Internet Copyright Infringement and Service Providers: The Case for a Negotiated Rulemaking Alternative

I. INTRODUCTION

The Internet has risen from obscurity to ubiquity virtually overnight. Although the Internet was not opened to the public until 1990,[1] as of February 1998, an estimated 62 million adults in the United States (30% of the adult population) had Internet access.[2] Similarly, although the World Wide Web is only seven years old, it is estimated to already contain over 150 million documents (some 50 to 60 *billion* words).[3] Electronic mail may now be sent to 186 countries around the globe.[4] The Internet promises to be the exiting new technology that will help "build a bridge to the twenty-first century."[5]

The power of the Internet lies in its ability to distribute information around the globe with unprecedented speed and efficiency. Unfortunately, "friction-free markets and friction-free piracy run in tandem."[6] Consequently, intellectual property theft on the Internet has reached epidemic proportions. Pirated copies of computer software and "cracker" utilities used to defeat software copy-protection schemes are widely available.[7] Copyrighted images and literary works are routinely

[1] Robert H Zakon, *Hobbes' Internet Timeline v3.1* (visited Feb. 1, 1998) <http://info.isoc.org/guest/zakon/Internet/History/HIT.html>.

[2] *Latest Intelliquest Survey Reports 62 Million American Adults Access the Internet/Online Services* (last modified Feb. 5, 1998) <http://www.intelliquest.com/about/release41.htm>.

[3] Gus Venditto, *Search Engine Showdown*, INTERNET WORLD, May 1996 <http://www.internetworld.com/1996/05/showdown.html>.

[4] David Zgodzinski, *Third-World Internet*, INTERNET WORLD, Nov. 1996 <http://lib.nmsu.edu/staff/mmolloy/lsc311/3rdwrld.txt>.

[5] The theme of the 1996 Clinton/Gore Presidential campaign.

[6] David McCandless, *Warez Wars*, WIRED, Apr. 1997, at 178 <http://www.wired.com/wired/5.04/warez/ff_warez.html>.

[7] On March 16, 1998, a Web search using the "AltaVista" Internet search page (<http://www.altavista.digital.com>) and using the search term "warez" (Internet slang

displayed and copied, both in intentional and unknowing violation of their owners' rights. Bootleg copies of sound recordings, video, and other multimedia works are increasingly being exchanged on the Internet.[8]

The software industry has been hit particularly hard since it "empowers every customer to become a manufacturing subsidiary . . . the user of each and every piece of software has all of the capability to make a perfect copy."[9] The Internet has compounded this problem by providing software pirates with an instant international distribution channel. "Instead of reaching the limited number of people who can crowd around a card table at a flea market, pirates can peddle their wares to tens of millions of on-line users around the world."[10]

The magnitude of losses due to online infringement has defied accurate measurement. For instance, while total worldwide computer

for pirated software) produced 37,349 documents, up from 6,343 documents in November 1996. Web sites hosting information and utility programs used to defeat software copy protection systems can be easily found using a Web search with the terms "cracks," "crackz," "codez," "serials," or "serialz."

Usenet (*see infra* Part II.C.4) and Internet Relay Chat (*see infra* Part II.C.3) also have many public groups for the exchange of pirated software, cracks, and serial numbers.

[8] An increasing problem is the unauthorized distribution of music recordings, made possible by recent advances in software that allow the songs to be more efficiently transmitted and stored. *See, e.g.*, Janelle Brown, *Heat Turned Up on Digital Music Pirates* (last modified Feb. 12, 1998) <http://www.wired.com/news/news/culture/story/10234.html>. Further advances in technology will soon make it more practical, and thus more common, to use the Internet to exchange other works such as films and multimedia works.

> Today, Internet piracy focuses on computer programs, video games, and recorded music. Movies and videos are not much in evidence—yet. That's because our audio-visual content is so rich in information that it can't yet move easily everywhere in the digital network—the volume of flow is too great for some of the pipes. We know that the reprieve is temporary, however. The same technology that will smooth the way for legitimate delivery of video on demand over digital networks will also prime the pump for copyright pirates.

Prepared Testimony by Jack Valenti, Pres. and CEO, Motion Picture Ass'n of Am., Before the House Judiciary Comm., Subcomm. on Courts and Intellectual Property: WIPO Copyright Treaties Implementation Act and the Online Copyright Liability Limitation Act, Federal News Service, Sept. 16, 1997, available in LEXIS, Legis Library, Fednew File [hereinafter *Valenti Testimony on H.R. 2180 & H.R. 2281*].

[9] Brain S. McWilliams, *PC World Online News Radio: Pirates Among Us* (visited Feb. 11, 1998) <http://www.pcworld.com/news/newsradio/wasch/index.html> (interview with Ken Wasch, Pres., Software Publishers Ass'n) (RealAudio-encoded sound file) [hereinafter *Ken Wasch interview*].

[10] Bob Kruger, *Statement by Bob Kruger, BSA VP for Enforcement on the Threat of Internet Piracy* (visited Feb. 12, 1998) <http://www.bsa.org/piracy/internet/internet_sta.html>.

software industry losses are estimated at over $13 *billion* annually,[11] various estimates have placed the contribution of online piracy at anywhere from one third of the total losses to a relatively insignificant portion of the total losses.[12] An inherent problem with measuring losses due to online infringement is that each pirated copy does not represent a lost sale. Many pirates collect copyrighted works "for the sheer thrill of it."[13] "Pirates are like street gangs rooting around nests of copied programs just to see what is there, and copying them like trading card hobbyists, for show, not for any practical purpose."[14] Perhaps the biggest problem with Internet piracy, however, is that it is an "insidious problem."[15] Widespread and open copyright abuse, it is feared, will establish a systemic cultural disregard for authors' intellectual property rights: "The reason we go after pirates is to clean up the Internet for commerce, otherwise anarchy reigns."[16]

Internet piracy has therefore justifiably been the source of increasing alarm among intellectual property authors. Congress has yet to decide the issue and the few court decisions involving online copyright violations have failed to produce a clear consensus as to how copyright doctrine should apply to service providers. Many copyright holders and commentators assert that the best solution is to hold Internet service

[11] *Business Software Alliance Statistics* (visited Feb. 12, 1998) <http://www.bsa.org/piracy/diduknow.html> (figures based on study of 1996 worldwide losses).

