Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 18 *Volume XVIII*
Number 3 *Volume XVIII Book 3*

Article 3

2008

Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers

Rob Frieden
Pennsylvania State University, rmf5@psu.edu

Internet Packet Sniffing and Its Impact on the Network Neutrality Debate and the Balance of Power Between Intellectual Property Creators and Consumers

Rob Frieden*

A PDF version of this article is available online at http://law.fordham.edu/publications/article.ihtml?pubID=200&id=2733. Visit http://www.iplj.net for access to the complete Journal archive.

* Pioneers Chair and Professor of Telecommunications and Law, Pennsylvania State University. Email address: rmf5@psu.edu.

INTRODUCTION

Developing information, communications and entertainment technologies have helped discrete markets to converge.[1] Previously stand alone markets for content and the conduit used to transmit content also have become fully integrated into a single medium thereby challenging the assumptions contained in "legacy" regulations and laws,[2] including the treatment of

[1] "Over the last two decades, the communications industry has undergone rapid technological advancements leading to the convergence of services. New technological capabilities allow companies to compete in markets which previously had no competition. While potentially beneficial to the consumer, convergence within the communications industry has created a regulatory nightmare." Ryan K. Mullady, *Regulatory Disparity: The Constitutional Implications of Communications Regulations That Prevent Competitive Neutrality*, 2 U. PITT. J. TECH. L. & POL'Y 1 (2007). For background on the impact of converging telecommunications and information processing technologies see, for example, INTERNATIONAL TELECOMMUNICATION UNION, ITU INTERNET REPORT 2006: DIGITAL.LIFE (Dec. 2006), http://www.itu.int/digitalife.

[2] Telecommunications regulation in the United States operates on a medium specific basis with separate rules and policies applicable to broadcasting, cable television, telecommunications services and information services. *See* Rob Frieden, *The FCC's Name Game: How Shifting Regulatory Classifications Affect Competition*, 19 BERKELEY TECH. L.J. 1275 (2004) [hereinafter Frieden, *The FCC's Name Game*]; Rob Frieden, *Adjusting the Horizontal and Vertical in Telecommunications Regulation: A Comparison*

intellectual property.[3] For example, the World Wide Web[4] seamlessly blends the telecommunications links needed to transmit information bits and packets[5] with the content carried over these links. However, separate laws and regulations apply to operators of neutral networks providing telecommunications services that deliver digital bits versus networks that actively combine telecommunications[6] with the bits that represent information[7] and

*of the Traditional and a New Layered Approac*h, 55 FED. COMM. L.J. 207 (2003) [hereinafter Frieden, *Adjusting the Horizontal and Vertical*].

[3] With the exception of the Digital Millennium Copyright Act ("DMCA") 17 U.S.C. §§ 1201–05 (1998), the most currently applicable intellectual property laws enacted by the United States Congress occurred prior to the onset of the Internet. *See* Copyright Act of 1976, Pub. L. No. 94-553, 90 Stat. 2541 (codified as amended 17 U.S.C. § 101 (2007)). For background on the history of copyright law, see Anuj Desai, *Big Entertainment Needs a Sequel to the Highly Anticipated Flop: MGM v. Grokster*, 41 GA. L.R. 579, 584–91 (2007). "At a basic level, the Internet's technology requires the insertion of intermediaries between interacting parties in two ways. First, for all interactions over the Internet, the communication necessarily involves the Internet itself, as well as the parties necessary to facilitate the particular communications . . . [and second] commercial transactions on the Internet require the use of other intermediaries." Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 254 (2005).

[4] "Perhaps the most significant development on the Internet was the World Wide Web, a user-friendly graphic user interface ("GUI") and effective means for computers running different operating systems to communicate with each other. The creator of the World Wide Web, Tim Berners-Lee, developed the Web to perpetuate a neutral network built on end-to-end principles. As neutral and therefore uncontrolled platforms, both the Internet generally and the Web specifically have spawned a dazzling rate and range of innovation." Bill D. Herman, *Opening Bottlenecks: On Behalf of Mandated Network Neutrality*, 59 FED. COMM. L.J. 103, 109–10 (2006); *see also* TIM BERNERS-LEE & MARK FISCHETTI, WEAVING THE WEB: THE ORIGINAL DESIGN AND ULTIMATE DESTINY OF THE WORLD WIDE WEB BY ITS INVENTOR (1999).

[5] "[T]he Internet is a 'packet-switched' network. In such networks, fixed circuits are not dedicated for the duration of a communication. Instead, the data that is transmitted, whether files, email, Instant Messages, voice, is broken into small packets. Each packet travels its own route over the Internet. The entire set of contents is reassembled when it is received at the other end." Susan Landau, *National Security on the Line*, 4 J. TELECOMM. & HIGH TECH. L. 409, 424 (2006).

[6] Telecommunications is defined as "the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received." 47 U.S.C. § 153(43) (1997). Telecommunications service means "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used." *Id.* § 153(46). The Communications Act defines telecommunications carrier as "any provider of telecommunications services, except that such term does not include aggregators of telecommunications services (as defined in §

entertainment content. Similarly Internet Service Providers ("ISPs") qualify for a status that exempts them from liability for carrying tortious or harmful content, in light of the actual or perceived burden content scrutiny would impose.[8]

ISPs now can accrue financial and efficiency gains by engaging in vertical integration of the production, editing, and delivery of content.[9] Similarly ISPs have upgraded, or soon will upgrade, their networks with hardware and software that enables them to acquire knowledge about what kinds of content they

226). A telecommunications carrier shall be treated as a common carrier under this Act only to the extent that it is engaged in providing telecommunications services, except that the Commission shall determine whether the provision of fixed and mobile satellite service shall be treated as common carriage." *Id.* § 153(44).

[7] Information service is defined as "the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service." *Id.* § 153(20). "[T]he language and legislative history of [the Communications Act of 1996] indicate that the drafters . . . regarded telecommunications services and information services as mutually exclusive categories." In the Matter of Federal-State Joint Board on Universal Service, Report to Congress, 13 F.C.C.R. 11501, 11522–23 (1998). While information service providers use telecommunications to transmit bitstreams, the FCC has chosen not to separate this functionality from the information processing that also occurs. In other words, the FCC considers telecommunications to be subordinate to, and fully integrated with, the predominant information service. *See* Vonage Holdings Corp. v. Minn. Pub. Utils. Comm'n, 290 F. Supp. 2d 993, 1000–01 (D. Minn. 2003) (applying the FCC's dichotomy).

[8] Section 509(c)(1) of the Communications Decency Act, (codified at 47 U.S.C. § 230(c)(1) (1998)), states 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."

[9] "Vertical integration enables a firm to coordinate investment and production decisions across its divisions. A comparison of the costs of contractual exchange with those of internal exchange often reveals vertical integration to be the least-cost method of achieving the desired level of coordination. The minimization of coordination costs is extremely important in a market subject to rapid technical change." J. Gregory Sidak, *A Consumer-Welfare Approach to Network Neutrality Regulation of the Internet*, 2 J. COMPETITION L. & ECON. 349, 460 (2006). "Relative to contracting at arm's length for network management and for delivery of Internet content and applications, vertical integration reduces these costs of specifying, monitoring, and enforcing the rules that direct activities required for the coordinated production of services to end users." *Id.* at 461; *See also* Joseph Farrell & Philip J. Weiser, *Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age*, 17 HARV. J.L. & TECH. 85, 97–100 (2003).

switch, route and transmit.[10] Such active traffic management can disqualify ISPs[11] from safe harbor[12] copyright liability exemptions for infringement occurring as a result of their carriage of content.[13] The decision to engage in active management of content results not from an affirmative obligation to do so, but instead the desire to tap new business opportunities accruing from the ability to scrutinize bitstreams. Such scrutiny can facilitate the prioritization of traffic into tiers corresponding to different quality of service commitments. It also can provide notification to ISPs with

[10] "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 Systems, Optimizing Application Traffic with Cisco Service Control Technology, Solution Overview, http://www.cisco.com/en/US/products/ps6150/prod_brochure0900aecd80241955.html (last visited Nov. 29, 2007).

[11] The DMCA applies to "service providers" defined in § 512(k)(1)(A) and applicable to provisions of transitory communications services as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." 17 U.S.C § 512. For three other safe harbor exemptions from liability for copyright infringement "service provider" is more broadly defined in § 512(k)(l)(B) as "a provider of online services or network access, or the operator of facilities therefor." *Id.*

[12] A safe harbor constitutes "[a]n area or means of protection [or a] provision (as in a statute or regulation) that affords protection from liability or penalty." BLACK'S LAW DICTIONARY 1363 (8th ed. 2004). The DMCA provides qualified immunity from liability for direct or secondary infringement of copyrighted material that traverses an ISP's network. *See* 17 U.S.C § 512. "Congress enacted the safe harbors in response to concerns expressed by online service providers about their potentially overwhelming liability for copyright infringement committed by their users." Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV., 1345, 1369 (2004).

[13] Title II of the DMCA added § 512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. *See* 17 U.S.C. § 512 (1999). The limitations are based on the following four categories of conduct by a service provider: 1) Transitory communications 2) System caching; 3) Storage of information on systems or networks at direction of users; and 4) Information location tools. *See id.* § 512(a)–(d). ISPs lose safe harbor liability exemption when they have actual knowledge of copyright infringement. *See, e.g.*, *id.* § 512(c)(1)(A). Each limitation completely bars monetary damages, and restricts the availability of injunctive relief. *See, e.g.*, *id.* § 512(a).

instructions that make Digital Rights Management ("DRM")[14] more effective. Instead of relying on piracy protection embedded in files already delivered by an ISP to recipients' computers, active scrutiny of traffic possibly can preempt the transmission of pirated files in the first place in much the same way as an ISP might block and refuse to deliver unauthorized, harmful and bandwidth hogging traffic such as spam and computer viruses.

Provided ISPs do not induce copyright infringement, while feigning no knowledge, case law prior to[15] and after enactment of the Digital Millennium Copyright Act ("DMCA")[16] has exempted ISPs that operate as neutral conduits. Courts also have exempted ISPs and other intermediaries[17] for the unknowing carriage of

[14] Digital Rights Management ("DRM") refers to the use of technological tools by copyright owners and distributors to regulate the uses of their works, and in particular to restrict reproduction. For background on the types of current DRM technologies used to guard against music piracy, see Nika Aldrich, *An Exploration of Rights Management Technologies Used in the Music Industry*, 2007 B.C. INTELL. PROP. & TECH. F. 051001 (2007), http://bciptf.org/index.php?option=com_content&task=view&id=30&Itemid=30.

[15] *See, e.g.*, Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., 907 F. Supp. 1361, 1381 (N.D. Cal. 1995) (holding online operator of system for posting comments to multiple recipients was not liable for direct and vicarious infringement when a subscriber directly infringed copyrights by posting large portions of copyrighted content).

[16] *See supra* note 13. ISPs that financially benefit from infringement, about which they know or should know, and can prevent the infringement using affordable means, may lose the DMCA safe harbor. MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005); In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir. 2003), *cert. denied*, 540 U.S. 1107 (2004). The *Grokster* case does not impose an affirmative obligation on ISPs to seek out and install the most effective technology to prevent intellectual property piracy. "[T]his evidence of unlawful objective is given added significance by MGM's showing that neither company attempted to develop filtering tools or other mechanisms to diminish the infringing activity using their software. While the Ninth Circuit treated the defendants' failure to develop such tools as irrelevant because they lacked an independent duty to monitor their users' activity, we think this evidence underscores Grokster's and StreamCast's intentional facilitation of their users' infringement." 545 U.S. at 939. However at some point the deliberate refusal to acknowledge blatant piracy and to do something about it, if technologically and financially feasible, may support the inference that an ISP actually induces the infringement. ISPs now have both inexpensive technological resources and the commercial motivation to manage traffic. *See* Center for Democracy and Technology, *Interpreting Grokster: Limits on the Scope of Secondary Liability for Copyright Infringement*, STAN. TECH. L. REV. 3 (2006), http://stlr.stanford.edu/pdf/CDT-grokster.pdf (last visited Nov. 28, 2007).

