISP manager noted in describing the slowing of P2P traffic, "[t]he heavy users of P2P are outraged that their (non time critical) data is treated as lower priority than your web browsing or video conferencing. And realistically, 97% of your customer base don't even notice. Everyone is happy, except the lechers, who were too happy anyway, at the expense of the ISP." Naomi Hamilton, *Top broadband ISPs deny P2P shaping, supra* note ___

There are several good reasons for the particular choice of the BitTorrent application for targeting. First, BitTorrent packets may be anywhere from 25% to half of *all* internet traffic.[149] Second, we can reasonably assume that the ISPs concluded that since *the vast* bulk of BitTorrent usage is the unauthorized distribution of films, BitTorrent users would have a weaker case to complain publicly – essentially complaining about the ISP interrupting their illegal behavior. But there seem to be two more important reasons for the choice of BitTorrent. First, there were widespread reports that BitTorrent by design seeks out faster connections whenever it is in use – meaning that when a large ISP adds capacity, particularly long transmission, the BitTorrent protocol will shift its usage to that ISP.[150] In the words of an executive at Rogers, one of Canada's larger ISPs, "[y]ou can't spend your way out of this problem. [P2P] has a behaviour that swamps all other behaviours."[151] Second -- and despite popular misconceptions -- identifying BitTorrent packets probably does *not* require ***deep*** packet inspection.[152] The particular characteristics of BitTorrent make it possible to identify these packets by *the traffic pattern* of the packets, not their content. Because the traffic flow is fundamental to the BitTorrent architecture, efforts to camouflage the BitTorrent packets against ISP detection seem to have had limited success.[153]

---

149 John Davidson, *Look Who's Stealing the Show*, THE FINANCIAL REVIEW, Jan. 14, 2006, at 17. (One of Australia's three largest ISPs estimated BitTorrent was "about half the traffic" on their network "and, by extension, the Australian internet.")

150 Nate Anderson, *Canadian regulators allow P2P throttling*, ARS TECHNICA, November 20, 2008 (Reporting Cisco Systems submission to Canadian authorities that "even if more bandwidth were added to the network, P2P file-sharing applications are designed to use up that bandwidth."), available at http://arstechnica.com/old/content/2008/11/canadian-regulators-allow-p2p-throttling.ars; Peter Nowak, *Rogers says its internet interference is necessary, but minimal*, CBC News, June 10, 2008 (explanation of Mike Lee, chief strategy officer of ISP Rogers, as to why "peer-to-peer traffic has been singled out") available at http://www.cbc.ca/technology/story/2008/06/10/tech-rogers.html.

151 *Id.*

152 *Id.* ("Applications such as BitTorrent are easy to detect because they are the only uses of the internet that reassemble files from a large number of different computers.")

153 WIKIPEDIA, *BitTorrent (protocol)* ("In general, although encryption can make it difficult to determine *what* is being shared, BitTorrent is vulnerable to traffic analysis. Thus even with MSE/PE, it may be possible for an ISP to recognize BitTorrent and also to determine that a system is no longer downloading, only uploading, information and terminate its connection by injecting TCP RST (reset flag) packets.") available at http://en.wikipedia.org/wiki/BitTorrent_(protocol) ; *See also* WIKIPEDIA, *BitTorrent protocol encryption* ("Encryption also won't stop a traffic shaping system configured to universally slow down all encrypted, unidentifiable or unknown protocols using a method as simple as packet loss."), available at

The complexity of the issue is revealed by the initial regulatory opinions we have seen. In the United States, the Federal Communications Commission determined, by a 3 to 2 vote, that Comcast's practice of impeding packets of some P2P applications was arbitrary and discriminatory.[154] The FCC found that Comcast's practices could adversely affect competitors to its own Video On Demand (VOD) product and that Comcast's particular practices where both under-inclusive and over-inclusive as to its claimed network management goals. In contrast, in November 2008, the Canadian Radio-television and Telecommunications Commission (CRTC) decided that Bell Canada can continue to throttle P2P traffic as necessary to manage its network.[155] The CRTC decision found that network congestion was indeed being caused by a limited group of P2P users. Their decision was technically limited to Bell Canada's activities in relation to its wholesale provision of ISP transmission services to its competitors in retail ISP services, but the CRTC decision implicitly accepted Bell Canada throttling P2P packets for its own retail customers.[156] One could reconcile these decisions based on some differences between the ISPs: unlike Comcast, Bell Canada only throttled BitTorrent packets during hours of higher general usage and was more forthright about what it was doing (once discovered).[157] But it should also be

---

http://en.wikipedia.org/wiki/BitTorrent_protocol_encryption#Remains_vulnerable_to_disrupted_peer_traffic

154 FEDERAL COMMUNICATIONS COMMISSION, *In the Matter of the Formal Complaint of Free Press and Public Knowledge Against Comcast*, FCC 08-183, August 20, 2008, available at http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf. *See also* John Dunbar, *FCC Rules Against Comcast*, Aug. 2, 2008, WASH. POST, *available at* http://www.washingtonpost.com/wpdyn/content/article/2008/08/01/AR2008080101205.html; *FCC Find Comcast's Practices of Slowing or Impeding Internet Peer-to-Peer Transfers Abritrary and Discriminatory in Violation of FCC Policy*, Bloomberg Law Reports, _____ at 18.