[12] *Compare* McCandless, *supra* note 6, at 133-34 (estimates ranging from one third to twelve percent of total losses) *with Ken Wasch Interview*, *supra* note 9 ("I don't think that [Internet piracy is] a big source of lost profits in the industry. . . . We lose some opportunity, but [individuals are] not where the largest loss to the industry is.").

[13] Deborah Shapley, *Corporate Internet Police Hunt Down E-Pirates*, N.Y. TIMES CYBERTIMES (last modified May 19, 1997) <http://www.nytimes.com/library/cyber/week/051997police.html>. *See also* McCandless, *supra* note 6, at 135 ("They pirate software because they can. It's a game . . . It's a hobby, like stamp collecting. It's an act of bloodless terrorism. And it's an addiction."); *Statement of Sandra Sellers, Vice Pres. of Enforcement and Education, Before the Subcomm. on Courts and Intellectual Property, Comm. on the Judiciary, U.S. House of Representatives Oversight Hearing on Electronic Copyright Piracy and Legislative Hearing on H.R 2265, The "No Electronic Theft (NET) Act"* (last modified Sept. 11, 1997) <http://www.house.gov/judiciary/4025.htm> [hereinafter *Sellers Statement on H.R. 2265*] ("The Internet has given rise to another type of pirate, the consummate 'hacker' or 'warez' aficionado, who copies and distributes computer software simply for self-aggrandizement—the reputation, the thrill, the 'fun' of having the latest programs or the biggest 'library' of 'warez' titles.").

[14] Shapley, *supra* note 13.

[15] *Ken Wasch Interview*, *supra* note 9.

[16] Brown, *supra* note 8 (quoting Jim Griffin, Dir. of Tech., Geffen Records).

providers liable for user misconduct, forcing them to clean up the Internet. Service providers counter that the growth of the Internet will be impeded if they are held liable for harms that they are powerless to prevent. A new legal framework is needed that will address the concerns of both groups.

> Crime is rampant out here in the new frontier of cyberspace. But unlike the pioneers of the Wild West, you won't hear guns shots or shouts for help; the Internet crime wave is shrouded in the silent circuitry of the global computer network.
>
> . . . .
>
> The law always lags behind the development of new frontiers, but both legislation and enforcement of electronic rights will have to develop quickly if the Internet is ever to prosper as mass medium, if cyberspace is truly to become the planet's incubator of ideas, information and communications. Without suitable protection, the people and companies who invest their time and resources in creative work will have no incentive to help settle this frontier.[17]

Those who wish to settle this new frontier must first understand it. A thorough knowledge of Internet technology is crucial to arriving at workable policies that will promote the growth of the Internet as a content-rich and productive medium. Unfortunately, most scholarly analysis involving online copyright infringement has exhibited a fundamental lack of understanding of the subject matter. Similarly, although most courts considering Internet issues have at least made a laudable effort to become more familiar with the technology,[18] their decisions have nonetheless frequently been grounded upon incorrect facts and faulty assumptions and have failed to provide clear answers to the

[17] Michael Baroni, *Rounding Up the Posse in a Lawless Frontier*, N.Y. TIMES CYBERTIMES (last modified June 8, 1997) <http://www.nytimes.com/library/cyber/week/060897lawless.html>.

[18] The background section on Internet technology in *ACLU v. Reno* occupied 21 of the opinion's 59 pages (subtracting headnotes). 929 F. Supp. 824, 830-50 (E.D. Pa. 1996). The technical background section in *Shea v. Reno* occupied 11 of the opinion's 29 pages (subtracting headnotes). 930 F. Supp. 916, 925-35 (S.D.N.Y. 1996). Although not separated from the other text of the opinion, technological background material constituted a similar proportion of the opinion in *Religious Tech. Ctr v. Netcom Online Communication Servs., Inc.* 907 F. Supp. 1361 (N.D. Cal. 1995).

These technological findings of fact have been so extensive as to have prompted one reporter to describe the 21-page section in *ACLU v. Reno* as "one of the most lucid primers about the Internet yet seen." Peter H. Lewis, *Internet Primer Written by and for Newbies*, N.Y. TIMES CYBERTIMES (last modified June 18, 1996) <http://www.nytimes.com/library/cyber/compcol/0618compcol-lewis.html> ("newbie" is Internet slang for "beginner"). Mike Godwin, staff attorney for the Electronic Frontier Foundation, one of the plaintiffs in *ACLU v. Reno*, was similarly impressed with the District Court's "far-reaching—even visionary – decision." Mike Godwin, *Sinking the CDA*, INTERNET WORLD, Oct. 1996, at 108 (also noting that the "legally relevant facts about how the Net works and how it is used" outlined in the opinion "seem likely to impose strong legal and practical limits" on the Supreme Court's ability to overrule the District Court).

service provider liability question. Likewise, the few laws that Congress has passed in response to the Internet have been widely criticized as technically unworkable[19] and the Congressional testimony to date on the bitterly divisive issue of service provider liability shows that witnesses on both sides of the issue have frequently presented Congress with testimony comprised of equal measures of fact and hyperbole.

This Comment argues that the Internet service provider liability debate should be settled with a regulatory approach. Not only is the technical expertise required to create workable policies beyond the capability of the courts, but also the subject matter itself is wholly statutory and, thus, appropriately resolved by Congress. In addition to providing much-needed legal certainty, a negotiated rulemaking approach would replace the current contentious environment characterized by litigation, blame shifting, and positional thinking with a forum that inspires compromise and creative thinking, thus providing the best opportunity for the development of realistic, efficient, and fair solutions to the Internet service provider liability debate.

[19] *See, e.g.*, Byron F. Marchant, *On-Line on the Internet: First Amendment and Intellectual Property Uncertainties in the On-Line World*, 39 HOW. L.J. 477 (1996).