[17] *See, e.g.*, Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1086 (C.D. Cal. 2004) (DMCA insulates payment intermediaries from claims of copyright infringement);

defamatory[18] or obscene[19] content. Conversely, ISPs that actively manage traffic have recognized the benefit in attempting to restrain the scope of their traffic management activities to a level below that which would inform them about illegal content.[20] Such safe harbors absolve ISPs of having to invest the time, money and effort needed to examine all content. However, new revenue-generating opportunities have become available to ISPs that use equipment and software to examine bitstreams so that ISPs can offer different quality of service levels and otherwise differentiate the treatment of traffic.[21]

Gentry v. eBay, Inc., 121 Cal. Rptr. 2d 703, 706 (Cal. App. 2002) (online auction site not liable for sale of counterfeit goods).

[18] *See, e.g.*, Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 141 (S.D.N.Y. 1991) (holding ISP that operates as a neutral conduit for over 150 special interest forums was not a publisher for content created by others with management, editing and other control functions performed by a third party); Lunney v. Prodigy Servs. Co., 250 A.D.2d 230, 238 (N.Y. App. Div. 1998), *aff'd*, 723 N.E.2d 539 (N.Y. 1999) (ISP not responsible when defamatory comments posted by an imposter); Blumenthal v. Drudge, 992 F. Supp. 44, 52 (D.D.C. 1998) (holding ISP not liable for defamatory statement posted even when the ISP pays a monthly fee for the content and has the contract right to control it editorially). Section 230(c)(1) of the Communications Act, as amended, 47 U.S.C. § 230(c)(1) (2006), specifies 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." *See, e.g.*, Ben Ezra, Weinstein, & Co. v. Am. Online, Inc., 206 F.3d 980, 983 (10th Cir. 2000) (interpreting § 230 as granting immunity for distribution of inaccurate stock prices concerning the plaintiff's business); Zeran v. Am. Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997) (finding that § 230 conferred immunity on America Online even though, after several notifications, it did not quickly remove postings falsely portraying Zeran as celebrating the Oklahoma City bombings); Barrett v. Rosenthal, 146 P.3d 510, 513 (Cal. 2006) (finding that § 230 creates immunity for a defendant who republishes defamatory speech regardless whether the ISP acted as more than a completely passive conduit); Doe v. Am. Online, Inc., 783 So. 2d 1010, 1017 (Fla. 2001) (affirming on § 230 immunity grounds the dismissal of a mother's complaint alleging tort liability against AOL for retransmitting sexually explicit photographs and a videotape).

[19] *See* Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 611 (E.D. Pa. 2004) (invalidating law requiring ISPs to disable access to child pornography sites as overbroad and ineffective).

[20] "The source ISP, in contrast, may be involved in multiple ways that are relevant both in assessing the 'fairness' of 'blaming' the source ISP for the misconduct . . . and in assessing how effectively the source ISP can serve as a gatekeeper to stop the misconduct . . . ." Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 256 (2005).

[21] 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

The ventures that manufacture equipment used to switch, route and transmit Internet traffic and the carriers providing these services have a keen interest in shaping a new generation of Internet services that deviates from a "one size fits all," least common denominator.[22] By offering customized and diversified features, ISPs can create new profit centers while more closely catering to the specific needs of end users and content creators. Opponents to these initiatives consider them unreasonable price and quality of service discrimination based on the view that "network neutrality"[23] should provide a level competitive playing field for all services carried over the World Wide Web. Network neutrality opponents claim that limits on service diversification would create disincentives for much-needed infrastructure investment as well as foreclose opportunities to customize Internet

in the "payload" of packets. Accordingly an ISP would not know whether a particular bitstream contains obscene or defamatory content. However, examining packet "headers" would enable the ISP to determine what use, copying and retransmission rights recipients have for the traffic managed by the ISP. *See* Alex Pisarevsky, Note, *Cope-ing with the Future: An Examination of the Potential Copyright Liability of Non-Neutral Networks for Infringing Internet Content*, 24 CARDOZO ARTS & ENT. L.J. 1359 (2007).

[22] "It comes down to this: the industry needs to put forth meaningful ways to identify, promote and commercialize digital assets while protecting copyright holders. If it doesn't, all stakeholders will miss out on the opportunity to generate revenue from IP-based entertainment distribution." Dr. Matthew Lucas, *Peer-To-Peer Networks, DRM and OSS/BSS*, BILLING & OSS WORLD, Mar. 5, 2007, http://www.billingworld.com/articles/feature/Peer-to-Peer-Networks-DRM-and-OSS-BSS.html.

[23] "In light of the financial stakes involved in the scope of regulation applied to conventional, so-called legacy services and new information services, numerous organizations have pursued a public policy agenda supporting deregulation and the eradication of government oversight, including traditional regulatory over pricing, interconnection and quality of service. These groups reject any view that even as telecommunications becomes less regulated, a new concept of 'network neutrality' should force largely unregulated Internet Service Providers ("ISPs") to forego the option of offering differentiated and tiered Internet services. Opponents of net neutrality view the concept as jeopardizing operational and pricing flexibility. Net neutrality advocates fervently argue that the Internet cannot achieve maximum contributions to national productivity, economic opportunity and innovation unless government ensures end-to-end connectivity by foreclosing a balkanized or tiered Internet." Rob Frieden, *Network Neutrality or Bias?—Handicapping the Odds for a Tiered and Branded Internet*, 29 HASTINGS COMM. & ENT. L.J. 171, 174–76 (2007) [hereinafter Frieden, *Network Neutrality or Bias?*].

services, including the offer of "better than best efforts" routing[24] for content providers keen on securing more reliable services than that available from the current, "best efforts"[25] delivery standard.

Network neutrality opponents recognize that technological innovations and diversifying Internet user requirements can create new or more robust revenue streams. The ability to scan Internet traffic, through instantaneous examination of bitstreams, makes it possible for ISPs to offer premium services to both end users and content providers. Some consumers may willingly pay a premium for faster, better, and smarter access to content. Candidates for premium service include users of gaming software, peer-to-peer file sharing[26] and Internet-mediated telephone calls, commonly referred to as Voice over the Internet Protocol ("VoIP").[27]

---

[24] *See, e.g.*, T. Randolph Beard, George S. Ford, Thomas M. Koutsky & Lawrence J. Spiwak, *Network Neutrality and Industry Structure*, 29 HASTINGS COMM. & ENT. L.J. 149 (2007); Christopher S. Yoo, *Network Neutrality and the Economics of Congestion*, 94 GEO. L.J. 1847 (2006) [hereinafter Yoo, *Network Neutrality*]; Christopher S. Yoo, *Beyond Network Neutrality*, 19 HARV. J.L. & TECH. 1, 13–18 (2005) [hereinafter Yoo, *Beyond Network Neutrality*]; Christopher S. Yoo, *Would Mandating Broadband Network Neutrality Help or Hurt Competition? A Comment on the End-to-End Debate*, 3 J. TELECOMM. & HIGH TECH. L. 23, 51 (2004) [hereinafter Yoo, *Would Mandating Broadband Help or Hurt Competition?*].

[25] "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." Yoo, *Beyond Network Neutrality*, *supra* note 24, at 8.

[26] "Emerging peer-to-peer networks destabilized the equilibrium achieved under the DMCA between copyright owners and ISPs. Peer-to-peer networks facilitate direct exchange of files among individual users. While infringing materials distributed on the web involve identifiable websites, the distribution of infringing materials on peer-to-peer networks is difficult to control. Data is replicated by multiple peers and can be located by peers without relying on a central index server. The distributed architecture of peer-to-peer networks makes it difficult to identify the source of infringing materials and to locate the infringers." Niva Elkin-Koren, *Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 15, 17 (2005–06).

[27] Voice over the Internet Protocol ("VoIP") offers voice communications capabilities, much like ordinary telephone service, using the packet switched Internet, for all or part of the link between call originator and call recipient. VoIP calls originating or terminating over the standard dial-up telephone network require conversion from or to the standard telephone network's architecture that creates a dedicated "circuit-switched" link, as opposed to the ad hoc, "best efforts" packet switching used in the Internet. *See* Robert Cannon, *State Regulatory Approaches to VoIP: Policy, Implementation, and Outcome*, 57

Similarly, some content and service providers may willingly pay for enhancements that provide more protection and privacy and greater reliability that traffic will arrive in a timely manner to a large, possibly temporary audience of prospective customers.

Candidates for a premium service typically have higher bandwidth requirements, less tolerance for dropped, lost or delayed packet delivery and generate more traffic volume than typical users. To accommodate these requirements manufacturers have developed equipment that can examine and prioritize Internet traffic at an increasingly granular level. While ISPs previously lacked both the technological wherewithal and the incentive to deviate from plain vanilla best efforts,[28] they now have the capacity to inspect traffic on a packet-by-packet basis. The ability to "sniff" packets makes it possible for ISPs to deviate from "best efforts" routing by discriminating on the basis of price paid for service and as a function of what kind of traffic a bitstream represents. Deep packet inspection[29] makes it possible for ISPs to

FED. COMM. L.J. 479, 484 (2005); Mark C. Del Bianco, *Voices Past: The Present and Future of VoIP Regulation*, 14 COMMLAW CONSPECTUS 365, 368 (2006); Robert M. Frieden, *Dialing for Dollars: Should the FCC Regulate Internet Telephony?*, 23 RUTGERS COMPUTER & TECH. L.J. 47 (1997) [hereinafter Frieden, *Dialing for Dollars*]; Chérie R. Kiser & Angela F. Collins, *Regulation on the Horizon: Are Regulators Poised to Address the Status of IP Telephony?*, 11 COMMLAW CONSPECTUS 19, 21 (2003); Sunny Lu, Note, *Cellco Partnership v. FCC & Vonage Holdings Corp. v. Minnesota Public Utilities Commission*: *VoIP's Shifting Legal and Political Landscape*, 20 BERKELEY TECH. L.J. 859, 861 (2005).

[28] Prior to 1995 the United States government largely underwrote development of the Internet by funding two major backbone networks, the ARAPANET and NSFNet and by serving as an anchor tenant user of these networks. "The 'Internet' is a worldwide system of computer networks and individual computers that are interconnected by communications facilities. The antecedents of the Internet were systems for two relatively small groups of research-oriented governmental, academic and corporate entities—ARPANET and NSFNET. ARPANET received its principal support from the Department of Defense and related agencies, while NSFNET's support came from numerous sources, including the NSF and other federal agencies, academic institutions, and corporate sponsors." Island Online, Inc. v. Network Solutions, Inc., 119 F. Supp. 2d 289, 292 (E.D.N.Y. 2000) (references omitted). Network operators funded by the United States government and keen on promoting greater accessibility to the Internet and connectivity of networks had little interest in measuring traffic levels and charging network operators that generated more traffic than they received.