155 Canadian Radio-television and Telecommunication Commission, *The Canadian Association of Internet Providers' application regarding Bell Canada's traffic shaping of its wholesale Gateway Access Service,* Telecom Decision CRTC 2008-108, November 20, 2008, available at http://www.crtc.gc.ca/eng/archive/2008/dt2008-108.htm [hereinafter Telecom Decision CRTC 2008-108].

156 What is called the "Gateway Access Service," *Id.*

157 This is also what the Australian ISP Westnet said it was doing in 2007. Naomi Hamilton, *Top broadband ISPs deny P2P shaping, supra* note ___ ("The amount of bandwidth available to peer to

mentioned that the CRTC initiated a broader process to review traffic management and net neutrality issues that is continuing into 2009.[158]

Of course, another approach to the few ISP subscribers/P2P devotees who chew up inordinate amounts of bandwidth would be to charge each user for the true amount of bandwidth she is consuming – and some efforts at this are taking place.[159] The problem is that such a business model would likely expose ISPs to vicarious liability under copyright law. Vicarious liability arises "'"when the right and ability to supervise [the infringer] coalesce with an obvious and direct financial interest in the exploitation of copyrighted materials."'[160] ISPs already fulfill the first requirement for vicarious liability: that can *control* the activity at issue. Case law concerning both internet and meatspace businesses makes it likely that the only other requirement for vicarious liability – direct financial benefit -- can be fulfilled where the "where the availability of infringing material 'acts as a "draw for customers"'"[161] or where the ISP's "future revenue is directly dependent upon 'increases in user-base"'[162] driven by the availability of infringing material. If an ISP "meters" its usage and the amount of usage increases with the unauthorized downloading of copyrighted materials, that ISP makes itself a plump target for a vicarious liability claim. [163]

---

peer traffic is dynamically limited only when the bandwidth required to service the other applications exceeds expectations.")

158 Telecom Decision CRTC 2008-108, *supra* note __ at para. 80; Canadian Radio-television and Telecommunications Commission, *Review of internet traffic management practices of Internet service providers*, Telecom Public Notice CRTC 2008-19, November 20, 2008, available at http://www.crtc.gc.ca/eng/archive/2008/pt2008-19.htm.

159 Amy Schatz, Dionne Searcey, and Vishesh Kumar, *Officials Step Up Net-Neutrality Efforts*, WALL STREET JOURNAL, February 13, 2008 (describing Time-Warner experimenting with differential, capacity-usage pricing models); *Time Warner tries metering, supra* note ___.

160 Shapiro, Bernstein & Co. v. H. L. green Co., 316 F.2d 304, 307 (2d Cir. 1963).

161 A&M Records v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir 2001), quoting Fonovisa, 76 F.3d 259, 263-264 (9th Cir. 1996).

162 *Id.*

163 *See also* Marobie-Fl., Inc. v. National Ass'n of Fire Equip. Distribs, 983 F. Supp. 1167, 1179 (N.D. Ill. 1997) ("it is undisputed that NAFED paid Northwest a one-time set-up fee of $ 20 and that since that time NAFED has paid Northwest a flat fee of $ 67.50 each quarter. It is also undisputed that the fee Northwest receives has never changed based on how many people visit NAFED's Web Page or what is accessed. In other words, NAFED's infringement did not financially benefit Northwest. Accordingly, Northwest cannot be held vicariously liable for NAFED's infringement.")

In the debate about network neutrality, the copyright issue is a bit of a wild card. Copyright advocates recognize that such "traffic management technology, if widely used, would be a crippling blow to . . . file-sharing networks,"[164] but it is not politically wise for them to defend the transmission ISPs too loudly. On the other side, for Public Knowledge and the Electronic Frontier Foundation, advocacy against ISPs discrimination against P2P fits both "network neutrality" and their general struggle against internet copyright enforcement.[165] In contrast, companies like eBay and Amazon have an interest in separating copyright enforcement via traffic management and packet inspection from the more general network neutrality concerns that affect them. The recording and film industries have already stepped into the debate, forcing the different Congressional sponsors of network neutrality proposals to craft their proposals to protect only "lawful" traffic and to argue with colleagues whether and how network neutrality will hamper ISPs ability to fight copyright piracy.[166]

One of the most strident critiques of DPI characterizes DPI as the equivalent of postal inspectors opening and reading people's mail. This is both true and false – and understanding the two perspectives is important in recognizing how a legal

---

164 Svensson, *supra* note ____.

165 Consider the comment by EFF attorney Peter Eckersley implicitly connecting "innovative" new internet tools with college students' creation and use of P2P: "The bottom line is that if ISPs start regularly engaging in conduct like this, then kids in their dorm rooms or small startup companies that are trying to develop innovative new uses of the Internet are going to have to come and get permission from players like Comcast . . ." *Comcast Acknowledges Delaying Some Internet Traffic*, *supra* note ___.