> At present, it appears that many jurists and politicians, as well as the regulators that they influence, are attempting to provide patch-work responses to issues arising in the on-line world—responses that are likely to do more harm than good, that may be difficult to enforce, and that are unlikely to resolve the problem identified. Many politicians and regulators have no personal experience with the on-line world or know how to use their computers on the Internet.

Id. A CNN Online report described similar criticism of the negotiators at the December 1996 international copyright protection conference sponsored by the World Intellectual Property Organization:

> The group of telecommunications companies, including AT&T, MCI, Netscape, America Online and CompuServe, said all three proposed [World Intellectual Property Organization copyright] treaties have features that are ill-advised, and that the people who are to decide on the law know nothing about cyberspace.
>
> "Not only do these people not understand the technology, but they actually have no experience of Internet at all," said Barbara Dooley, head of Commercial Internet Exchange Association. "The ideas they're working with are not 21st century yet."

Communications Industry: Copyright Laws Will Ruin Internet (visited Jan. 12, 1997) <http://www.cnn.com/TECH/9612/06/internet.copyright/index.html>. Similarly, a software company executive expressed little faith in the ability of a judge to deal with these complicated technological issues: "Bringing Internet cases through the judicial system is a nightmare . . . Try talking to a judge about 'dynamically assigned IP addresses.' We don't have a chance." McCandless, *supra* note 6, at 133, 177.

Part II will introduce the fundamentals of computer communications, distinguishing bulletin board services, Internet service providers, and online services; describing the basic architecture of the Internet; and identifying the primary Internet services and how each is used to facilitate online copyright infringement. Part III will highlight the difficulty that courts have faced in addressing this conceptually new and technologically complex subject by providing a review and analysis of the recent reported decisions related to service provider copyright liability. Part IV will introduce the arguments for imposing strict liability on service providers and will then analyze the economic and social consequences of shifting incentives to prevent infringement on service providers. Finally, Part V will recommend a regulatory solution to both the service provider liability question and the larger question of how to prevent online infringement, arguing that a comprehensive approach involving statutory changes and regulatory oversight of Internet service providers will provide for the optimum distribution of economic incentives, thereby making possible the development of systems that can minimize losses to both content providers and service providers.

II. AN OVERVIEW OF INTERNET TECHNOLOGY

To those without an understanding of the Internet, cyberspace can seem as intimidating and threatening as it does promising. Even most experienced Internet users do not understand the underlying technologies of the Internet. Indeed, many Internet visionaries and computer market leaders see information services as a future utility that will delivered by user-friendly "information appliances" and are therefore making a conscious effort to keep information technologies transparent to the average user.[20] This school of thought properly recognizes that we should not need to know how the entire telephone system works in order to place a phone call.

While there may be little utility in requiring the average Internet user to understand its technological architecture, it is essential that our lawmakers have such an understanding. Knee-jerk legislative reactions by uniformed lawmakers will only add to the growth-stifling uncertainties about the future of the Internet. As one Internet publishing executive noted: "This legislative time-gap between what politicians

[20] *See infra* text accompanying notes 267-70 (describing the "network computing" movement).

understand well enough to regulate and what is technologically operative today is an abyss of potential legal and financial risk."[21]

If the Internet is to live up to its potential, lawmakers must recognize that "cyberspace" isn't at all like interstellar space. Whereas interstellar space is a void, cyberspace is a finite, but complicated, system of computers, wires, and people. Congress must avoid an overly simplistic view of cyberspace if it is to craft effective laws that will help define and add certainty to the unique and often delicate relationships between the entities that collectively comprise cyberspace.

A. Distinctions between Bulletin Board Services, Internet Access Providers, and Online Services

Before the recent rise in popularity of the Internet, most computer communications were accomplished using bulletin board services. As a result, much of the legal precedent and commentary involving computer communications has been based on bulletin board service technology. The technological architecture of Internet, however, is dramatically different from that of a bulletin board service.

1. Bulletin Board Services

A bulletin board service (BBS) is a central computer that serves as an electronic message center.[22] A caller reaches a BBS by dialing in directly to the BBS host computer, or "server."[23] Since most BBSs are

[21] Bill Washburn, *No Slam Dunk*, INTERNET WORLD, Mar. 1996, at 32, 33 <http://www.internetworld.com/1996/03/imo.html>.

> Given the chaotic and free-wheeling nature of the Net, more than a few government leaders and bureaucrats around the globe are likely to take various drastic actions. Many people seek to preserve the familiar. The threat to the status quo implicit in the Internet constitutes what many fear is change run amok.

Id.

[22] *See generally The BBS Corner - What BBSes Are All About* (last modified Jan. 1, 1998) <http://www.thedirectory.org/diamond/about.htm>; *The BBS Corner - Frequently Asked Questions* (last modified Jan. 1, 1998) <http://www.thedirectory.org/diamond/ faq.htm>.

[23] It is, however, possible to dial in to one BBS and to use a communications service such as Telnet to reach another BBS from there. *See* Adam Gaffin, *EFF's Guide to the Internet, v. 3.15*, § 6.4 (visited Apr. 14, 1998) <http://www.eff.org/papers/eegtti/>.

either private or commercial enterprises, a BBS operator, or "Sysop,"[24] typically controls access by requiring callers to enter a user name and password, which are provided only to those who have paid the subscription fee and/or been approved. Callers to a BBS can play online games, communicate with other users in "chat rooms," send ("upload") and retrieve ("download") files, and send ("post") or retrieve messages. The software packages used to run BBS servers are proprietary and non-standardized, so the services available on any given BBS are defined both by the capability of the software used and by the Sysop's choice as to which of the available services he wishes to enable.

2. *Internet Access Providers*

Although some users may be able to connect to the Internet through schools, libraries, and even businesses, most users access the Internet from home using a commercial service provider,[25] either an online service or an Internet access provider (IAP). IAPs range in size from large commercial providers like AT&T's Worldnet Service and Netcom to small local providers with perhaps only a hundred accounts. Connecting to an IAP is quite similar to connecting to a BBS; the caller instructs his computer to call the IAP's remote host computer and is then required to provide his unique user name/password combination. Once the user is logged on to an IAP, however, the similarities end. An IAP's communications server provides no services of its own; it merely provides a gateway to the Internet, allowing the caller to access the virtually unlimited range of available Internet services by connecting to an Internet server hosting that service. IAPs, therefore, do not provide content; they merely provide *access* to content located elsewhere.