[29] "Deep packet inspection uses specialized high-speed hardware and software that can identify packets in real-time. A service provider could use deep packet inspection to distinguish peer-to-peer traffic or even just traffic from a single peer-to-peer file-sharing

diversify service on the basis of allocated bandwidth, routing priority and performance guarantees. It also may prevent an ISP from turning a blind eye to "red flags" generated by the process of deep packet inspection evidencing obvious infringement even before a copyright holder notifies the ISPs of the infraction.[30] Likewise, Digital Rights Management[31] functions integrated into

application and either block it or reduce its available bandwidth. Without deep packet inspection, service providers and others could only resort to crude application-level techniques, such as cutting off all streaming video clips using standard formats after a certain time." Kevin Werbach, *Breaking the Ice: Rethinking Telecommunications Law for the Digital Age*, 4 J. TELECOMM. & HIGH TECH. L. 59, 92 (2005). "Depending on how net neutrality is defined, it can be argued that there are widespread violations of the principle. Vertically integrated incumbents are expanding their tactics from the shotgun approach of blocking to a more nuanced approach. In the United States particularly, incumbents are looking to increase their broadband revenue streams not by blocking, but by discrimination, charging more for faster download speeds or for certain types of traffic sent by unaffiliated parties. This approach is greatly facilitated by new filtering and 'deep packet inspection' network-management tools that allow service providers to determine the types of traffic flowing across their networks. With these tools, network operators can offer improved speeds—and, conversely, to block or degrade the service—for specific types of traffic." Del Bianco, *supra* note 27, at 394–95.

[30] The Committee Report on the DMCA, 17 U.S.C. § 512 (2006), provides more expansive insights on the meaning of the language contained in the law. While the DMCA does not expressly contain a "red flag" test for assessing whether an ISP has actual knowledge of copyright infringement, the Committee Report suggests the reasonableness of such a test when evaluating the appropriateness of safe harbors for ISPs storing and linking to copyright infringing content. 17 U.S.C. § 512(c)–(d). For example, the Committee Report suggests that § 512 (c)(1)(A)(ii) establishes such 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." H.R. REP. NO. 105-551, pt. 2, at 53 (1998) [hereinafter DMCA Committee Report]. Addressing linkage to sites probably containing infringing material the DMCA Committee Report suggests the reasonableness of a similar red flag test: "a service provider would have no obligation to seek out copyright infringement, but it would not qualify for the safe harbor if it had turned a blind eye to 'red flags' of obvious infringement." *Id*. at 57.

[31] Copyright holders increasingly rely on digital rights management "technologies that prevent you from using a copyrighted digital work beyond the degree to which the copyright owner wishes to allow you to use it." MIKE GODWIN, WHAT EVERY CITIZEN SHOULD KNOW ABOUT DRM, A.K.A. "DIGITAL RIGHTS MANAGEMENT," 1 (2004),

deep packet inspection may become a standard technical component that ISPs can avoid only at the risk of losing the DMCA safe harbors.[32]

An ISP able to examine packets for purposes of assigning bitstreams into various tiers of service also provides an ISP with greater knowledge about the nature and type of the traffic it handles.[33] Arguably, an ISP engaging in quality of service ("QOS") and price discrimination through deep packet inspection no longer operates as a neutral conduit lacking actual or constructive knowledge of what the packets represent. ISPs that sniff packets actively examine the header of packets that provide traffic routing information, but also can identify characteristics of the content "payload" contained in the packet. For example, the packet header can identify the payload as a portion of a music file and can specify the intellectual property rights retained by the owner of the content as well as the usage and copying opportunities available to the recipient.

http://www.publicknowledge.org/pdf/citizens_guide_to_drm.pdf; *see also* Dan L. Burk, *Legal and Technical Standards in Digital Rights Management Technology*, 74 FORDHAM L. REV. 537, 538 (2005).

[32] 17 U.S.C. § 512(i)(1)(B) (2002) conditions ISP safe harbor eligibility on their accommodation and noninterference with "standard technical measures" to identify and protect copyright infringement. 17 U.S.C. § 512(i)(2)(A)–(C) defines these measures as ones that "have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process; are available to any person on reasonable and nondiscriminatory terms; and do not impose substantial costs on service providers or substantial burdens on their systems or networks."

[33] In addition to packet switching, equipment manufacturers and ISPs have a keen interest in new traffic switching, routing and transmitting architectures that provide greater flexibility in tiering and managing traffic. One promising design, IP Multimedia Subsystem ("IMS"), offers both wireline and wireless carriers greater control over the quality of service in setting up and managing telephone calls and data sessions. This management enhancement extends to the software and service applications that ride on a bitstream transmission path. For background on IMS, see Light Reading, IMS Guide (Mar. 24, 2005), http://www.lightreading.com/document.asp?doc_id=70728 (last visited Nov. 26, 2007); Nortel, IP Multimedia Subsystem (IMS) Solution, http://www2.nortel.com/go/solution_content.jsp?segId=0&catId=0&parId=0&prod_id=52540 (last visited Nov. 26, 2007).

The output of affordable deep packet inspection and other technologies[34] now available to ISPs raises questions whether non-neutral network operation disqualifies ISPs for a safe harbor exemption from liability for carrying copyright infringing traffic provided by § 512 of the DMCA.[35] Operators of next generation Internet networks will have the technological capability and commercial motivation to deviate from operating as neutral conduits, but the possibility exists that they have not fully assessed the legal and financial consequences vis-à-vis the intellectual property rights of the content creators whose work they carry.

The sometimes acrimonious debate over network neutrality has largely ignored whether ISPs engaging in packet inspection risk losing a valuable exemption from liability for contributory copyright infringement and vicarious liability. Likewise the debate has not addressed the impact of non-neutral network operation on the balance of power between consumers and creators of intellectual property. Arguably ISPs will have much greater capability to protect intellectual property rights, in light of the contractual QOS commitments they make to specific customers and the enhanced knowledge of the nature and type of the traffic that traverses their networks. Such technological capability may further condition or eliminate the DMCA safe harbor because ISPs may no longer claim they lack "actual knowledge that the material or an activity using the material on the system or network is infringing."[36]

---

[34] The capabilities of IMS trigger the same fear as deep packet inspection in terms of depriving users routing flexibility and tiering services. "IMS is all about the core network being smart enough, and tied so tightly to applications that it allows the network to become application aware. Now the network is USER aware, and protocol aware. What does this mean? This means the network can very tightly control packets. IMS knows what kind of packets are on the network, set prioritization based on the types of packets, and even prioritization by end-user or content provider. The sneakiest component of IMS is the 'Policy Management Component.' This section was just glossed over in the session, but warning bells immediately went off in my head. POLICY MANAGEMENT. Now the network can automatically discriminate and control my bits. They can control content provider bits. They can differentiate on ANYTHING and ANYONE." Jules.ca, IMS—The Fruits of the Devil? (Nov. 12, 2006), http://jules.squarespace.com/jules-dot-ca/2006/11/12/ims-the-fruits-of-the-devil.html.

[35] Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2360 (1998) (codified as amended at 17 U.S.C. §§ 1201–05 (Supp. 2002)) ("DMCA").

[36] 17 U.S.C. § 512(c)(1)(A)(i) (Supp. 2002).

This Article will examine the current debate about Internet neutrality in terms of its impact on intellectual property rights, including consumers' fair use opportunities. The Article will assess whether and how ISPs might lose their safe harbor for copyright infringement liability based on new technological means to know about the content they carry. Additionally, the Article will consider whether ISPs have an affirmative duty to conduct packet inspection absent a legislative mandate. The Article also will examine the applicability of litigation[37] over mandatory processing of broadcast television "flags,"[38] which specify consumer use options, but which require equipment processing on user premises.

The Article concludes that ISPs' regulatory status as information service providers does not provide an absolute exemption from responsibilities to examine the content they carry and to provide reasonable safeguards for protecting copyrights, including the possible retention and disclosure of logs that can help identify and punish copyright infringement and other unlawful activities. Such affirmative efforts to protect creators' intellectual property rights might limit, condition, or eliminate consumers' fair use opportunities and privacy expectations.

I. NETWORK NEUTRALITY AND DIGITAL RIGHTS MANAGEMENT

In quick succession the Internet has evolved from a collaborative project among governments and universities to a commercial medium operated primarily by private ventures.[39] The

[37] Am. Library Ass'n v. FCC, 406 F.3d 689 (D.C. Cir. 2005).

[38] The broadcast video flag is "a content-protection signal that broadcasters may choose to embed into a digital broadcast transmission as a way to prevent unauthorized redistribution of [Digital Television] DTV content." BRIAN T. YEH, CONGRESSIONAL RESEARCH SERVICE, CRS REPORT TO CONGRESS, COPYRIGHT PROTECTION OF DIGITAL TELEVISION: THE BROADCAST VIDEO FLAG (2007), http://ipmall.info/hosted_resources/crs/RL33797-070111.pdf.

[39] For background on how the Internet evolved from a government underwritten project to a privatized and commercialized medium, see Rob Frieden, *Revenge of the Bellheads: How the Netheads Lost Control of the Internet*, 26 TELECOMM. POL'Y 425, 425–44 (2002) [hereinafter Frieden, *Revenge of the Bellheads*]; *see also* Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel,

first generation Internet used government subsidies to build a robust medium capable of routing electronic mail around outages to users in widely dispersed locations. The government agencies, contractors and universities linked via this Internet emphasized expansion and network connectivity with little regard for the cost of service largely because government underwriting obviated close scrutiny of cost causation. Even if operators wanted to determine traffic flows, measurement tools lacked sufficient calibration and generated significant costs by reducing the amount of payload traffic that carriers could handle.

Conceptualizing the Internet as a "network of networks,"[40] first generation Internet operators cooperated on interconnection arrangements with an eye toward promoting the accessibility and reach of the Internet. The first interconnection agreements between ISPs refrained from exact route mapping and traffic metering, instead relying on the Transmission Control Protocol to route traffic "on the fly" based on current conditions as opposed to fixed routing used by telephone companies.[41] ISPs initially refrained from metering traffic based on the expectation that traffic volumes were roughly equivalent and the cost of metering was not worth the bother in light of the availability of external government funding.

The United States largely abandoned its underwriter and anchor tenant role in 1995 with the decommissioning of NSFNet,

Larry G. Roberts & Stephen Wolff, A Brief History of the Internet, http://www.isoc.org/internet/history/brief.shtml (last visited Nov. 26, 2007).

[40] "The Internet is a network of networks, and its utility largely depends on the principle of universal interconnectivity. This is true both as a technical and as an economic matter." James B. Speta, *FCC Authority to Regulate the Internet: Creating It and Limiting It*, 35 LOY. U. CHI. L.J. 15, 31 (2003). "In particular, the routes packets traverse is dynamically determined through addresses carried in the packets themselves. If a particular communication link is busy, the packet will be routed through a less-congested path. In theory—this occurs much less often in practice—each packet of a communication may travel a different route to its destination." Susan Landau, *National Security on the Line*, 4 J. TELECOMM. & HIGH TECH. L. 409, 424 (2006).

[41] "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." *See* Yoo, *Beyond Network Neutrality*, *supra* note 24, at 8.

the major backbone network funded by the National Science Foundation.[42] The ensuing privatization of the Internet forced operators to pay closer attention to infrastructure costs and traffic streams with an eye toward recovering costs from the responsible parties. ISPs largely abandoned the offer of zero cost network access to other ISPs, known as peering, except for similarly sized counterparts with matching traffic, available bandwidth, and geographical reach. Smaller ISPs now must pay for "transiting"[43] access to larger ISPs' networks and the access these ISPs have secured to other ISPs' networks.

The Internet's developing third generation[44] appears poised to exploit technological innovations, expanding broadband access and converging markets with even greater service diversity and market segmentation. This next generation[45] World Wide Web will not appear as a standard, "one size fits" all medium primarily because consumers will expect more and different features. For example, online game players and VoIP [46] users will require "better than

---

[42] *See supra* note 26.