166 Anne Broache, *RIAA: Don't let Net neutrality hurt piracy fight*, May 6, 2008, available at www.news.com/8301-10784_3-9937153-7.html (describing Congressman Markey saying "[t]his whole idea that this legislation helps piracy is 100 percent wrong," while Congresswoman Mary Bono Mack said :[i]t would be remiss for us as a body to interfere with these [anti-piracy] efforts. I think this bill would do that.") The bill, H.R. ____, only applies its network neutrality principles to the "ability of consumers to access, use, send, receive, or offer lawful content, applications, or services over broadband networks," prompting recognition from the head of the RIAA to conclude that the bill views "unlawful" content as unworthy of protection under the principles and that such an approach might pressure ISPs to "focus on the piracy problem." *Id.*
In May 2008, Congressman John Conyers. chairman of the House Judiciary Committee, also reintroduced net neutrality legislation which similarly prohibits networks from blocking, impairing, or discrimination against "lawful" content. [MORE] Anne Broache, *Democrats revive another Net neutrality proposal*, www.news.com, May 8, 2008.

concepts are ***not*** adequately dealing with the automation endemic to the internet. The packets are being "opened" for sure, but beyond that our metaphors and anthropomorphisms can quickly lead us astray. I believe that the packets can only be said to be "read" when people become aware of their contents or, at a minimum (and metaphorically), there is some (automated) impact on the sender or receiver from the monitoring done by the DPI, i.e. a packet is blocked. Richard Posner has made a similar point in regards to data mining:

> **The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy. But machine collection and processing of data cannot, as such, invade privacy. Because of their volume, the data are first sifted by computers . . . . This initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer.**[167]

While I do not agree with all that Posner concludes from this line of reasoning, it is valid point to say that the machine sifting of data – *by itself, with no other events* -- is not the same thing as a human being reading your communications. (Law academics cannot objectively say that it is the same thing because there ***is*** a chilling effect – because whether there is a chilling effect depends on people ***believing*** it is the same thing, the very beliefs that law professors are molding/trying to mold.) And this brings us to a theme of Part IV: that knowledge and other components of the DMCA – modelled on the behavior of sentient beings -- do not sensibly deal with how completely automated systems work.

To be understand this problem about how we characterize DPI, consider closed circuit video cameras (CCTV) that "watch" us, ubiquitously so in the UK and more and more in the US. Most people do not feel the pangs of concern about CCTV felt by staunch privacy advocates. Why? Perhaps because we just don't understand the danger. Or perhaps because we implicitly understand that the cameras are not really *watching* us; they are *recording* us and most of the data is destroyed before a human ever *sees* it. Of course, as data storage gets cheaper, the records will be kept longer, increasing the *probability* that something we did will be *seen* by a human. And gains in artificial intelligence will eventually allow CCTV systems to distinguish between a

---

[167] Richard A. Posner, *Our Domestic Intelligence Crisis,* Wash. Post, Dec. 21, 2005 at A31.

sidewalk lovers' quarrel and genuine spousal abuse – and the system will be able to trigger a response from the authorities. When a system can do that, it certainly seems like you were "seen." By the same token, if a DPI system recognizes your payload as email or VOIP chatter and ignores the packet, keeping no record of its passage, this is not the same thing as having your mail ***read*** by a human postal inspector who goes out to the local pub after work.

Consider a much closer parallel: the chip that is now inserted into much consumer computer and reprographic equipment that "detects and blocks attempts to view, scan or print copies of the redesigned $20 and $50 bills and, in a pop-up window, urges consumers to visit a Web site, www.rulesforuse.org, to learn about international counterfeit laws."[168] Imagine you are using a photocopier so equipped to scan a .pdf copy of this Article; in that situation the machine behaves completely normally. Do you feel your scanning was monitored, surveilled, or "read"?

Now let's say that you tried to scan and photocopy a new $50 bill and the machine refused and – on the little directions screen – urges you to visit the website above. Do you feel your scanning was monitored, surveilled, or "read"? If not, what's the difference between that and an automated system that detected an unauthorized feature film file transmission and blocked it? I agree that if your packet is stopped because the DPI system recognizes your payload as pornography or part of an unauthorized copy of an audiovisual work, it surely feels more like your packet was "read" than if it had passed through the system without triggering any reaction, *while it still is not the same thing as being "read" because there is still no human knowing about your activities.*

To see how folks in the technological moment of the DMCA (1998) did not envision transmission ISPs having awareness of packet contents, consider this question: has any transmission ISP engaged in deep packet inspection ***already*** lost the

---

168 Ted Bridis, Associated Press, *U.S. offers Internet downloads of new $50 bill.* Oct. 1, 2004, available at http://www.usatoday.com/tech/news/techinnovations/2004-10-01-50-bill-download_x.htm

protection of the § 512(a) safe harbor? While at least one telecommunications law scholar has concluded that ISPs may lose their 512 safe harbor because of the "knowledge" triggered by deep packet inspection,[169] I think the answer is no. There is no awareness or knowledge condition in section 512(a). Sections 512(c) and (d) condition the safe harbor for web hosts and "information location tools" on those types of ISPs having neither "actual knowledge" of infringement nor being "aware of facts or circumstances from which infringing activity is apparent." This was pretty clearly intended as a 'red flag' test.[170] But no such condition is present in the § 512(a) safe harbor – precisely because in 1998 there was no expectation that ISPs providing transmission facilities would "read" in real time the packets transiting their systems. Certainly everyone knew that ISPs providing transmission facilities could and did "sift" packets – that's how traffic is directed -- but there was no expectation that transmission ISPs could ever see "facts or circumstances from which infringing activity is apparent." If now an ISP implements a system that makes a human aware of packets "from which infringing activity is apparent" at something like wire speed, there is no loss of the 512(a) safe harbor.