Due to the vastly greater audience, reach, and flexibility of the Internet, BBSs are becoming obsolete and their numbers are dwindling.[26] Since each Internet server functions much like a BBS server, and there are thousands of Internet servers available from a single

[24] As used throughout this Comment, the term "Sysop" is intended to generically refer to the person or organization responsible for administering a server.

[25] Seventy percent of all Internet access is done from the home. *Latest Intelliquest Survey Reports 62 Million American Adults Access the Internet/Online Service*, *supra* note 2. *See also* Information Technology Association of America, *Intellectual Property Protection in Cyberspace: Towards a New Consensus*, § 2 (visited Oct. 15, 1997) <http://www.itaa.org/copyrite.htm> [hereinafter *ITAA Discussion Paper*].

[26] *See* David H. Dennis, *The Inet-Access Frequently Asked Questions List*, § 10.13 (last modified Dec. 23, 1996) <http://www.amazing.com/internet/faq.html> ("The BBS world as a whole seems to be dying with the dominance of the Internet").

connection to an IAP, the IAP's "on-ramp" to the Information Superhighway has largely replaced the closed environment of BBSs.[27]

3. Online Services

Online services (such as America Online and CompuServe) are somewhat of a hybrid between an IAP and a BBS. They not only provide Internet access like an IAP, but they also provide their own proprietary value-added services like a BBS. Once connected, the caller has access not only to the online service's host computers, but also has access to the other remote Internet servers. Although the number of users connecting to the Internet through online services continues to grow in absolute terms, they are quickly losing market share to the more direct connection offered by IAPs.[28]

As opposed to IAPs, online services allow the user access to a broad array of content provided by the online service itself. This simple but often overlooked distinction is critical to a meaningful analysis of service provider liability. This Comment is primarily concerned with the legal questions surrounding liability for *user*-supplier content. Therefore, value-added service providers like BBSs and online services, to the extent that they provide their own content, are beyond the scope of this article, since existing legal doctrines are largely sufficient to address issues related to *provider*-supplied content.

As will be discussed further, the degree to which a provider has both the right and ability to exert control over user content is often a critical legal distinction. At one extreme are BBSs, which provide subscribers

[27] Some BBSs have begun to add "gateways" (access) to Internet services. *See id.* To the extent that they do so, they begin to resemble an online service (discussed in the next section).

[28] Most of the content and services that could formerly only be found on an online service can now be found on the Internet:

> [J]ust two years ago, the common wisdom was that the future of on-line activity would be driven by multi-faceted on-line service providers such as Prodigy, CompuServe and America Online. Today, the focal point is no-frills Internet access. Rapid enhancements and improved ease of use of the Internet and World Wide Web are making the services offered directly by the access provider far less critical.

Prepared Testimony of Ken Wasch, Pres., Software Publishers Ass'n, Before the House Judiciary Comm., Courts and Intellectual Property Subcomm., Federal News Service, Sept. 16, 1997, *available in* LEXIS, Legis Library, Fednew File [hereinafter *Wasch Testimony on H.R. 2180*].

with access to content physically contained in the mass storage devices of their servers. This access provides BBS Sysops with some *ability* to control the content and, since the content has been supplied either by the Sysop or a BBS subscriber, BBS Sysops typically have the *right* to remove content.

At the other extreme are IAPs, which only provide access to content resident on servers located outside their system. Since an IAP has no physical access to the information resident on servers located outside its system, it has neither the right nor the ability to control that content.

The primary shortcoming of this polar classification, however, is that IAPs typically provide more than simple access to the Internet. Most IAPs also operate servers in order to provide their subscribers with basic Internet services such as e-mail, Usenet news, and Web page hosting.[29] Thus, the term "Internet service provider" (ISP) is a more accurate description of most IAPs. "ISP," as used throughout the remainder of this Comment, is meant to encompass both providers that offer only access to the Internet and those that also operate Internet servers.[30]

B. What is "the Internet?"

The Internet may justifiably seem quite daunting. Although, like most fields in high technology, Internet technology is expressed in a strange language consisting of an alphabet soup of acronyms and complex technical jargon,[31] the basic concepts are quite simple. It is not a

[29] Observations based upon an October 4, 1997 examination of "the List," a comprehensive Internet service provider database located at <http://thelist.internet.com/>. *See also ITAA Discussion Paper, supra* note 25, § 2.

Since, like BBS Sysops, ISP Sysops have access to the content resident on their Internet servers, it may seem reasonable to equate the responsibilities of ISP Sysops and BBS Sysops. For reasons more fully developed later in this Comment, however, such a classification would be overly simplistic.

[30] "Internet service provider" may have also have other meanings, as there are many different organizations that provide Internet-related "services." A provider supplying Web site hosting is often referred to as an Internet presence provider (IPP). The regional and national commercial networks that supply network access points to IAPs are also referred to as "service providers." Finally, the Sysops of Internet servers are also sometimes referred to a "service providers." As used throughout this Comment, the term "Internet service provider" is meant to encompass all of these categories.