[43] Internet transiting refers to a traffic routing arrangement whereby one ISP agrees to accept traffic for onward routing for compensation. Transiting involves a settlement and payment of funds because one ISP requires access to the links, subscribers and content available via another ISP's network and its peering arrangements. "Transit is the business relationship whereby one ISP provides (usually sells) access to all destinations in its routing table." WILLIAM B. NORTON, INTERNET SERVICE PROVIDERS AND PEERING, DRAFT 2.5, 1 (May 30, 2001) http://www.equinix.com/pdf/whitepapers/PeeringWP.2.pdf.

[44] The Internet's first generation emphasized network expansion and efforts to promote connectivity with little regard for cost, because a third party (government) subsidized such efforts. The second generation marked a migration from government subsidization to private, commercial network operation. The ongoing migration to a third generation appears to emphasize diversification of services, prices and quality as ISPs pursue price and QOS discrimination opportunities. *See, e.g.*, International Telecommunication Union, What Rules for IP-enabled NGN?, Workshop (March 23–24, 2006), *available at* http://www.itu.int/osg/spu/ngn/event-march-2006.phtml (last visited Nov. 26, 2007).

[45] *See, e.g.*, *id.*

[46] Voice over the Internet Protocol ("VoIP") refers to the use of the Internet to carry and deliver on a real time, immediate basis packets of data that correspond to a voice conversation. VoIP services range in quality, reliability and price and can link both computers and ordinary telephone handsets. For technical background on how VoIP works, see Stephen E. Blythe, *The Regulation of Voice-Over-Internet-Protocol in the United States, the European Union, and the United Kingdom*, 5 J. HIGH TECH. L. 161 (2005); SUSAN SPRADLEY & ALAN STODDARD, TUTORIAL ON TECHNICAL CHALLENGES ASSOCIATED WITH THE EVOLUTION TO VOIP, POWER POINT PRESENTATION (2003), http://www.fcc.gov/oet/tutorial/9-22-03_voip-final_slides_only.ppt (last visited Nov. 24,

best efforts" [47] routing of bits and presumably will accept the obligation to pay for less delay, jitter[48] and dropped packets.[49] Already privacy, QOS and other factors support efforts to offer users the benefit of private networking with conditional and managed access via the public Internet. Similarly content providers can use caching[50] and premium traffic routing and

2007). *See also* Del Bianco, *supra* note 27; R. Alex DuFour, *Voice Over Internet Protocol: Ending Uncertainty and Promoting Innovation Through a Regulatory Framework*, 13 COMMLAW CONSPECTUS 471 (2005); Jerry Ellig and Alastair Walling, *Regulatory Status of VoIP in the Post-Brand X World*, 23 SANTA CLARA COMPUTER & HIGH TECH. L.J. 89 (2006); Amy L. Leisinger, *If It Looks Like a Duck: The Need for Regulatory Parity in VoIP Telephony*, 45 WASHBURN L.J. 585 (2006).

[47] "The Internet is a vast network of individual computers and computer networks that communicate with each other using the same communications language, Transmission Control Protocol/Internet Protocol (TCP/IP). The Internet consists of approximately more than 100 million computers around the world using TCP/IP protocols. Along with the development of TCP/IP, the open network architecture of the Internet has the following characteristics or parameters: 1. Each distinct network stands on its own with its own specific environment and user requirements, notwithstanding the use of TCP/IP to connect to other parts of the Internet. Communications are not directed in a unilateral fashion. Rather, communications are routed throughout the Internet on a best efforts basis in which some packets of information may go through one series of computer networks and other packets of information go through a different permutation or combination of computer networks, with all of these information packets eventually arriving at their intended destination. 2. Black boxes, for lack of a better term, connect the various networks; these boxes are called 'gateways' and 'routers.' The gateways and routers do not retain information but merely provide access and flow for the packets being transmitted. 3. There is no global control of the Internet." Konrad L. Trope, *Voice Over Internet Protocol: The Revolution in America's Telecommunications Infrastructure*, COMPUTER & INTERNET LAWYER, Dec. 2005, *available at* http://www.accessmylibrary.com/coms2/summary_0286-12328904_ITM.

[48] "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.'" EDWARD W. FELTEN, CTR. FOR INFO. TECH. POLICY, NUTS AND BOLTS OF NETWORK NEUTRALITY (2006), http://itpolicy.princeton.edu/pub/neutrality.pdf.

[49] For services that need immediate, "real time" packet delivery, e.g., streaming audio and video, any failure to receive packets in time and in proper sequence will result in a noticeable degradation in service quality. The packets are lost and cannot be resent.

[50] Caching refers to intermediate and temporary storage of data. "Google makes and analyzes a copy of each Web page that it finds, and stores the HTML code from those pages in a temporary repository called a cache." Field v. Google, Inc., 412 F. Supp. 2d

management service to secure more reliable service than that available from best efforts routing.

Service diversification can require many reasonable and lawful types of discrimination between Internet users notwithstanding a heritage in the first two generations of nondiscrimination and best efforts routing of traffic. Most ISPs offer access on an unmetered, monthly subscription basis, but some ISPs already offer different levels of bit delivery speeds to subscribers. Likewise ISPs increasingly have the ability to examine individual traffic streams[51] and prioritize them creating a dichotomy between plain vanilla, best efforts routing and more expensive, superior traffic management services.

"[T]he potential exists for carriers operating the major networks used to switch and route bitstreams to go beyond satisfying diverse [consumer] requirements . . . ."[52] Advocates for the principle of network neutrality[53] claim the potential exists for ISPs to engineer a fragmented and "balkanized" next generation Internet to achieve anticompetitive goals.[54] The worst case

1106, 1110 (D. Nev. 2006) (holding that the DMCA provides a "safe harbor" exemption from liability for making cached copies of copyrighted works).

[51] "A packet sniffer (also known as a network analyzer or protocol analyzer or, for particular types of networks, an Ethernet sniffer or wireless sniffer) is computer software or computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and eventually decodes and analyzes its content according to the appropriate RFC or other specifications." Packet Sniffer, Wikipedia, http://en.wikipedia.org/wiki/Packet_sniffer (last visited Nov. 12, 2007) (emphasis omitted).

[52] Rob Frieden, *Internet 3.0: Identifying Problems and Solutions to the Network Neutrality Debate*, INT'L. J. OF COMM. (forthcoming), *available at* http://law.bepress.com/cgi/viewcontent.cgi?article=9455&context=expresso (last visited Nov. 26, 2007) [hereinafter Frieden, *Internet 3.0*].

[53] For links to a representative sample of advocacy papers and analyses of network neutrality, see Papers, Conferences & Surveys—National Regulatory Research Institute, http://www.nrri.ohio-state.edu/Telecom/hot-topics-links/net-neutrality/papers (last visited Nov. 24, 2007). *See also* Frieden, *Internet 3.0*, *supra* note 52; Frieden, *Network Neutrality or Bias?*, *supra* note 23.

[54] *See, e.g.*, Barbara A. Cherry, *Misusing Network Neutrality to Eliminate Common Carriage Threatens Free Speech and the Postal System*, 33 N. KY. L. REV. 483 (2006); Brett Frischmann & Barbara van Schewick, *Network Neutrality and the Economics of an Information Superhighway: A Reply to Professor Yoo*, 47 JURIMETRICS J. (forthcoming 2007), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1014691; Mark A. Lemley and Lawrence Lessig, *The End of End-to-End: Preserving the Architecture of*

scenario envisioned by network neutrality advocates is a reduction in innovation, efficiency, consumer benefits, and national productivity occasioned by a divided Internet: one medium prone to congestion and declining reliability and one offering superior performance and potential competitive advantages to users able and willing to pay, or affiliated with the ISP operating the bitstream transmission network.[55] Opponents of network neutrality mandates scoff at the possibility of the worst-case scenario and view government intervention as anathema.[56]

the Internet in the Broadband Era, 48 UCLA L. REV. 925 (2001); Barbara van Schewick, *Towards an Economic Framework for Network Neutrality Regulation*, 5 J. TELECOMM. & HIGH TECH. L. 329 (2007); Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. TELECOMM. & HIGH TECH. L. 141 (2005), *available at* http://ssrn.com/abstract=388863.

[55] *See* Jeff Chester, *The End of the Internet?*, THE NATION, Feb. 1, 2006, www.thenation.com/doc/20060213/chester; Freepress: Net Freedom Now!, http://www.freepress.net/deadend/=neutrality, *available at* http://web.archive.org/web/20070410094102/http://www.freepress.net/deadend/=neutrality (last visited Apr. 10, 2007) (on file with author); Net Neutrality—Common Cause, http://www.commoncause.org/site/pp.asp?c=dkLNK1MQIwG&b=1421497 (last visited Nov. 12, 2007); Andrew Raff, *IPTAblog: Net Neutrality Reading List*, http://www.iptablog.org/2006/02/28/net_neutrality_reading_list.html (Feb. 28, 2006, 20:49 EST); TREVOR R. ROYCROFT, ECONOMIC ANALYSIS AND NETWORK NEUTRALITY: SEPARATING EMPIRICAL FACTS FROM THEORETICAL FICTION (Issue Brief Prepared for Consumer Federation of America, Consumers Union and free Press) (2006), http://www.freepress.net/docs/roycroft_study.pdf (last visited Nov. 27, 2007); Save the Internet: Fighting for Internet Freedom, http://www.savetheinternet.com (last visited Nov. 12, 2007); Tim Wu, *Why You Should Care About Network Neutrality, The Future of the Internet Depends on it!*, SLATE, May 1, 2006, http://www.slate.com/id/2140850.

[56] *See* Raymond L. Gifford, *The Internet Left Gets a Case of the Vapors*, PROGRESS SNAPSHOT RELEASE 2 (The Progress & Freedom Foundation) June 15, 2006, *available at* http://www.pff.org/issues-pubs/ps/2006/ps_2.15_intenet_left.pdf; Thomas W. Hazlett, *Neutering the Net*, FIN. TIMES, Mar. 20, 2006, *available at* http://news.ft.com/cms/s/392ad708-b837-11da-bfc5-0000779e2340.html; David P. McClure, Network Neutrality: Phantom Problem, Unintended Consequences (U.S. Internet Industry Association), Mar. 14, 2006, http://www.usiia.org/pubs/NNPrimer.doc; NET NEUTRALITY OR NET NEUTERING: SHOULD BROADBAND INTERNET SERVICES BE REGULATED (Thomas M. Lenard & Randolph J. May eds., 2006); J. Gregory Sidak, Visiting Professor of Law, Georgetown University, Testimony before the United States Senate Committee on Commerce, Science, and Transportation (Feb. 7, 2006) (transcript available at http://commerce.senate.gov/pdf/sidak-020706.pdf); J. Gregory Sidak, *A Consumer-Welfare Approach to Network Neutrality Regulation of the Internet*, 2 J. COMPETITION L. & ECON. 349 (2006); Adam Thierer, *Are 'Dumb Pipe' Mandates Smart Public Policy? Vertical Integration, Net Neutrality, and the Network Layers Model*, 3 J. TELECOMM. & HIGH TECH. L. 275 (2005); Yoo, *Beyond Network Neutrality*, *supra* note 24; Yoo,

A. Deep Packet Inspection and Digital Rights Management

ISPs engaging in price and QOS discrimination must engage in active network management. Rather than operate as a neutral conduit with no reason to examine the nature and types of traffic that traverse their networks, ISPs keen on taping new service diversification opportunities, have to use technologies that examine the packets the ISPs will switch, route and deliver. Next generation Internet routing equipment provides operators the ability to "sniff" and inspect specific packet streams so that the ISP can perform a number of revenue generating functions including the assignment of traffic to regular or priority subnetworks, guarding against theft of service, and filtering out spam.[57]

Such packet inspection also provides ISPs with a greater ability to determine whether the traffic they carry respects all intellectual property rights of the content creator. In other words, packet sniffing provides the means for ISPs to determine whether their network has become a medium for the unlawful transport of files to recipients lacking lawful authority to consume, copy, and share intellectual property.[58]

Internet equipment providers recognize the market opportunity created by deeper and more granular traffic inspection:

> In order to deal with the increasingly competitive broadband market, service providers need the tools that allow them to differentiate services not only by bandwidth tiers, but on application and content bases as well. And because of the increasing diversity of stakeholder needs, such as the use of

Network Neutrality, *supra* note 24; Yoo, *Would Mandating Broadband Help or Hurt Competition?*, *supra* note 24.