To further consider where we were in 1998, conduct a thought experiment: an ISP which did the *opposite* of what Comcast has done. Consider an ISP that used DPI to determine which packets were P2P applications, and gave those packets priority over all others. Imagine the ISP did this long enough to become known among Internet users for having the fastest, most reliable connections for BitTorrent and

---

169 Frieden ("For ISPs actual knowledge can occur when an ISP engages in deep packet inspection.")

170 17 U.S.C. 512(c)(1)(A)(i) and (ii) for web hosting and 17 U.S.C. 512(d)(10(A) and (B) for information location tools. The Committee reports expressly interprets the 512(c) provisions as setting up a 'red flag' test: ""if the service provider becomes aware of a 'red flag' from which infringing activity is apparent, it will lose the limitation of liability if it takes no action. 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." United States House of Representatives, 105th Congress, 2d Sess., Committee on Commerce, Rpt. 105-551, Pt. 2, *Digital Millennium Copyright Act of 1998* (July 22, 1998); available at: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_reports&docid=f:hr551p2.105.pdf

other P2P protocols. Or perhaps the ISP offered pro-P2P packet discrimination as an enhanced, more expensive monthly subscription ($6.00 a month for the "P2P Pro" service). Surely this sort of discrimination *in favor* of the P2P packets would result in loss of the §512(a) safe harbor, wouldn't it? Of course, what we are asking is whether a §512(a) ISP can be liable under the common law standard for court-developed vicarious liability developed in copyright law. But, again, ***as a matter of the statute*** the vicarious liability standard appears in section 512 ***only*** in relation to web host and search engine ISPs.[171] It does not appear in the transmission safe harbor. It is not that Congress had a principled reason to think that vicarious liability standards *would* not apply to transmission ISPs; policymakers simply thought that vicarious liability standard *could* not apply to ISPs because of the non-discriminatory model of the internet as it was then understood.

[171] A web host ISP cannot "receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity." 17 U.S.C. § 512(c)(1)(B). The exact same wording appears in the information location tool safe harbor at 17 U.S.C. § 512(d)(2). The wording is absent from 512(a).

IV. NEW CURVE OF RESPONSIBILITY, IF NOT LIABILITY?

It might have been inevitable that the liability limitation regime(s) described in Part I would be subject to revisitation, either by judges creatively revising the system or by policymakers facing pressure from parties who come to understand more fully how the liability limitations disadvantage them.[172] It is also no surprise that technological developments and new, unforeseen business models might destabilize rules that had seemed "increasingly settled." Of course, just because the rules are being destabilized or are under pressure does not mean they will change. Perhaps, after a period of questioning, we will stay with the same norms. But for policy and law activitists who have also advocated that law change in response to technology, the fact that the present contours of ISP liability are the present contours cannot be a reason against change. In the words of one commentator, "the fact that we've done it this way for ten years is not a strong argument that it must always be done this way."[173]

This Part brings together the various ways in which pressure is being brought to bear on ISPs to take greater responsibility to stop copyright infringements on the Internet – but does not offer an over-arching solution or proposal. If forced to predict, I would anticipate that the financial liability of ISPs will remain largely unchanged, but we will have additional norms of ISP 'responsibility,' whether those norms are through patterns of conduct, industry agreements, limited governmental (regulatory) pressure, and/or court decisions. Most importantly, the responsibility regime is likely to move beyond the *fault-based* norms of a tort regime toward a simple *regulatory* structure predicated on the least-cost avoider either being the ISP *or including the participation of the ISP*. That becomes clearer in the discussion of "knowledge" versus automated processes in Part V. This Part begins with the ways that judges – outside the P2P case law – are imposing their own thinking about the proper role of ISPs in copyright enforcement; then xbxb.

---

172 Mann & Belzley, *supra* note __ at 243 (noting a "growing backlash of pressure, as parties, who perceive that those exceptions disadvantage them, seek the establishment of more rigorous regulatory regimes.")
173 Mark Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 109-110 (2007).

This emerging, yet undefined responsibility of ISPs can be thought of having two broad areas. The first is filtering/blocking/disablement – whether we are speaking of BitTorrent packets, hyperlinks, uploads to UGC sites, or repeat copyright infringers. The second area is data retention and disclosure, i.e. retention of information about users both as evidence of infringement and to identify/locate the alleged infringer. Data retention policies and requirements are a massively controversial issue where the privacy/national security dilemma will surely control the debate more than any copyright interests. The discussion here focuses on the filtering/blocking/disablement wing of ISP responsibility.

A. Stormy clouds and lightning - relitigating the issue in the courts

In light of these technological developments in filtering, it is important to remember that the statutory schemes to limit liability in Part I were focused on financial liability.[174] It is also important to see that little in the reasoning of the P2P cases in part II constrains their analysis to P2P software systems – not surprising, given the challenge even technologists would face in defining "peer to peer." Thus, many of the court decisions adverse to P2P developers were followed by grave prognostications about the chilling effects on technological development generally.

While we have yet to see a great chilling of technology triggered by the P2P court decisions – no grave "technological winter"[175] -- it is not surprising to see the basic tenets of those decisions start to influence attitudes on more mainstream ISPs, both in the courts and legislatures. Exemplary of this are the Ninth Circuit's 2007

---

174 This fits with the explanation that the lobbying concern of ISPs in "act I" was fear of financial exposure to private litigants more than fear of exposure to civil orders from central authorities.