[31] This strange language was the source of both frustration and entertainment for the Philadelphia District Court judges who were required to decide the recent challenge to the Communications Decency Act:

> To decide who is right, the three judges last week sat through two days of dense testimony, much of it peppered with highly technical computer terms.
>
> The confusing array of acronyms in computer parlance—FTP, HTTP, HTML, TCP/IP and what have you—quickly became a source of amusement to the judges. "Oh, an abbreviation!" exclaimed a delighted Stewart Dalzell, a Federal district court judge on the special panel, upon learning that "bot"

commercial entity, or really even an entity at all. Like the international telephone system, the Internet is merely a network of interconnected networks. The Internet is the result of a series of agreements between the institutional owners of large networks. There is no central governing body. Operational policies and technical standards are set by three international volunteer groups.[32]

Starting in the 1960's from a single network with just a few computers, the Internet has gradually added new commercial networks. These core networks, called the Internet "backbones," are high-speed data pipelines, interconnected with one another to form the heart of the Internet.[33] Although network interconnections are often made at other intermediate points, in general, national networks connect to the backbones, smaller regional networks connect to the national networks, Internet service providers connect to the regional networks, and businesses and consumers connect to ISPs. In 1992, there were less than a million host computers and less than 7,000 networks connected to the Internet, but by the end of 1997, the Internet had grown to almost 20 million hosts and more than 1.3 million *networks*.[34]

was not another acronym, but merely short for "robot."

Pamela Mendels, *Awash in Cyberspace Jargon, Judges Remained Good Sports*, N.Y. TIMES CYBERTIMES (last modified Mar. 24, 1996) <http://www.nytimes.com/library/cyber/week/0324notebook.html> (discussing American Civil Liberties Union v. Reno, 929 F. Supp. 824 (E.D. Penn. 1996)).

[32] *See generally* E. Krol & E. Hoffman, *RFC 1462: FYI on "What is the Internet?"* (last modified Apr. 15, 1996) <http://www.internic.net/nic-support/fyi/fyi20.html> (providing overview of Internet governance). The Internet Society (ISOC) (*see* (visited Apr. 14, 1998) <http://info.isoc.org/index.html>) is responsible for the global cooperation and coordination of the Internet; it is the ultimate authority that sets the overall policies that shape the future of the Internet. The Internet Architecture Board (IAB) (*see* (visited Apr. 14, 1998) <http://www.iab.org/iab/>), specially appointed members of the ISOC, decides on the essential hardware and software standards. Policies that govern relations between the network owners are handled by the Internet Engineering Task Force (IETF) (*see* (visited Apr. 14, 1998) <http://www.ietf.cnri.reston.va.us/home.html>), a voluntary association of network designers, operators, vendors, and researchers.

[33] *See generally* Jack Rickard, *Internet Architecture* (visited Feb. 1, 1998) <http://www.boardwatch.com/isp/fall97/intarch.html> (providing detailed explanation of the backbone networks and their history). For a graphical map of one U.S. backbone, as well as links to U.S. its regional and global networks, see *The UUNET U.S. Backbone* (visited Feb. 26, 1998) <http://www.uu.net/lang.en/network/current/us.shtml>.

[34] Tom Steinert-Threlkeld, *Coming of Age: It Only Gets Tougher for the ISP* (last modified Feb. 6, 1998) <http://www.zdnet.com/products/content/articles/199802/isp.challenges/>. The number of Internet host computers exceeded 1,000 in 1984, 10,000

The key element that made the creation of the Internet possible was the agreement to use a common language, Internet Protocol (IP), and a common unit of communication, the IP "packet."[35] The best analogy is to see the Internet backbones as the postal system and the IP packets as postcards. Each computer on the Internet is assigned a unique number, called its "IP address." Like a postcard, each IP packet is small and of a uniform size. A large message is broken up into many small packets. Also like a postcard, each packet is labeled with both destination and return addresses (the IP addresses of both the origination and destination computers). The computers at the ends of each physical link in the Internet ("routers") act like postal workers, sorting each packet and forwarding it another "midstream" router closer to the destination computer.[36] Because each packet is individually addressed, although the packets typically get bounced around from computer to computer on their way, the routers can always determine where each individual packet is heading (and also from where it came). As a result, despite many different packets taking many different paths, the destination computer can reconstruct each message by sequentially ordering the individual packets as they arrive.[37]

in 1987, 100,000 in 1989, and 1,000,000 in 1992. Zakon, *supra* note 1.

[35] *See* Charles L. Hedrick, *Introduction to the Internet Protocols* §§ 2.0 - 2.2 (1987) (visited Apr. 14, 1998) <http://www.cis.ohio-state.edu/htbin/rfc/hedrick-intro.html>. Internet Protocol specifies that data must be sent in a fixed size "datagrams," which are colloquially referred to as "packets" or "IP packets." *See id.* § 2.2. *See also* Richard Wiggins, *How the Internet Works*, INTERNET WORLD, Oct. 1996 <http://www.internetworld.com/1996/10/howitworks.html> (explaining packets in less technical terms). The size of the packets will vary depending on the particular network over which they must travel. *See* Hedrick, § 8.

[36] *See generally Routing in the Internet* (visited Feb. 1, 1998) <http://www.scit.wlv.ac.uk/~jphb/comms/iproute.html> (providing details on the mechanics of packet routing). The volume of packets traveling the Internet is staggering—in the 24-hour period ending February 23, 1998, the routers at the New York Network Access Point (one of the four major network interconnecting points) carried as many as 25,000 packets *per second*. *New York NAP Usage Statistics* (visited Feb. 23, 1998) <http://www.nlanr.net/NAP/> (Web page allowing the visitor to query the New York NAP about its recent usage; the information is returned in graphical form).

An October 1995 estimate placed the daily data flow through Internet routers at around a terabyte (1,000,000,000,000 bytes, or the equivalent of 700 million book pages). Paul Samuelson, *Weblock*, PC COMPUTING, October 1995, at 71.

[37] *See* Hedrick, *supra* note 35, § 8. This seemingly chaotic system of message propagation was purposely designed into the Internet. The predecessor to the Internet was a network called ARPANET, created in 1969 by the Advanced Research Project Agency (ARPA). ARPANET was funded by the U.S. government to network the computers of certain universities, defense contractors, and the military. This system of dynamic routing of small packets of information would allow the network to continue to function even if portions of the system were destroyed by a military attack. *See generally* Gaffin, *supra* note 23, § 1.7; *History of the Internet* (visited Feb. 1, 1997) <http://www.hotwired.com/web101/97/31/index4a.html>.