[57] "Deep packet inspection (DPI) technology allows service providers to peer inside next-generation network (NGN) packets to see what users are up to – what applications they are using, where their traffic is going, and so on. It all sounds distinctly Orwellian, but it seems that service providers are embracing the concept with enthusiasm." Light Reading.com, Deep Packet Inspection, http://www.lightreading.com/document.asp?doc_id=111404 (last visited Nov. 12, 2007).

[58] For discussion about the differences between actual knowledge of copyright infringement and notification about the possibility of such infringement, see Emily Zarins, *Notice Versus Knowledge Under the Digital Millennium Copyright Act's Safe Harbors*, 92 CAL. L. REV. 257 (2004).

> P2P applications . . . they must be able to differentiate the online experience of individual users—not by IP address alone, but through the identification of individual users by name. . . . The Cisco Service Control Engine combines deep packet inspection with specific subscriber identification, allowing the service provider to properly segment its customer base and provide individualized services to differing demographic 'clusters.' As a result, the service provider competes on factors other than price, and can generate incremental revenue from application-based services rendered.[59]

Cisco, a major Internet equipment manufacturer, also states that its traffic interrogation capabilities offer "the ability to identify traffic streams of individual users, and control application and network use differentially based on assigned 'online' rights, [thereby] ensur[ing] protection of critical applications [and] network fairness . . . ."[60]

B. Network Neutrality Qualifies ISPs for Copyright Infringement Safe Harbors

Currently, § 512 of the DMCA[61] provides ISPs with conditional exemptions from direct or secondary liability for copyright infringement that occurs over their networks. In an effort to balance the obligation to protect copyright holders with an interest in promoting investment in the Internet and its use as an engine for commerce, Congress included in the DMCA a chapter entitled the Online Copyright Infringement Liability Limitation Act.[62] The DMCA establishes four safe harbor exemptions from liability for online "service providers"[63] when they operate as a neutral, transitory conduit for content, engage in temporary caching or storing of content, and when they provide search tools

---

[59] Cisco Service Control Engine: Q & A, http://www.cisco.com/en/US/products/ps6151/products_qanda_item0900aecd8041c9d4.shtml (last visited Nov. 12, 2007).

[60] *Id.*

[61] 17 U.S.C. § 512 (2007).

[62] *See* Ellison v. Roberston, 357 F.3d 1072, 1076 (9th Cir. 2004).

[63] *See supra* note 11 (explaining the DMCA's definitions of "service provider").

that link to information created by others.[64] The DMCA generally bars any monetary damages for direct, contributory, and vicarious infringements of ISPs provided they conform with the statute's safe harbor provisions.[65] It also restricts the availability of injunctive relief for copyright holders.[66]

To qualify for these safe harbors ISPs must not have actively participated in the placement and selection of the content, or determined who shall receive the content.[67] The ISP cannot benefit materially from the infringement,[68] but courts have differed in their common law and DMCA interpretations of what ISPs can do in terms of revenue generation without triggering liability for contributory infringement.[69] Of particular importance in light of the network neutrality debate, ISPs cannot know about the infringement[70] and must take affirmative steps to remove offending materials about which it has received notice,[71] as well as terminate service to repeat infringers.[72] ISPs also must accommodate and cannot interfere with "standard technical measures" used to identify and protect copyrighted works. [73] However the DMCA provides no guidance about technical measures installed and applied by an ISP as opposed to measures embedded in the content by the copyright holder. A "red flag" standard suggested in the

---

64 *See Ellison*, 357 F.3d at 1076–77.

65 *See* 17 U.S.C. § 512(a)–(e).

66 *See id.* § 512(j).

67 *See id.* § 512(a)(1)–(3).

68 *See id.* § 512(c)(1)(B). The DMCA safe harbor for the storage of copyright infringing content requires that in addition to not having had actual knowledge of and timely removing the infringing content, the 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." *Id.*

69 *Compare* Costar Group v. LoopNet, Inc., 164 F. Supp. 2d 688, 704–05 (D. Md. 2001) (holding that defendant's website that permitted real estate brokers to post listings did not accrue direct financial benefit because, amongst other considerations, the defendant did not charge for user access), *aff'd*, 373 F.3d 544 (4th Cir. 2004), *with* Perfect 10, Inc. v. Cybernet Ventures, 213 F. Supp. 2d 1146 (C.D. Cal. 2002) (granting plaintiff's motion for preliminary injunction in part on a finding that defendant very likely received direct financial benefit from infringing activity in light of its revenue accrual based on number of subscribers and visits to infringing sites).

70 17 U.S.C. § 512(c)(1)(A)(i)–(ii).

71 *Id.* § 512(c)(1)(C), (d)(3).

72 *Id.* § 512(i)(1)(A).

73 *Id.* § 512(i)(1)(B).

Committee Report on the DMCA[74] would not obligate ISPs to engage in active monitoring of content that ISPs store or provide links to,[75] nor would it automatically eliminate the safe harbor whenever the ISP examined content using technical or human resources.[76] On the other hand, when "the infringing nature of such sites would be apparent from even a brief and casual viewing, safe harbor status for a provider that views such a site and then establishes a link to it would not be appropriate."[77]

Safe harbors for storage and linking to infringing material emphasize the need for ISPs to lack actual knowledge about infringing activity, including facts or circumstances from which infringing activity is apparent. Courts found that Internet ventures such as Napster[78] and Grokster[79] induced infringing activity and surely knew or should have known that it frequently occurred. These ventures received a financial benefit directly attributable to the infringing activities[80] and they also had the "right and ability"[81] to control such conduct.

---

74 COMM. ON COMMERCE, DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998, H.R. DOC. NO. 105–551, pt. 2, at 53 (1998).

75 *See id.* "[A] service provider would have no obligation to seek out copyright infringement, but it would not qualify for the safe harbor if it had turned a blind eye to 'red flags' of obvious infringement." *Id.* at 57.

76 *See id.* at 57–58 ("A question has been raised as to whether a service provider would be disqualified from the safe harbor based solely on evidence that it had viewed the infringing Internet site. If so, there is concern that on-line directories prepared by human editors and reviewers, who view and classify various Internet sites, would be denied eligibility to the information location tools safe harbor, in an unintended number of cases and circumstances. . . . For instance, the copyright owner could show that the provider was aware of facts from which infringing activity was apparent if the copyright owner could prove that the location was clearly, at the time the directory provider viewed it, a 'pirate' site . . . where sound recordings, software, movies, or books were available for unauthorized downloading, public performance, or public display. Absent such 'red flags' or actual knowledge, a directory provider would not be similarly aware merely because it saw one or more well known photographs of a celebrity at a site devoted to that person. The provider could not be expected, during the course of its brief cataloguing visit, to determine whether the photograph was still protected by copyright or was in the public domain; if the photograph was still protected by copyright, whether the use was licensed; and if the use was not licensed, whether it was permitted under the fair use doctrine.").

77 *Id*. at 58.

78 A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1019–20 (9th Cir. 2001).

79 Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 937–41 (2005).

80 *See id*. at 939–40; *Napster*, 239 F.3d at 1023.

ISPs operating in a network neutral environment qualify for the safe harbor exemption from copyright infringement liability. Nevertheless, it follows that to qualify for the safe harbor ISPs might have to eschew deep packet inspection or limit its nature and scope because this process would evidence a non-neutral operating environment where the ISP has the ability to know when copyright infringement takes place. ISPs may soon view network neutrality obligations contained in the DMCA as providing a less valuable safe harbor if it forecloses their use of deep packet inspection.

C. Non Neutral Network Operation May Lose the DMCA Safe Harbor

ISPs deploying deep packet inspection have maximum flexibility to pursue price and QOS discrimination at the likely loss of the DMCA § 512 safe harbors. Arguably deep packet inspection constitutes an affirmative effort on the part of the ISP to monitor the flow of packets traversing the ISP's network. While monitoring by itself may not eliminate the safe harbor qualification, deep packet monitoring probably does because the packet header information likely will identify significant information about the nature and type of traffic sufficient to put the ISP on actual notice of any copyright infringement. While the ISP needs only information about QOS and other features for which a particular user and user generated traffic stream qualifies, the ISPs cannot lawfully ignore copyright status if such information becomes part of the standard header information ISPs routinely inspect and process.[82]

The header information contained in packets, subject to inspection, can provide information sufficient for automated decision making regarding the QOS and other diversified services available to ISP traffic. Such automation empowers information processing equipment and software to make binding decisions about the treatment of specific bitstreams quite possibly without

---

[81] 17 U.S.C. § 512(c)(1)(B) (1999).

[82] *See* 17 U.S.C. § 512(i)(1)(B) (conditioning ISP safe harbor eligibility on their accommodation and non-interference with "standard" DRM techniques).

any human involvement. The judgments made by computer chips and code will have a profound impact on how bitstreams are treated during their journey through one or more ISP networks and possibly also what recipients of the traffic can do with the content after receiving it.

1. The Significance of Where and Why Packet Inspection Occurs

ISPs offering tiered Internet services typically will need to inspect packets using equipment located on the ISPs' premises as part of the process for assigning traffic to superior or regular treatment. In other words, when ISPs take affirmative steps to operate non-neutral networks, they have explicitly decided to probe traffic and to subject them to differential treatment based on what the packet headers disclose. ISPs can lawfully deploy deep packet inspection because this functionality occurs at ISP locations, using ISP equipment and most likely with notice, if not express approval by the subscriber.

Voluntary deep packet inspection contrasts with regulator-compelled examination and processing of similar type header information, e.g., broadcast "flags,"[83] using consumer electronic devices. In *American Library Ass'n v. FCC*,[84] the Court of Appeals for the District of Columbia rejected as beyond the FCC's jurisdiction a mandate for compulsory processing of copyright protection directives by consumers' digital television receivers.[85] The court rejected the FCC's assertion of jurisdiction over any

[83] *See* Am. Library Ass'n v. FCC, 406 F.3d 689, 691 (D.C. Cir. 2005) ("The broadcast flag is a digital code embedded in a . . . broadcasting stream, which prevents digital television reception equipment from redistributing broadcast content . . . ."). "The effectiveness of the broadcast flag regime is dependent on programming being flagged *and* on devices capable of receiving broadcast DTV signals (collectively 'demodulator products') being able to recognize and give effect to the flag." *Id.* at 693.