175 Following the *MGM v Grokster* litigation there was a fair amount of hyperbolic rhetoric such as that the decision would cause "ten years of chilled innovation," *See* Robert Hof, *Ten Years of Chilled Innovation*, interview with Professor Lawrence Lessig, BUSINESSWEEK, June 29, 2005, at http://www.businessweek.com/technology/content/jun2005/tc20050629_2928_tc057.htm. *See also* Poster at SiliconValley.com ("Monday's Supreme Court decision in MGM v. Grokster may well be the beginning of technology's next long winter.")

decision in *Perfect 10 v. Amazon.com*[176] and, to a lesser degree, some of the language in a California district court opinion a year later, *Io Group, Inc. v. Veoh Networks, Inc.*[177] From these storm clouds of judicial language threatening ISPs, we will turn to the 2007 Belgian court decision, *SABAM v. S.A. Tiscali (Scarlet)*,[178] a bolt out of the blue on ISP responsibility for copyright infringement.

1. The *Perfect 10 v. Amazon.com* and *Io v. Veoh* cases

The Ninth Circuit's 2007 *Perfect 10 v. Amazon.com* decision was widely – and correctly -- viewed as a pro-ISP result; it is less commonly understood that the decision carries the seeds for imposing liability for copyright infringement on a wide variety of internet companies. The plaintiff, Perfect 10, is a provider of high-quality pornography and had found that many of its photographs of nude models being reproduced on third party sites without authorization. Just as mp3 technology had caused limited music infringement before P2P search technologies, the proliferation of these unauthorized images would probably be much more limited were it not for effective image search technologies. So Perfect 10 brought suit against Google and Amazon (which uses Google services) for the activities of "Google Image Search" (GIS).

Google Image Search (GIS) works like the Google's text search systems except in the interface it presents to users. When Google bots discover an image on an Internet website, GIS makes a small-scale (thumbnail) reproduction of the entire image and stores it on Google servers, indexing it pursuant to the text information attendant to the image – which is the actual basis of the user's search. When a user types, for example, "Spiders from Mars," the GIS transmits to and displays on the user's

176 487 F.3d 701; 2007 U.S. App. LEXIS 11420 (9th Cir. 2007)
177 586 F. Supp. 2d 1132; 2008 U.S. Dist. LEXIS 65915 (N.D. Cal. 2008)
178 All references to the case are to the English translation, SABAM v. S.A. Scarlet, District Court of Brussels, No. 04/8975/A, Decision of 29 June 2007, published in CAELJ Translation Series #001 (Mady, Bourrouilhou, & Hughes, trans.), 25 Cardozo Arts & Ent. L. J. 1279 (2008) [hereinafter SABAM v. S.A. Scarlett, CAELJ Translation Series #001]. The decision is on appeal, but no decision is anticipated before the end of 2009. (Communication with Alain Strowel, November 2, 2008). On October 22, 2008 the Court of First Instance issued an opinion, discussed below, in response to a post-decision petition by Tiscali.

computer a set of thumbnail images relevant to the David Bowie album, each with a hyperlink. Clicking on one thumbnail hyperlink – say www.davidbowietribute.com -- does **not** take the user immediately to the source page – as the Google text search engine would. Instead, the user would get a framed screen with a top third showing the Google-generated thumbnail of Bowie's band and the hyperlink, while the lower 2/3 of the screen showing the actual third party David Bowie tribute website.[179] The user has to click on the hyperlink again to get to the third party website without Google's presence on the user's screen.

Perfect 10 brought claims against [a] Google's creation, storage, and retransmission/display of the thumbnail versions of the Perfect 10 images and [b] Google's providing the framed hyperlink to the full-size image causing the full-size image to display on the user's computer (while a Google page displayed on the upper third of the screen). In the case of the framed hyperlinks, Perfect 10 made separate claims for direct infringement – arguing that Google *itself* displayed the full-size images – and contributory and vicarious liability for the infringement carried on by the third party websites.

The district court concluded that Perfect 10 was likely to prevail on its claim that the GIS creation, storage, and then transmission of the thumbnail images to users infringed the copyright in these images, particularly the right of public display.[180] While Google raised the same fair use arguments that had succeeded for the image search defendant in *Kelly v. Arriba*, there was one seemingly important difference. Because Perfect 10 provided evidence that there was a prospective market for thumbnail images of its models that it had begun to exploit that market (cell phones), the district judge concluded that the fourth fair use factor tipped the analysis in favor of the copyright holder.[181] (It is not clear why the court made these determinations vis-à-vis

---

179 487 F.3d at 711-712.

180 416 F. Supp. 2d at 844.

181 416 F. Supp. at 845-851. The district court also concluded that Google's use of the thumbnails was more commercial that Arriba's because of Google's very successful advertising sales, *Id.* at 849. All this made the district court conclude that the first factor tipped "slightly" toward Perfect 10.

the right of public display, since a market for downloadable thumbnails is a market that involves rights of reproduction and distribution, while we have never had a determination that the image on a cell phone is publicly displayed.)

Concerning the framed hyperlinks, the district court concluded that GIS activities did not constitute direct infringement of Perfect 10's distribution or display right for those images – on the grounds that GIS only provides a user's computer with the directions to retrieve an image from the internet, not the image itself,[182] commonly called the "server test" for distribution. The district court also concluded that Google was neither contributorily nor vicariously liable for infringement by third party websites – to which the GIS might direct Internet users.

The Court of Appeals embraced the district court's use of the "server test" for internet distribution of works and affirmed the conclusion that GIS neither directly distributes nor displays the full-size images hosted on third party websites. While affirming the district court conclusion on direct liability for the full-size images, the Court of Appeals disagreed with the district court's analysis on both direct liability for the thumbnail images and for contributory liability for the full-size images. As to the former, the Court of Appeals essentially reaffirmed – and strengthened -- its *Kelly v. Arriba* reasoning that a visual search engine's creation and distribution of thumbnail images is (or is likely to be) a fair use, despite a fact pattern suggesting displacement of a market that the copyright owner was attempting to exploit.[183]

While the court's fair use analysis in relation to the thumbnail images raises some interesting issues,[184] it is the court's discussion of contributory liability that merits

---

182 *Id.* at 844-845.