Although personal computers are capable of creating the packets, individual users cannot directly gain access to the Internet.[38] To bridge this gap, an ISP creates an intermediate network (like the local post office) between its dial-up subscribers and the Internet. At the subscriber end of this network is a device called an "access server" and at the other end is a router connected to the Internet.[39] A caller's computer transmits and receives packets from the ISP's access server using a standard language called Point-to-Point Protocol (PPP).[40] When a caller initially connects to an ISP, the ISP's access server assigns to the caller's computer a 12-digit IP address from the pool of IP addresses that the ISP has registered ("dynamically assigned addressing").[41] At the moment the caller's computer is assigned an IP address, it actually becomes part of the Internet; the caller's computer can now communicate with any other computer connected to the Internet because the remote computer now has a return address to which it can send its reply. The ISP's network translates the caller's incoming PPP packets into Internet-standard IP packets and forwards them to its routers, which in turn connect to other routers on a regional network. Information returning simply follows the reverse procedure.

C. *Internet Services*

In addition to an understanding of the Internet itself, a real-world, nut-and-bolts understanding of the mechanics of how pirated works are actually exchanged is crucial to a meaningful discussion of Internet

[38] *See generally* Gaffin, *supra* note 23, §§ 1.1-1.4, 1.6 (providing thorough, but somewhat dated, explanation of the process of connecting to the Internet).

[39] *See generally* Dennis, *supra* note 26, §§ 6.24-6.26 (providing technical overview of required telephone equipment).

[40] PPP is the most commonly used protocol for transmitting TCP/IP information over standard telephone lines. *See generally* Drew D. Perkins, *RFC1171: The Point-to-Point Protocol for the Transmission of Multi-Protocol Datagrams Over Point-to-Point Links* (last modified July 1990) <http://www.cis.ohio-state.edu/htbin/rfc/rfc1171.html>.

[41] Service providers purchase contiguous blocks (CIDR blocks) of consecutive IP addresses. Rather than permanently assigning each IP address to a given subscriber, the ISP is able to maximize its fixed allocation of IP addresses by assigning them only as needed. Most service providers use this method of "dynamically assigned addresses." The alternative method of fixed IP addresses, whereby each user is permanently assigned an IP address, is inefficient. Under the fixed IP address system, for instance, a service provider with a 100-address CDIR block is limited to 100 subscribers. By dynamically assigning these addresses, the provider is able to take advantage of the fact that its subscribers are not constantly connected. *See* Dennis, *supra* note 26, § 18.2.

copyright infringement. Because the Internet only provides the link between computers, it is necessary to use one of several Internet services in order to actually transmit information. This section will introduce the most commonly used Internet services, briefly illustrating how each service works, how each is used to facilitate online copyright infringement, and the degree to which Sysops can detect and respond to these abuses.

1. Electronic Mail

One of the simplest and most widely used Internet services is electronic mail, or "e-mail," a user-to-user worldwide messaging system. In order to use e-mail, a user must arrange with a mail server Sysop to establish a "mailbox" (a defined space on the mail server's mass storage devices) in which to store incoming mail. The user is assigned a unique user name/password combination to prevent unauthorized access to the mailbox.

Although files may be sent using e-mail, its potential as a medium of massive copyright abuse is inherently limited by its single user-to-single user propagation—e-mail messages must be individually sent to each user.[42] Further, mail server Sysops typically limit the size of each mailbox, making the exchange of large files like pirated software cumbersome since, to avoid filling up the recipient's mailbox, large files must be split into smaller messages and sent over a period of time.

Another problem for the would-be e-mail abuser is that return addresses are normally attached to the messages by the sending mail server, thereby making messages relatively easy to trace back to the sender. This problem is to a certain degree eliminated by the use of certain mail servers known as "anonymous remailers," mail servers designed to conceal the sender's identity by replacing the message's return address with an address pointing to the remailer.[43] It is highly

[42] Although it is quite easy using most e-mail applications to send a single message to many separate users, the messages still inherently must be sent individually to each recipient's mail server. There are, however, computers called "mail exploders" or "list servers" that provide the user with the ability to send a single e-mail message to all users on a particular list. *See generally Internet Mailing Lists: Guides and Resources* (visited Apr. 4, 1997) <http://www.nlcbnc.ca/ifla/I/training/listserv/lists.htm>.

[43] *See generally* Andre Bacard, *Anonymous Remailers* (visited Nov. 12, 1996) <http://www.well.com/user/abacard/remail.html>. Any reply to that message is sent through the same remailer, which maintains a list enabling it to reverse the procedure, forwarding the reply to the recipient's true address. Since the remailer system is premised on the Sysop's implicit promise not to divulge that information, faith in the security of anonymous remailers has been shaken since the Sysop of the most popular remailer, Finland-based anon.penet.fi, was compelled by Finnish authorities to disclose

impractical to use anonymous remailers as a method of piracy, however, since most remailers severely restrict the maximum individual message size, making it impractical to exchange large works like software and images.[44]

A mail server Sysop has little ability to detect infringing messages on its server. Since e-mail is a one-to-one messaging system, e-mail users have an expectation of privacy.[45] More importantly, the Electronic Communications Privacy Act of 1986 makes it a federal crime to intercept e-mail[46] or to view stored electronic communications.[47] There are, however, several provisions that allow Sysops to investigate potential e-mail abuses in order to protect their own interests or to assist law enforcement.[48] Finally, e-mail users are increasingly relying on encryption to ensure e-mail privacy. It is virtually impossible for the Sysop to view the contents of an encrypted message.[49]

the identities of three user's names. *See* Ron Newman, *The Church of Scientology vs. anon.penet.fi* (last modified Sept. 30, 1996) <http://www.cybercom.net/~rnewman/scientology/anon/penet.html>.

A user may obtain more secure anonymity by "chain-remailing," a method whereby the user sends his e-mail message to one remailer, which in turn sends it to another remailer, and so on. *See* Bacard. The only way to send e-mail with absolute anonymity, however, is by sending the message through an anonymous remailer that removes the original return address and inserts nothing in its place. The obvious limitation with using such a remailer is that the sender cannot get a reply unless the recipient already knows his return address.