[84] *Id.*

[85] *See id.* at 693 ("The broadcast flag does not have any impact on a DTV broadcast transmission. The flag's only effect is to limit the capacity of [a consumer's] receiver apparatus to redistribute broadcast content after a broadcast transmission is complete."); *id.* at 692 ("Title I [of the Communications Act of 1934, as amended, 47 U.S.C. § 151 *et seq*.] does not authorize the Commission to regulate receiver apparatus after a transmission is complete.").

demodulator product, if that demodulator product was needed to process and enforce the copy protection flag:

> the *Flag Order* does not require demodulator products to give effect to the broadcast flag until *after* the DTV broadcast is complete. The *Flag Order* does not regulate the actual transmission of the DTV broadcast. In other words, the *Flag Order* imposes regulations on devices that receive communications after those communications have occurred; it does not regulate the communications themselves. Because the demodulator products are not engaged in 'communication by wire or radio' when they are subject to regulation under the *Flag Order*, the Commission plainly exceeded the scope of its general jurisdictional grant under Title I in this case.[86]

The broadcast flag case prevents the FCC from extending its regulatory authority over equipment that receives or processes signals over which the FCC does have jurisdiction.[87] It follows that the FCC could not extend its jurisdiction over consumers' computers, including ones that attach to telecommunications links over which the Commission has jurisdiction. Likewise it follows that should an ISP elect to activate flag and header processing, ostensibly to have the capability to differentiate traffic streams, the ISP can create a non-neutral network environment, either with the express permission of its subscribers or because it uses its own equipment and does not trespass and take control over subscribers' equipment. Just as the FCC cannot effectuate a copyright protection scheme that would require it to extend its jurisdiction impermissibly, ISPs can activate a copyright protection scheme—intentionally or otherwise—when using their own equipment to inspect packet headers without trespassing or otherwise intruding on equipment located on users' premises.

D. The Implausibility of Activating a Non-Neutral Network That

---

86 *Id.* at 703.

87 *See id.* at 703–05.

Ignores Copyright, or Deep Packet Inspection That Retains Network Neutrality

In light of the value accruing from DMCA safe harbors, ISPs may attempt to claim that deep packet inspection can occur without impacting ISPs' knowledge of whether copyright infringement has occurred. Similarly an ISP might claim that, notwithstanding its use of deep packet inspection, the ISP will continue to comply with the spirit of network neutrality. In application, deep packet inspection appears to offer an all or nothing value proposition: either an ISP has the ability to examine content and to discriminate on the basis of several different QOS variables or it does not. To argue that an ISP can discriminate and still qualify for DMCA safe harbors and respect network neutrality would require creative interpretation of what constitutes network neutrality and "actual knowledge" of copyright infringement.

II. WHAT CONSTITUTES NETWORK NEUTRALITY?

At its core, network neutrality requires ISPs to eschew many types of price and QOS discrimination, on grounds that consumers deserve the right to access any Internet service on equal footing and service providers should have the same technological means for reaching consumers. In other words, consumers and content providers should not have to put up with tactics, such as deep packet inspection, that could identify packets and prioritize them, possibly resulting in a superior/inferior dichotomy of packet processing and delivery.

The fairness and nondiscrimination aspects of network neutrality may differ in terms of how ISPs serve end users versus how ISPs process traffic. Some, but not all, network neutrality advocates would accept tiered and differentiated service to end users based on such variables as allocated bandwidth, anticipated bitstream delivery speeds, and amount of content that a subscriber can upload and download in one month. Such "customer tiering" would offer different prices based on legitimate customer differentials thereby eliminating subsidies flowing from low volume users to high volume users when both groups pay the same flat, "all-you-can-eat" subscription rate that ISPs typically offer.

Network neutrality advocates uniformly oppose access-tiering[88] that would use techniques, such as deep packet inspection, to identify the source and type of traffic with an eye toward bifurcating service into superior, better than best efforts service and regular best efforts routing. Advocates for network neutrality worry that access tiering will create artificial congestion and an inferior Internet service environment for anyone refusing to pay for premium service.

Incumbent carriers and like minded opponents to network neutrality have characterized their opposition to network neutrality in terms of standing firm against government intrusion,[89] the imposition of a remedy in search of a problem,[90] and the need to remedy free ridership of ISP networks by content providers.[91] Outside the headlines and congressional committee hearing

---

[88] *See Network Neutrality: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 109th Cong. 54–58 (2006), *available at* http://commerce.senate.gov/public/_files/30115.PDF [hereinafter *Network Neutrality*]; *see also Network Neutrality: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 109th Cong. (2006) (statement of Professor Lawrence Lessig, Professor of Law, Stanford Law School), *available at* http://commerce.senate.gov/pdf/lessig-020706.pdf [hereinafter Lessig].

[89] *See, e.g.*, Hands Off the Internet, http://handsoff.org/blog/ (last visited Nov. 30, 2007). "Hands Off The Internet is a nationwide coalition of Internet users united together in the belief that the Net's phenomenal growth over the past decade will continue if government does not attempt an unwise effort to regulate a market that is otherwise working to give consumers the choices, freedom, prices and diverse experiences they desire in the new age of the Internet." Hands Off the Internet, http://handsoff.org/hoti_docs/aboutus/ (last visited Nov. 30, 2007).

[90] *See* Arpan Sura, *The Problem With Network Neutrality*, FREEDOMWORKS, May 2, 2006, http://www.freedomworks.org/informed/issues_template.php?issue_id=2571 ("Currently there are no principles of network neutrality encoded into law. So ISPs are already free to block or favor content as they please. It's telling that none of them has. In fact, no proponent of network neutrality can cite an existing problem to which network neutrality is a solution."). *But see* Save the Internet: Big Lie 3, http://www.savetheinternet.com/=lie3 (last visited Nov. 30, 2007) ("The constant refrain of the Astroturf groups like McCurry's 'Hands Off the Internet' is that Network Neutrality is a solution in search of a problem. They cite the absence of numerous examples of blocking or degradation to back this argument. This is a red herring. There are multiple real-world instances of blocking and impairment.").

[91] *See* Arshad Mohammed, *Verizon Executive Calls for End to Google's 'Free Lunch,'* WASH. POST, Feb. 7, 2006, at D01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020601624.html ("The network builders are spending a fortune constructing and maintaining the networks that Google intends to ride on with nothing but cheap servers. . .").

rooms[92] these carriers object to network neutrality on two more practical concerns: 1) it would foreclose pricing and QOS initiatives, made possibly through new techniques including deep packet inspection, that can generate new revenues and profits; and 2) it would resurrect some of the regulatory constraints and content scrutiny obligations the carriers thought they had avoided once and for all having qualified for both copyright and information service provider safe harbors.

A. Network Neutrality as a Constraint on Price Discrimination

Network neutrality, whether imposed by law or public interest based FCC regulation, can impose direct restrictions on ISP pricing and diversification of services based on such factors as reliability, allocated bandwidth, performance during network congestion, ability to handle spikes in demand, and quality of service. Not all network neutrality advocates object to "customer tiering"[93] that constitutes price and QOS discrimination on the end user, demand side. ISPs already offer end users different subscription rates based of bandwidth and bitrates. Additional differentiation could involve variable service quality, based on the ability to handle peak demand bursts as occurs in peer-to-peer networking, video gaming, delivery of large files, and real time streaming of video programming. Deep packet inspection would make it possible for ISPs to identify priority traffic and to provide superior and preferential processing for a premium price.

Similarly the concept of network neutrality does not foreclose attempts by incumbent carriers to reshape access pricing into a conventional two-sided market[94] where ISPs would demand and

---

92 *See, e.g.*, *Network Neutrality*, *supra* note 88; *The Communications Opportunity, Promotion, and Enhancement Act of 2006: Hearing Before the Subcomm. on Telecomm. & the Internet of the H. Comm. on Energy & Commerce*, 109th Cong. (2006), *available at* http://a257.g.akamaitech.net/7/257/2422/3aug20061330/www.access.gpo.gov/congress/house/pdf/109hrg/28317.pdf.

93 *See Network Neutrality*, *supra* note 88, at 54–58; *see also* Lessig, *supra* note 88.

94 Jean-Charles Rochet & Jean Tirole, *Two-Sided Markets: A Progress Report* 2 (Institut d'Économie Industrielle [IDEI], Univ. of Toulouse, Working Paper No. 275, Mar. 12, 2004), *available at* http://faculty.haas.berkeley.edu/hermalin/rochet_tirole.pdf ("Two-sided (or more generally multi-sided) markets are *roughly* defined as markets in which one or several platforms enable interactions between end-users, and try to get the

receive payments downstream and upstream regardless of whether they serve end users. Under the current pricing arrangement a two sided market already exists for ISPs that can collect an Internet access subscription from end users for DSL and cable modem access to the Internet cloud[95] and also charge fees for providing small ISPs access to major portions of the Internet population these small ISPs cannot reach via their own networks.

Former AT&T Chairman Ed Whitacre has objected to the one sided market scenario where AT&T receives subscription payments from end users, but no additional payments from content generators who "use" AT&T networks without making direct payments to AT&T.[96] However, nothing about network neutrality forecloses AT&T from erecting a service so attractive to Google and other heavy users of the Internet as to entice them to opt for a contractual agreement providing for premium carriage of their traffic in lieu of the shared routes made available through the peering[97] and transit[98]arrangements secured by the ISPs directly

two (or multiple) sides 'on board' by appropriately charging each side. That is, platforms court each side while attempting to make, or at least not lose, money overall.").

[95] Rob Frieden, *Internet 3.0: Identifying Problems and Solutions to the Network Neutrality* Debate, 1 INT'L J. COMM. 461, 474 & n. 47, *available at* http://ijoc.org/ojs/index.php/ijoc/article/viewFile/160/86 ("The Internet cloud refers to the vast array of interconnected networks that make up the Internet and provides users with seamless connectivity to these networks and the content available via these networks."); *see also* Alex Barnett Blog, *So What Do We Mean by the 'Internet Cloud'?*, http://alexbarnett.net/blog/archive/2007/04/04/what-is-the-internet-cloud_3F00_.aspx (Apr. 4, 2007, 23:30 EDT).

[96] *At SBC, It's All About "Scale and Scope"*, BUS. WK., Nov. 7, 2005, http://www.businessweek.com/@@n34h*IUQu7KtOwgA/magazine/content/05_45/b3958092.htm ("Now what they would like to do is use my pipes free, but I ain't going to let them do that because we have spent this capital and we have to have a return on it. So there's going to have to be some mechanism for these people who use these pipes to pay for the portion they're using. Why should they be allowed to use my pipes? The Internet can't be free in that sense, because we and the cable companies have made an investment and for a Google or Yahoo! or Vonage or anybody to expect to use these pipes [for] free is nuts!").

[97] Internet peering refers to a reciprocal traffic routing arrangement whereby one ISP agrees to accept traffic for onward routing in exchange for a similar routing commitment by another ISP. Peering typically involves no settlement or payment of funds as ISPs agree to peer only if they generate and receive roughly the same volume of traffic. William B. Norton, Internet Service Providers and Peering, Draft 2.5, 2–3 (undated) (unpublished manuscript), *available at* http://pages.cs.wisc.edu/~akella/CS740/S07/740-Papers/Nor00.pdf (last visited Nov. 12, 2007).

serving these heavy users. For example, Akamai[99] and other network management firms offer clients enhanced Internet traffic routing and content delivery by offloading traffic from best efforts routing options and onto better-than-best efforts options. Traffic can reach consumers with greater likelihood for on time delivery and reliability when ISPs and other Internet companies directly manage particular traffic streams with an eye toward reducing the number of routers the traffic has to traverse, avoiding circuitous routing and inserting traffic on the most reliable and least congested networks.

Many universities, along with corporations, government research agencies, and not-for-profit networking organizations, have agreed to achieve this type of outcome by underwriting superior routing through the Internet2 network,[100] a series of broadband links not regularly available to non-investors. Internet2 has links to and from the plain vanilla Internet, but investors have enhanced the likelihood of reliable and qualitative superior routing by creating a direct or near direct links among investing organizations. The corporate equivalent to this better-than-best efforts complete link from content source to consumer are virtual private networks and Intranets that carve out a small portion of the overall infrastructure used to provide Internet telecommunications.

Nothing would foreclose AT&T and other ISPs from engineering a superior and complete Internet routing arrangement using the carrier's own facilities, or those of other carriers with which AT&T negotiated a special traffic management and routing

---

[98] Internet transiting refers to a traffic routing arrangement whereby one ISP agrees to accept traffic for onward routing for compensation. Transiting involves a settlement and payment of funds because one ISP requires access to the links, subscribers and content available via another ISP's network and its peering arrangements. "Transit is the business relationship whereby one ISP provides (usually sells) access to all destinations in its routing table." *Id.* at 1.