183 The Court of Appeals strengthened its Kelly holding by saying that the fourth factor has diminished importance when considering the activities of a search engine, but the panel avoided creating a more blanket ruling that thumbnails created by visual search engines are *per se* fair use by noting that "the district court did not make a finding that Google users have downloaded thumbnail images for cell phone use. This potential harm to Perfect 10's market remains hypothetical. We conclude that this factor favors neither party." 487 F.3d at 725.

184 The first issue is how a doctrine principally developed in a text-based copyright environment is to be applied to an image-based copyright environment. A small percentage of text in a work can serve the purposes of a critic, a news reporter, or a search engine user,

our attention here. First, neither the trial court nor the appellate court began their analysis with 17 U.S.C. §512, although Google is unquestionably a §512(d) information location service provider and the Ninth Circuit had already held that section 512 shields ISPs from both direct and secondary liability.[185]

Instead, the appellate panel began with a discussion of *Napster* and its holding that "if a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement."[186] After further discussing the standards of contributory liability in *Napster, Netcom*, and the Supreme Court's *Grokster* decision, the panel concluded "that a computer system operator can be held contributorily liable if it 'has *actual* knowledge that specific infringing material is available using the system' and 'can take simple measures to prevent further damage' to copyrighted works, yet continues to provide access to infringing works."[187] Disagreeing with the district court's analysis that "Google did not materially contribute to infringing conduct," the appellate panel concluded:

> **There is no dispute that Google substantially assists websites to distribute their infringing copies to a worldwide market and assists a worldwide audience of users to access infringing materials. We cannot discount the effect of such a service on copyright owners, even though Google's assistance is available to all websites, not just infringing ones. Applying our test, Google could be held contributorily liable if it had knowledge that infringing Perfect 10 images were available using its search engine, could take simple measures to prevent further damage to Perfect 10's copyrighted works, and failed to take such steps.**[188]

---

but a small percentage of a (still) visual work will rarely be as serviceable in parallel circumstances. The Ninth Circuit panel addresses this problem – as in the *Kelly v. Arriba* case – by recognizing that the amount taken is viewed relative to the use and that, then, still image search engines need to present entire images. This reasoning will not apply to something experienced linearly – across time – i.e. text, sound recordings, and moving images beyond a couple seconds. The second difficult issue coming out of Kelly and Perfect 10 is how to interpret "transformative." [MORE]

185 Napster, 239 F.3d at 1025.

186 487 F.3d at 728 quoting Napster, 239 F.3d at 1021. Of course, this immediately raises an interesting point – in Napster, the infringing materials was not "on" Napster's servers, although it would be fair to say it was "on" Napster's "system."

187 487 F.3d at 729.

188 *Id.*

The panel then concluded that the factual record from the district court was not inadequately developed on these issues and remanded the case.

Much can be made of this test announced by Judge Ikuta and her panelists. I will argue below that the most important and open-ended question is what "knowledge" means. This is because we are fast moving to a world where -- relative to its size, wealth, and technological capacities -- Google can take "simple measures . . .to prevent further damage to [the] copyrighted works." In a world where Google's subsidiary YouTube is deploying Google-developed filters to detect and remove tens of thousands of hours of moving images, how will Google be able to argue that filters to identify and remove a few thousand still images are not "simple measures"?

In this respect, the district court and Court of Appeals seems to have looked at things without current information about filtering technology OR with the wrong framework. The district court had found that "Google's software lacks the ability to analyze every image on the [I]nternet, compare each image to all the other copyrighted images that exist in the world . . . and determine whether a certain image on the web infringes someone's copyright."[189] The Court of Appeals held this finding was not clearly erroneous,[190] but that misunderstands the appropriate test.

Not that this Ninth Circuit panel is alone. For example, in 2007, Mark Lemley wrote that Google should not be asked to filter search results because "comparing everything on the Web to everything ever copyrighted in real time is computationally infeasible with existing or any foreseeable technology."[191] That the way many of us commonly (mis)conceptualized the problem,[192] but the issue is the technological

---

189 416 F. Supp. 2d at 858

190 This Court of Appeals discussion of the filtering technology occurs in the opinion's section on vicarious liability, but would appear to apply to the test announced for contributory liability as well. Indeed, the panel noted in the vicarious liability discussion that "Google's failure to change its operations to avoid assisting websites to distribute their infringing content may constitute contributory liability." 487 F.3d at 731.

191 Mark Lemley, *Rationalizing Internet Safe Harbors*, 6 J. TELECOMM. & HIGH TECH. L. 101, 110 (2007). *See also Id.* at 102 ("Even if it employed an army of lawyers to scrutinize all of the content, it would still be in no position to tell which pages were infringing or defamatory")

192 I made the same error – assuming that the relevant question concerns *all* copyrighted

capacity to detect quickly infringements of a *finite set of designated works in a designated database*. That's a much smaller problem computationally, one our technologies can increasingly handle. Google would not be asked to "compare each image to all the other copyrighted images that exist in the world," it would only be asked to compare each image *it wants to index* to the *copyrighted images that have been submitted to it by copyright owners* like Perfect 10. This is what the filters on YouTube are now being designed to do. There may still be problems of the database becoming too large – but small policy changes, not technology advances, can address those issues.