[44] Most anonymous remailers limit individual message size to 30,000 bytes, about 1/50th the capacity of a single 3½" diskette. Even a small image file exceeds this limitation.

[45] E-mail sent or received from a user's place of business provides an exception to this rule. Many companies routinely monitor the e-mail of their employees. *See generally* Karen L. Casser, *Employers, Employees, E-mail and the Internet, in The Internet and Business: A Lawyer's Guide to Emerging Legal Issues* (Joseph F. Ruh Jr., ed.) (visited Mar. 15, 1998) <http://cla.org/RuhBook/chp6.htm>.

[46] 18 U.S.C. §§ 2510-2521 (1997).

[47] *Id.* §§ 2701-2709.

[48] The Sysop may engage in random checks for the purpose of quality control. *See id.* § 2511(2)(a)(i). He may also intercept any messages necessary for "the protection of the rights or property of the provider of that service." *Id.* Provided that the government follows strict procedures, the Sysop must intercept messages at the request of authorized government officials. *See id.* § 2511(2)(a)(ii). These procedures are detailed in sections 2516 to 2518. Similarly strict requirements apply to the disclosure of messages stored on the Sysop's servers. *See id.* §§ 2702, 2703.

[49] *See infra* notes 203-05, 260-61 and accompanying text (providing overview of encryption).

2. *File Transfer Protocol*

Another widely used Internet service is FTP (File Transfer Protocol), a file transfer service using remote servers as a storage medium.[50] Although FTP server Sysops control access by requiring visitors to supply a user name and password combination, many servers allow the visitor to log on "anonymously."[51] Anonymous visitors are typically restricted as to which files they may access and are frequently not allowed to upload files to the server. Once connected to an FTP server, the user can navigate the directory structure of the server and select files to transfer. File descriptions are typically not presented, although many FTP servers provide text files briefly describing the contents of the files in any given directory.[52]

The use of FTP servers as a medium for intellectual property theft is widespread, primarily through their use as "drop sites."[53] To create a drop site, users log on to an FTP server, either anonymously or using a stolen password, and then use the server to exchange pirated works.

[50] *See generally* Gaffin, *supra* note 23, §§ 7.1-7.4; Perry Rovers, *Anonymous FTP Frequently Asked Questions (FAQ) List* (visited Apr. 4, 1997) <http://hoohoo.ncsa.uiuc.edu/ftp/faq.html>; *Anonymous FTP Abuses* (visited Mar. 15, 1998) <ftp://ftp.cert.org/pub/tech_tips/anonymous_ftp_abuses>.

[51] The typical anonymous login procedure allows the visitor to use "anonymous" or "guest" as a user name and an e-mail address as a password. The typical anonymous login procedure, however, is quite easy to fool. Since most FTP servers do not have the ability to check the information supplied, the visitor can log in with any fictional name and e-mail address.

[52] Since most FTP servers follow the DOS convention of eight-character file names with three-character suffixes, or "extensions," filenames are displayed in the format xxxxxxx.xxx, inherently limiting the amount of information conveyed.

[53] *See* McCandless, *supra* note 6, at 175; Noah Robischon, *Filching for Fun and Profit* (last modified May 8, 1997) <http://cgi.pathfinder.com/netly/editorial/0,1012,928,00.html>(describing the use of drop sites for the exchange of pirated music). The largest FBI crackdown on software piracy to date, "Operation Cyber Strike," specifically targeted FTP drop site abuse. *See* Courtney Macavinta, *FBI Hunts Software Pirates* (visited Mar. 4, 1997) <http://www.news.com/News/Item/0,4,7427,00.html>.

Software pirates also commonly exchange files over the Internet by configuring their own personal computers as FTP servers. *See* McCandless, *supra* note 6, at 176; *see also* Robischon, *supra.* Using currently available technology, however, these "private drop sites" have some inherent limitations that prevent their use as a widespread medium of abuse. First, residential phone lines do not have the capacity to support more than a few simultaneous users. Second, maintaining a private drop site may inconvenience its operator, since he must leave his computer constantly powered up and connected to the ISP. Finally, the operator's ISP may become irritated by his disproportionate use of the ISP's limited resources.

These drop sites are only temporary, however, as FTP server Sysops eventually discover and delete the files.[54]

Most FTP abuse is difficult for Sysops to detect. Since FTP servers are designed to facilitate the anonymous transfer of large files, any increase in activity must be exceptional to raise the Sysop's suspicions. Most FTP sites also have a huge number of files resident on the server, so any increase in the number of files must be significant enough to attract attention. Further, FTP filenames are typically limited to eight characters, making it difficult for the Sysop to monitor resident content by simply scanning the system for suspicious filenames. Restricting access and forbidding anonymous users to upload files are an FTP Sysop's only practical methods of controlling abuse.

3. *Internet Relay Chat*

Internet Relay Chat ("IRC") allows users around the world to send written messages to each other in real time ("chat").[55] Since IRC servers are linked together into networks, connection to a single server allows simultaneous communication with the hundreds or thousands of users connected to any other server on that network.[56] Most IRC servers allow anonymous access to all visitors, who are identified only by their chosen pseudonyms. Communications are topically organized into groups, or "channels."

Although the IRC protocol does not directly support file transfers, IRC is frequently used to facilitate intellectual property theft using other Internet services. Certain IRC channels operated by software pirates serve as the primary medium for alerting other users about new FTP

[54] One method used to help delay this inevitable discovery is the use of "hidden directories." This involves creating the drop site directories using certain attributes that make them partially invisible to the server's Sysop. The modification of attributes is accomplished through the use of FTP client applications that have been altered ("hacked") to allow the user to create hidden directories. The directories are invisible to the normal visitor; only users with a hacked FTP program (typically experienced software pirates) can see them. *See generally Anonymous FTP Abuses*, *supra* note 50.

[55] *See generally* Nicolas Pioch, *A Short IRC Primer* (last modified Jan. 1, 1997) <http://www.irchelp.org/irchelp/ircprimer.html>.