[99] "Akamai uses . . . [network] intelligence to optimize routes and replicate data dynamically to deliver content and applications more quickly, reliably, and securely." Akamai Edge Platform: Application Acceleration that Delivers Content and Applicatons Quickly, Reliably, and Securely, http://www.akamai.com/html/technology/edgeplatform.html (last visited Nov. 11, 2007).

[100] *See* The Internet2 Network, http://www.internet2.edu/network/ (last visited Nov. 11, 2007).

agreement.[101] Network neutrality only would foreclose AT&T from punishing Internet users who have declined the managed service option with "less-than-best efforts routing," that is, deliberately dropping packets, creating artificial network congestion, violating Service Level Agreements[102] and otherwise deteriorating the quality of service provided by network links that AT&T has agreed to make available to other peers and transit customers, including the ISPs directly serving heavy volume content providers such as Google.

B. Does Network Neutrality Impose Common Carrier Responsibilities on ISPs?

ISPs make a valid point that elements of network neutrality would impose elements of common carrier regulatory burdens that they have managed to avoid while still qualifying for the DMCA safe harbors. Having avoided compulsory nondiscrimination requirements, ISPs now want to use deep packet inspection and other techniques to engage in selective price and QOS discrimination while at the same time retaining the ISP status that eliminates most regulatory scrutiny.

While common carrier regulation imposes some degree of constraints that would not otherwise exist, one should examine closely the nature of common carrier-type restrictions that network neutrality would impose. Not all common carriers face the same level of constraints, and the Telecommunications Act of 1996 provides a method for selective elimination of common carrier burdens when the public interest supports such a reduction.[103] Technically cellular telephone companies still operate under some

---

[101] *See* Craig McTaggart, Was The Internet Ever Neutral?, (revised Sept. 30, 2006) (unpublished paper, prepared for the 34th Research Conference on Communication, Information and Internet Policy, George Mason University School of Law, Arlington, Virginia), *available at* http://web.si.umich.edu/tprc/papers/2006/593/mctaggart-tprc06rev.pdf (last visited Nov. 11, 2007).

[102] Service Level Agreements specify network performance commitments typically between ISPs and their customers.

[103] Communications Act of 1934, § 10(c) (codified as amended at 47 U.S.C. § 160(c) (1996)).

of the constraints of common carrier regulation,[104] but one could hardly say such regulation imposes any significant constraint on pricing and operational flexibility including the ability to operate clearly non-neutral networks in terms of content access and limitations on the flexible use of wireless telephone handsets. Indeed cellular carriers have avoided most common carrier restrictions including limitations on erecting "walled garden," preferred access to video and Internet-based content accessible on the screens of handsets used by subscribers.[105]

In other proceedings the FCC has shown that it can and will impose quasi-common carrier responsibilities on non common carriers if the public interest warrants, or Congress requires it. The FCC has required non common carrier, cable and satellite television companies to carry broadcast television signals as a form of economic and public interest regulation designed to safeguard the continuing viability of broadcast television stations.[106] Recently the FCC has required, non common carrier VoIP service providers to contribute to universal service funding,[107] to support enhanced 911 emergency access[108] and to cooperate with law

[104] In re Pers. Commc'ns Indus. Assoc.'s Broadband Pers. Commc'ns Servs. Alliance's Petition for Forbearance For Broadband Pers. Commc'ns Servs., 13 F.C.C.R. 16857 (1998); In re Implementation of Sections 3(n) and 332 of the Commc'ns Act, Regulatory Treatment of Mobile Servs., 9 F.C.C.R. 1411, 1478 (1994); Orloff v. FCC, 352 F.3d 415, 419 (D.C. Cir. 2003) (noting that although the Commission found that the competitiveness of the commercial mobile radio service market justified exempting such carriers from the tariff requirements of § 203 of the Act, the Commission had nonetheless declined to exempt them from §§ 201 or 202).

[105] *See* Rob Frieden, *Wireless Carterfone—A Long Overdue Policy Promoting Consumer Choice and Competition*, New America Foundation, Wireless Future Program, Working Paper No. 20 (Jan. 2008); *available at*: http://www.newamerica.net/files/Wireless_Carterfone_Frieden.pdf.

[106] *See* 47 U.S.C. §§ 325, 338–40, 534–35, 543, 548 (1999); Turner Broad. Sys., Inc. v. FCC (Turner I), 512 U.S. 622 (1994); Turner Broad. Sys., Inc. v. FCC (Turner II), 520 U.S. 180 (1997); 47 C.F.R. § 76.55–62 (2006) (cable must carry); 47 C.F.R. § 76.64 (2006) (cable retransmission consent); 47 C.F.R. § 76.66 (2006) (DBS signal carriage).

[107] Universal Serv. Contribution Methodology, 21 F.C.C.R. 7518 (2006).

[108] IP-Enabled Servs., 20 F.C.C.R. 10245 (2005). The FCC declined to determine the statutory classification of interconnected VoIP services, but asserted ancillary jurisdiction under Title I of the Act to require interconnected VoIP service providers to supply 911 emergency calling capabilities to their customers. *Id.*

enforcement officials[109] in much the same way as common carrier regulated telephone companies.

C. Are Network Neutrality Requirements Confiscatory and a Taking of Property?

Opponents to network neutrality also imply that network neutrality requirements constitute a "confiscatory" and unlawful "taking" of their property.[110] Having invested in next generation infrastructure at significant expense, both incumbent telephone and cable television operators expect to have nearly complete freedom from telecommunications service regulation. However next generation networks will offer an integrated blend of services, including the functional equivalents of traditionally regulated, legacy voice telephony and cable television.

The incumbent carriers appear ready to make two key arguments that equate regulation going forward as confiscatory: 1) robust facilities-based competition obviates the need for regulation, including common carrier aspects of network neutrality; and 2) commingling and integrating services that use telecommunications for bitstream transmission convert all retail offerings into information services. The incumbents have convinced many legislators and regulators that network neutrality requirements do not make sense in a competitive environment where the Internet serves as a single medium for convergent information, communications and entertainment services.

---

[109] Commc'ns Assistance for Law Enforcement Act & Broadband Access & Servs., 20 F.C.C.R. 14989 (2005).

[110] While reviewing courts have questioned the nature, type and rates of the FCC mandated common carrier interconnection and facilities-leasing requirements, the judiciary has not deemed the requirements confiscatory. "The incumbent carriers here are just like the electric utilities in *Duquene* in failing to present any evidence that the decision to adopt TELRIC [i.e., compulsory pricing of local exchange service elements on the basis of quite low Total Element Long Run Incremental Cost] was arbitrary, opportunistic, or undertaken with a confiscatory purpose. What we do know is very much to the contrary." Verizon Commc'ns, Inc. v. FCC, 535 U.S. 467, 527–28 (2002); FCC v. Fla. Power Corp., 480 U.S. 245 (1987) (holding that the rate set by the FCC was not confiscatory and thus did not amount to an unconstitutional taking).

D. The Information Service Classification Safe Harbor

Major ISPs also have led a successful campaign to qualify as information services their broadband first and last mile links to the Internet cloud, viz. DSL and cable modem access. This classification qualifies ISPs for an exemption from any common carrier, telecommunications service regulation. Having classified Internet access as an information service, the FCC will have to resort to clever and probably unsustainable semantic maneuvering to classify as a telecommunications service any software application, riding on top[111] of the information service classified bitstream transmission functionality.[112] If this scenario plays out

[111] The FCC uses telecommunications service and information service definitions to establish regulatory classifications, without considering the several layers of functionality involved. For example companies supplying software, which can be installed for use when initiating an Internet session, properly avoid FCC regulation. Likewise the FCC can avoid having to regulate the protocols and standards establishing standard operating procedures for switching, routing and managing Internet traffic. *See, e.g.*, *Net Neutrality: Before the S. Comm. On Commerce, Science and Transportation*, 106th Cong. (2006) (statement of Vinton G. Cerf, Vice President and Chief Internet Evangelist, Google, Inc.), *available at* http://commerce.senate.gov/pdf/cerf-020706.pdf. "The Internet's open, neutral architecture has proven to be an enormous engine for market innovation, economic growth, social discourse, and the free flow of ideas. The remarkable success of the Internet can be traced to a few simple network principles—end-to-end design, layered architecture, and open standards—which together give consumers choice and control over their online activities." *Id.*

[112] While the FCC also exempts bitstream transmitting carriers from regulation, in light of the information service classification, the Commission could opt to examine separately the different layers combined to support the delivery of a service, such as VoIP. For background on a revised regulatory regime that applies different degrees of government oversight based on the scope of competition in each layer of service that blends telecommunications packet delivery with intelligent networking, software applications and content, see Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*, 52 FED. COMM. L.J. 561 (2000); Robert Cannon, *The Legacy of the Federal Communications Commission's Computer Inquiries*, 55 FED. COMM. L.J. 167 (2003); Frieden, *Adjusting the Horizontal and Vertical*, *supra* note 2; Craig McTaggert, *A Layered Approach to Internet Legal Analysis*, 48 MCGILL L.J. 571 (2002); John T. Nakahata, *Regulating Information Platforms: The Challenge of Rewriting Communications Regulation From the Bottom Up*, 1 J. TELECOMM. & HIGH TECH. L. 95 (2002); Philip J. Weiser, *Law and Information Platforms*, 1 J. TELECOMM. & HIGH TECH. L. 1 (2002); Kevin Werbach, *A Layered Model for Internet Policy*, 1 J. TELECOMM. & HIGH TECH. L. 37 (2002); Richard S. Whitt, *A Horizontal Leap Forward: Formulating A New Communications Public Policy Framework Based on the Network Layers Model*, 56 FED. COMM. L.J. 587 (2004); J. Scott Marcus, *The Potential Relevance to the United States of the European Union's*

the FCC would have to extend its information service classification to other services made available to end users on a retail basis via information service classified DSL and cable modem links, including VoIP and video services delivered via the Internet, commonly referred to as Internet Protocol Television ("IPTV"). These services compete with and constitute the functional equivalent of legacy services heretofore subject to common carriage telecommunications service regulation for voice telephony and cable television regulation. If the information service classification extends vertically up to software applications, then the FCC will have created a deregulated safe harbor for just about any service or software application carried via DSL and cable modem links, regardless of its functional equivalency with legacy, regulated services.

The FCC has already begun to realize the quandary it has created for itself by fashioning such an elastic and expanding safe harbor. Now bereft of Title II jurisdiction over Internet access and Internet-mediated services, the Commission has resorted to Title I of the Communications Act, as amended, to retain an "ancillary" regulatory hook if and when necessary. The Commission already has applied this exception to the information service regulatory safe harbor by requiring VoIP service providers to contribute to universal telephone service funding, to make available emergency 911 access available and to cooperate with law enforcement officials. The Commission has rationalized its imposition of quasi-common carrier, telecommunications service regulation by invoking broad notions of the public interest, by making a distinction between how different laws define telecommunications,[113] and by making a questionable

Newly Adopted Regulatory Framework for Telecommunications, Federal Communications Commission, Office of Plans and Policy Working Paper Series No. 36 (July 2002), *available at* http://www.fcc.gov/osp/workingp.html (last visited Nov. 28, 2007); Douglas C. Sicker, *Further Defining a Layered Model for Telecommunications Policy* (2002) (unpublished paper *available at* http://intel.si.umich.edu/tprc/papers/2002/95/LayeredTelecomPolicy.pdf).