There are several important differences between the YouTube filtering and prospective GIS filtering situation. First, it is possible (probable) that GIS uploads far more material via the activity of Google spiders than YouTube users upload to YouTube – that would counsel against the filtering technology being a "simple measure." Second, still images require much less computational power for comparison than moving images – that would counsel in favor of the still image filtering technology being a simple measure. If the bottom line is that the limitation of Google's liability depends on it being "[w]ithout image-recognition technology," then the people in Mountain View are in an odd situation as they press forward technologically. *Perfect 10 v. Amazon.com* could be the springboard for effectively requiring ISPs to deploy serious filtering technology in a wide variety of situations.

In contrast, it was the use of (a kind of) image-recognition technology that helped Veoh secure summary on the validity of its Section 512(c) defense in the 2008 *Io Group v. Veoh Networks* litigation. Widely considered an early but imperfect test of the epic struggle between Viacom and YouTube which we will discuss below, *Io v. Veoh* concerned the unauthorized posting of pornographic video materials produced by Io on Veoh's UGC (user generated content) website. Io claimed that Veoh was ineligible for the 512 safe harbor because it had failed to adopt and reasonably implement a policy to terminate the accounts of repeat infringers as required by

---

works -- in a prior article. Justin Hughes, *The Internet and the Persistence of Law*, 44 BOSTON COLLEGE LAW REVIEW 359, 384, n. 81 (2003).

section 512(i) as a condition for the safe harbors.[193] Based on prior Ninth Circuit cases, the district dismissed this argument, holding that the many things Veoh did to try to keep infringers from using its service were more than "reasonable." In addition to having terminated over 1,000 users for repeat copyright violations,[194] Veoh established that it responded to most take down notices the same day it received them and when it identified a copyright infringement – either via a take-down notice or its own spot-checking – it used hash-based filtering "to terminate access to any other identical files and prevent additional identical files from ever being uploaded by any user."[195] In summarizing his analysis, Judge Lloyd wrote:

> **. . . the issue is whether Veoh takes appropriate steps to deal with copyright infringement that takes place. The record presented demonstrates that, far from encouraging copyright infringement, Veoh has a strong DMCA policy, takes active steps to limit incidents of infringement on its website and works diligently to keep unauthorized works off its website.**[196]

Of course, strictly speaking, the issue should have been straightforward compliance with section 512 requirement. Instead, for Judge Lloyd "[p]erhaps most importantly, there [wa]s no indication that Veoh has failed to police its system to the fullest extent permitted by its architecture."[197] In this sense, both *Perfect 10* and *Io v. Veoh* show courts reasoning more broadly about appropriate, technologically dependent standards for ISP conduct. [MORE]

2. The Belgian *Scarlet* decision

On June 29, 2007, a Belgian trial court surprised many in the international IP/IT community by ordering an ISP in that country to install filtering software to prevent the ISP's users from accessing unauthorized music downloads via peer-to-peer

---

193 586 F. Supp. 2d at 1143 (Io conceded that Veoh had adopted and informed subscribers of the termination policy, but "contend[ed] that there is a triable issue whether Veoh implements its repeat infringer policy in a reasonable manner.")

194 *Id.*

195 *Id.* (quoting a witness declaration) *Id* at 1154 ("Once content has been identified as infringing, Veoh's digital fingerprinting technology also prevents the same infringing content from ever being uploaded again.") To the degre

196 *Id.* at 1154.

197 *Id.* at 1153.

systems. In *SABAM v. S.A. Tiscali (Scarlet)*,[198] the court made this order following (a) an expert report on the feasibility of such filtering, and (b) express consideration of its power to order such relief in light of the EU Electronic Commerce Directive. Because it is the first, express consideration of these issues together the *Scarlet* decision is potentially influential and unquestionably controversial.

In June 2004, the Belgian Society of Authors, Composers, and Publishers (SABAM)[199] brought suit against then S.A. Tiscali, a medium-sized Belgian ISP, seeking injunctive relief pursuant to Article 87, section 1 of the Belgian Copyright Act of 2004. SABAM's principal request was for a court order that Tiscali stop user infringement of SABAM musical compositions "by making impossible or paralyzing all forms of sending or receipt by its clients of files containing musical compositions, transmitted without authorization of the copyright holder(s), using 'peer-to-peer' software, subject to a penalty of €25,000 per day or part of day during which S.A. Tiscali would not respect the order."[200] During the litigation, Tiscali changed its name to S.A. Scarlet Extended.[201]

While there may be much to debate about the *Scarlet* decision, the court's analysis covers many of the basic considerations in the P2P debates. In an interlocutory decision of November 26, 2004, the trial court concluded that copyright infringement of the SABAM musical repertoire was occurring on the Scarlet system and that the court was obligated "in principle, to order cessation of such activities."[202] With a standard that injunctive relief is only appropriate when it can "produce a result in the sense that it must effectively end the unlawful situation"[203] the court concluded that in 2004 it "was not sufficiently informed concerning the feasibility of technical

198 All references to the case are to the English translation, SABAM v. S.A. Scarlet, District Court of Brussels, No. 04/8975/A, Decision of 29 June 2007, published in CAELJ Translation Series #001 (Mady, Bourrouilhou, & Hughes, trans.), 25 Cardozo Arts & Ent. L. J. 1279 (2008) [hereinafter SABAM v. S.A. Scarlett, CAELJ Translation Series #001].
199 All sources indicate that SABAM is the "La Société Belge des Auteurs, Compositeurs et Editeurs" so it is unclear what each of the initials in « SABAM » represents.
200 SABAM v. S.A. Scarlett, CAELJ Translation Series #001, *supra* note ___ at 1282.
201 *Id.*
202 *Id.* at 1283.
203 *Id.* at 1285

measures that might be considered."[204]

On that basis, the court sought an expert opinion, which was delivered in January 2007. The expert identified eleven (11) "technically pertinent" solutions of which only seven were "applicable to Scarlett's network." Six of these were apparently technical solutions to block P2P applications entirely and only one – the filtering system offered commercially by Audible Magic – was identified by the expert as the "one that tries specifically to respond to the problem."[205] The expert's report was apparently pessimistic on whether the Audible Magic system could actually stop unauthorized transfers of music files across the ISP and SABAM felt compelled to introduced extensive evidence against the expert's conclusions.[206] In contrast to the expert's concern that Audible Magic's technology could not scale up to an ISP of Scarlett's size, SABAM introduced evidence of Audible Magic being used by MySpace, Microsoft, and "a leading Asian ISP."[207] The court also accepted evidence that over a three year amortization, the filtering system would cost the ISP roughly 50 centimes per month per customer.[208] The expert had expressed pessimism about the "enduring viability" of filtering solutions in the face of possible encryption – for the reasons described in Part ___ above; the court responded that "the issue of future potential encryption cannot be an obstacle to injunctive measures today."[209]

The court also addressed its grant of injunctive relief in the context of the E-Commerce Directive. Noting that one of the directive's "whereas" clauses presaged the deployment of "technical systems of protection and identification," the court reached the conclusion that the directive "does not actually affect the power of [a] judge granting injunctive relief and does not limit the measures that can be taken by

---

204 *Id* at 1283.
205 *Id.* at 1284 - 85.
206 *Id.* at 1284.
207 *Id.* at 1285-86. Scarlet did not contest SABAM's evidence on the technical capacity of Audible Magic. *Id.* at 1286.
208 *Id.*
209 *Id.* at 1286. SABAM also forced the expert to concede that he had not really examined the feasibility of encryption on P2P networks. *Id.*

him against [a] service provider."[210] A more interesting argument raised by Scarlet was that any injunctive relief requiring an ISP to filter internet traffic would violate Article 15 of the directive which provides that "Member states shall not impose a general obligation on providers . . . to monitor the information which they transmit."[211] The court concluded that Article 15, like the rest of that section of the directive, applies only to courts imposing financial liability on ISPs.[212]

The case is presently on appeal, but in the interim Scarlet filed a petition with the trial court to have the fine suspended, generally on grounds of impossibility and specifically on the grounds that Audible Magic withdrew from negotiations to install filters in the spring of 2008.[213] On the more general arguments, the court was opposed to "allowing the current hearing to be used in order to reargue the case before the court,"[214] while on the more specific issue of Audible Magic's withdrawal, the two sides argued about Scarlet's duties to pursue (simultaneously) alternative approaches and to what extent it actually had pursued discussions with alternative suppliers of a filtering system.[215] Reasoning that Audible Magic had withdrawn in April 2008 and that Scarlet could reasonably have needed six months to find an alternative solution, on October 22, 2008 the court of first instance revised its prior judgment, suspending the daily fine until November 1, 2008 and reimposing it thereafter.[216]

It is yet unclear how much influence the *Scarlet* decision will have with other EU jurisdictions. While the judges were only magisterial judges, the court's opinion gives – with the important exception of free expression considerations -- a thorough treatment to the key issues in such a fact pattern. British ISPs certainly reacted

---

210 *Id.* at 1288.
211 *Id.* at 1287.
212 *Id.* at 1288.
213 S.A. Scarlet Extended v. SABAM, District Court (Court of First Instance) of Brussels, No. 07/15472/A, Decision of 22 October 2008.
214 *Id.* at 8.
215 Scarlet argued "that it could not be required to work simultaneously on several solutions" *Id.* at 10, and that "SABAM acknowledges that one could not impose on the SA Scarlet an obligation to purchase simultaneously all of the potential solutions." *Id.* at 12. But the court also concluded that Scarlet had been in contact with other suppliers and identified "exploratory meetings" it had with a company called Imtech ICT. *Id.* at 9.
216 *Id.* at 13.

strongly to the decision, reasserting that ISPs should not "play judge and jury" in copyright infringement cases.[217] In February, 2008, a Danish court ordered a Danish ISP, Tele2 Denmark, to shut down access to the "Pirate Bay" file-sharing website.[218] But this decision simply seems to extend to P2P sites the reasoning of a 2006 Danish decision ordering an ISP to block the infamous Russian (non-P2P) site allofmp3.com, not a sudden embrace of the *Scarlet* court's reasoning. For their part, the motion picture industry has started a parallel litigation in Ireland, sensing that *Scarlet* could start a wave – or at least be a courtroom complement to legislative efforts in Europe forcing ISPs to become involved in copyright enforcement.

[Next sections excerpted – contact the author for more recent version]

217 David Meyer, *British ISPs stand firm after file-sharing ruling*, C/NET News.com, July 11, 2007, 9:50:18 PDT.
218 *Danish ISP shuts access to file-sharing Pirate Bay*, REUTERS, February 4, 2008.