[113] Communications Assistance For Law Enforcement Act, 47 U.S.C. § 1001(8)(B)(ii) (1994) defines a "telecommunications carrier" as "a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem

differentiation between the use of telecommunications to transport bits corresponding to an information service and the use of telecommunications to transport bits corresponding to retail telecommunications services.[114]

The FCC may yet again face close judicial scrutiny and reversal for creating a regulatory safe harbor only to chip away at it. First, the Commission may have unlawfully stretched its general public interest mandate under Title I of the Communications Act. *American Library Ass'n. v. FCC* already evidences a court's unwillingness to endorse the FCC's unilateral expansion of its regulatory mission absent express Congressional authority. Second, the Commission may not persuade reviewing courts that ancillary jurisdiction, under Title I, as opposed to conventional telecommunications service jurisdiction, under Title II, should apply to Internet services, such as VoIP, particularly in light of the Commission's selective imposition of telephone company regulations on VoIP service providers. Third, the Commission's telecommunications versus telecommunications service distinction, may not pass muster with reviewing courts in light of the fact that telecommunications bitstream delivery occurs in the very same way for both telecommunications services and information services.[115]

The information service provider classification serves the FCC's interest in safeguarding the Internet from conventional telecommunications service regulation, despite several instances

such a person or entity to be a telecommunications carrier for purposes of this subchapter." The FCC has interpreted this section as requiring the Commission "to deem certain service providers to be telecommunications carriers for CALEA purposes even when those providers are not telecommunications carriers under the Communications Act of 1934, as amended." In re Commc'ns Assistance for Law Enforcement Act and Broadband Access and Servs., 20 F.C.C.R. 14989, 14991 (2005).

[114] *See generally* Rob Frieden, *What Do Pizza Delivery and Information Services Have in Common? Lessons From Recent Judicial and Regulatory Struggles with Convergence*, 32 RUTGERS COMPUTER & TECH. L.J. 247 (2006) [hereinafter Frieden, *Pizza Delivery*].

[115] In Nat'l Cable & Telecomms. Ass'n v. Brand X Internet Servs., 545 U.S. 967, 1003 (2005) the Supreme Court affirmed the FCC's regulatory distinction between telecommunications and telecommunications services primarily on procedural grounds that favor judicial deference to expert regulatory agency decision making articulated by the Court in Chevron U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837 (1984). *See also* Frieden, *Pizza Delivery*, *supra* note 114, at 258.

where the FCC had selectively re-regulated some information services. However the FCC's emphasis on non-regulation results from its conclusion that ISPs do not operate and should not have to operate as common carriers, i.e., that ISPs need not operate as neutral conduits. ISPs can violate any principle of network neutrality and arguably still retain their largely unregulated status. On the other hand the DMCA, while not mandating common carriage, does require ISPs to operate in a manner that evidences no involvement with the content they carry. Accordingly when such traffic management occurs, an ISP may not have crossed the line into regulated telecommunications services, but it still may lose its copyright safe harbor exemption.

III. WHAT CONSTITUTES ACTUAL KNOWLEDGE OF COPYRIGHT INFRINGEMENT?

Common carriers operate as neutral conduits and typically carry content created by others. Conversely, ISPs can offer varying degrees of neutrality and can readily combine conduit with content the ISP creates and that created by others. For telecommunications common carriers actual knowledge about criminal and harmful content cannot exist, because the carrier never examines content absent an external directive such as a court order. For ISPs actual knowledge can occur when an ISP engages in deep packet inspection. However the ISP might claim that deep packet inspection provides only information sufficient for the ISP to know how to classify, switch, route and process traffic without actual knowledge of whether by transporting a particular bitsream the ISP has facilitated copyright infringement.

Answers to the questions whether, how, and when an ISP acquires actual knowledge of copyright infringement largely depend on what can and will become standard information contained in Internet packet headers. Arguably ISPs can limit their deep packet inspection to that minimally intrusive level needed to monitor traffic for purposes of "proper" and "routine" classification, switching, routing and processing. Under this scenario an ISP might ignore copyright information, i.e., take no affirmative steps to protect the copyright holder, and simply carry

packets containing headers that have copyright usage information that may impact how receivers of a file can use, copy, and resend the file.

Some types of DRM can provide enhanced copyright protection without any affirmative efforts by the ISP providing the link between sender and recipient. If this type of DRM becomes an industry standard, then ISPs possibly could transmit without any meddling, scrutinizing or processing, packets containing DRM instructions for processing by equipment on user premises. Simultaneously the ISP could use deep packet inspection to act on other information contained in the header to effectuate non-neutral networking.

A. Do ISPs Have an Affirmative Duty to Process DRM Restrictions on Use and Copying?

The possibility exists that standard DRM techniques may evolve to a point where they require some degree of intervention by the ISPs in advance of, or in lieu of processing by end user equipment. Contrary to passively transmitting DRM instructions and other types of safeguards, ISPs under this scenario would have to apply deep packet inspection, or some other form of header examination method, to make DRM processing successful. Such active examination of traffic raises both intellectual property rights and privacy questions. While an ISP may have a right to control copyright infringing behavior, does this control justify packet inspection to effectuate such a right? Likewise does deep packet inspection, or other forms of header examination, confer on ISPs the ability to prevent and otherwise control copyright infringement? Bear in mind that ISPs heretofore have demonstrated the right and ability to remedy copyright infringement only after the fact and in response to copyright holders that have performed the necessary forensic examination to determine who has infringed.[116] Deep packet inspection might

[116] 17 U.S.C. § 512(c)(3)(ii–iv) (1999) of the DMCA establishes burdens on copyright holders to identify copyright infringers before an ISP has any affirmative obligation to take down infringing content. *See, e.g.*, Hendrickson v. eBay, 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (holding that even though the eBay web site offered sale of pirated video

provide the ability to provide some degree of contemporaneous DRM, quite possibly on an automated basis once the ISP detects or has received notification by copyright holders of infringing activity.

The DMCA does not require ISPs to monitor their networks, or seek facts indicating the existence of infringement to qualify for the copyright safe harbors. On the other hand the DMCA also requires ISPs not to interfere with any "standard technical measures"[117] used to identify and protect copyrighted works. It appears that ISPs may not block or fail to transmit copy protection and other DRM safeguards that become effective once transmitted to end users' computers. However, the DMCA does not appear to require ISPs to deploy deep packet inspection, or to retrofit any sort of packet examination they employ to add DRM enforcement and copyright infringement detection capabilities.

The absence of an affirmative obligation to enforce DRM may not extend to a scenario where ISPs readily can use deep packet inspection to perform traffic and QOS tiering as well as copy protection as standard operating procedure. Arguably ISPs satisfy the right to control copyright infringement when they reserve the option of inspecting the traffic of subscribers as well as transit and peering traffic generated by other ISPs. ISPs might also have the ability to control such activity in light of the promising array of DRM, traffic management, and service diversification options offered by next generation Internet routers.

IV. NON-NEUTRAL NETWORKS AND THEIR ADVERSE IMPACT ON FAIR USE

An ISP deciding to operate a non-neutral network, willingly installs hardware and software that automatically makes binding decisions about how the ISP will manage specific bitstreams. This traffic management function can include decisions whether to block or complete delivery of packets to an intended recipient.

content, the plaintiff's written notifications did not comply with all DMCA requirements).

[117] 17 USC § 512(i)(1)(B).

When network management includes decisions about the use, copying, and sharing of content hardware and software substitute for people and impose new ex ante limitations instead of after the use examination whether infringement has occurred. Using technological intermediaries in lieu of human decision makers risks expanding DRM to a point where hardware and software operate as proxy censors[118] as well as repressors of fair use.[119]

Fair use in an offline environment involves empirical and value judgments based on somewhat ambiguous criteria: "The copyright law, although carefully worded, simply cannot be expressed in the kind of algorithmic language that is required of computer programs to automate functionality like printing or copying. This is especially true of 'fair use' . . . a deliberately vague exception to the monopoly rights of the copyright holder."[120]

Empowering hardware and software to establish and enforce a priori fair use policies usurps decision making by individuals and vests it with an intermediary that has every incentive to take the path of least resistance and lowest cost: "[I]f it is costly to distinguish protected from unprotected speech, the proxy censor is likely to abandon the effort to avoid errors and adopt a conscious policy of prophylactic self-censorship that blocks any content that could precipitate the threat of sanctions."[121]

---

[118] "To the extent that potential regulators can induce [providers of Internet equipment and services] to disrupt communications, whether by blocking payment to targeted websites, or by embedding obstacles to communication and mechanisms of surveillance in the hardware or software that facilitates communication, they can spawn effective proxy censors." Seth F. Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PA. L. REV. 11, 17 (2006).

[119] DRM technologies create "a burden of obtaining consent that has no parallel in the offline world. . . . [E]very permissions-based DRM implementation (in which the user must formally acquire some form of explicit authorization to engage in a particular use of the protected work) simply reproduces a variant of the 'judge on a chip' problem. No such system can ever replicate the experience of fair use in the offline world because the requirement of *ex ante* authorization by the copyright holder or its designee is a departure from offline practice and statutory requirements." Timothy K. Armstrong, *Digital Rights Management and the Process of Fair Use*, 20 HARV. J.L. & TECH. 49, 54 (2006).

[120] *Id.* at 52.

[121] Kreimer, *supra* note 118, at 28.

CONCLUSION

In light of the new profit centers available to non-neutral Internet networks, most ISPs soon will acquire and install routers with deep packet inspection capabilities. Having made the decision to abandon network neutrality, ISPs may have to calibrate their networks with greater precision to block copyright infringing traffic. Arguably the DMCA provides a safe harbor exemption from liability only when the ISP's costs associated with traffic scrutiny and management exceed the social benefits accruing from reduced piracy.

Given the risk of losing a safe harbor, ISPs likely will err on the side of accommodating DRM cooperation requests from copyright holders. ISPs probably will collaborate with copyright holders perhaps going so far as to program hardware with deep packet inspection software that achieve both traffic management goals, to pursue price and QOS diversification, as well as DRM, to mollify copyright holders. Should this scenario play out the current network neutrality debate will have addressed not only the future accessibility of the Internet to users and content providers, but also the future nature and scope of consumers' fair use opportunities to access, copy, and resend content available via the Internet.

Some network neutrality opponents reject the likelihood that a non-neutral network will occur,[122] while others claim that the Internet never was neutral in the first place.[123] Opponents to network neutrality do not appear to have considered whether and how hardware and software primarily installed to provide tiered and differentiated bit transport services, also will have an impact on consumers' access to content.[124] A non-neutral World Wide Web will have substantial and direct impact on both the conduit

---

[122] *See, e.g.*, NETCompetition.org, http://www.netcompetition.org (last visited Nov. 28, 2007).

[123] *See, e.g.*, *supra* note 90.

[124] *See* Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253 (2006) (noting the ability of software and software authors to serve as powerful intermediaries capable of achieving greater regulation and control of endpoint platforms such as personal computers); *see also* Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 669–70 (2003).

portion of the Internet and the content traveling via the conduit. When an ISP chooses to operate a non-neutral conduit, the ISP, internationally or not, should incur greater responsibility for the content it carries.[125]

[125] *See* David V. Richards, *Posting Personal Information on the Internet: A Case for Changing the Legal Regime Created by § 230 of the Communications Decency Act*, 85 TEX. L. REV. 1321, 1336–37 (2007); Karen Alexander Horowitz, *When is § 230 Immunity Lost?: The Transformation from Website Owner to Information Content Provider*, 3 SHIDLER J.L. COM. & TECH. 14, 14 (2007); Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 257 (2006); Michael L. Rustad & Thomas H. Koenig, *Rebooting Cybertort Law*, 80 WASH. L. REV. 335, 373–74 (2005).