[56] Undernet, the largest IRC network in the world, has approximately 100,000 users, with 20,000 online at any given time. *Welcome to the Undernet WWW Server* (visited Jan. 31, 1998) <http://www.nv.us.undernet.org>.

drop sites and for inviting other users to engage in private file exchanges.[57]

IRC is virtually impossible for a Sysop to monitor. IRC communications are in real-time, with hundreds of channels and thousands of users operating simultaneously. Since users log on anonymously and use pseudonyms, the Sysop can only identify them by their IP addresses. Further, since IRC servers are linked together in networks, only a small percentage of the communications flowing through any individual IRC server actually originate from users directly connected to that server. Denial of service is not a realistic option for IRC Sysops, since denying service to an IP address would not necessarily exclude that user, but instead simply impose a burden upon the ISP that owns that address, since an ISP's subscribers are typically assigned a different address each time they connect to the ISP.[58]

4. *Usenet*

Usenet is a one-to-many messaging system providing a worldwide public forum where users can read and post messages.[59] The Usenet system is a worldwide distributed message database consisting of approximately 200,000 servers connected to each other in a "peer-to-peer" arrangement; each news server has one or more "peers" with which it exchanges information. A message posted on one Usenet server is therefore automatically and rapidly propagated to every other news server in the worldwide system. As of February 1998, there were over 46,000 newsgroups,[60] topically arranged to cover almost any interest

[57] These private transfers are usually initiated by the use of IRC robots ("bots"), which are programs that allow a user's computer to automatically perform certain tasks on one or more IRC channels. Although most IRC server Sysops forbid the use of bots, their use is widespread in groups specializing in exchanging software, music, and adult material. Although bots can perform many functions, pirates use them to automatically initiate private communications (a "DCC session") between the bot operator and one or more other users. A DCC session is done directly between the computers; the communications no longer flow through the IRC servers. Once this private connection is established, the bot operator's computer becomes, in essence, an FTP host. Files may then be transferred between the two computers, but, as with e-mail, the one-to-one nature of the system limits its usefulness as a medium of mass distribution of protected works. *See generally* Eric Hauser, *mIRC Bot FAQ* (visited Jan. 29, 1998) <http://www.indy.net/~trekkie/botfq1.html>; "NemesisII," *Frequently Asked Questions About Internet Relay Chat roBOTS* (last modified Dec. 14, 1996) <http://www.irchelp.org/irchelp/botfaq.html>.

[58] *See supra* note 41 and accompanying text (describing dynamically assigned IP addresses).

[59] *See generally Usenet Help* (visited Feb. 25, 1998) <http://sunsite.unc.edu/usenet-i/usenet-help.html>.

[60] An exact number is impossible to accurately fix. Newsgroups are started by users and new groups are formed daily. Additionally, users will lose interest and

imaginable, and Usenet's *daily* volume, which has been doubling every year, exceeded half a million messages[61] (over 900 million bytes, the equivalent of 360,000 full pages of text).[62] Since any computer file may be converted into its text equivalent, many Usenet "messages" are actually computer programs, images, sound recordings, and other types of computer files.

Virtually all Usenet servers restrict access,[63] either by requiring the visitor to log on with a user name and password combination[64] or by only allowing access to visitors connecting from certain known IP addresses.[65] Like IRC, Usenet users may choose to be identified by a pseudonym. Once connected to a news server, the user is able to browse the newsgroups, select messages to retrieve, and post his own messages.

Usenet is the source of widespread intellectual property theft; it is truly the problem child of the Internet. Pirated software is openly exchanged in many newsgroups. These groups, of which the nine most popular are estimated to alone account for thirty to forty percent of Usenet's daily traffic, have been called online software piracy's "pulsing

abandon established groups. The statistic cited was the group count on Newscene, a leading Usenet provider, on February 1, 1998. *Welcome to the Newscene* (visited Feb. 1, 1998) <http://www.newscene.com>.

[61] *Slurp News* (visited Feb. 1, 1998) <http://www.slurp.net/>.

[62] *Deja News - The Source for Internet Discussion Groups* (visited Feb. 14, 1998) <http://www.dejanews.com/info/idg.shtml>.

[63] Although there are some "public" news servers, which allow access to any user, they represent less than 1/10th of one percent of the total servers. As of February 7, 1998, there were only 132 news servers open to the public. *Open NNTP Servers* (visited Feb. 14, 1998) <http://www.jammed.com/~newzbot/> (Web site containing the results of the author's computer program that automatically polls all Usenet news servers and indexes the results). Out of the few servers that are public, many do not allow users to post messages and most carry far fewer groups than private servers. *Id.* Over half of the public news servers carried fewer than 1,000 groups out of the 45,000 in existence.

Some private servers belong to universities or businesses and therefore restrict access to their students or employees. Most private servers, however, are commercial and thus restrict access to paid subscribers only. A few news servers require the user to purchase a stand-alone subscription, but the vast majority of the servers offer access as a value-added service provided as part of an ISP's basic service package.

[64] This is the access-restriction method typically used by most news servers that provide service as stand-alone subscriptions.

[65] News servers that either belong to businesses or universities or are offered as part of an access provider's value-added services typically use this method, which allows access by anyone connecting from an IP address that it owns.

heart."[66] The regular participants in these groups are remarkably sophisticated and organized, with established rules and procedures for posting and requesting pirated software.[67] A large portion of the software posted is provided by organized software piracy groups,[68] which are so well organized and efficient that they frequently make new software available in the newsgroups even before it can be shipped to retail stores.[69]

There are also many groups specializing in the exchange of adult images, the vast majority of which are unauthorized copies of protected works.[70] Other newsgroups specialize in the exchange of "mp3's," commercial music recordings that have been specially processed to reduce transmission time.[71] Other groups specialize in providing utility programs ("cracks") and serial numbers used to defeat software copyright protection schemes.

[66] *See* McCandless, *supra* note 6, at 134.

[67] These piracy newsgroups have developed sophisticated protocols and procedures for trading pirated software using Usenet. *See The Usenet Warez FAQ* ("PolitenessMan!," ed.) (visited Oct. 16, 1997) (current Internet location unknown, on file with *San Diego Law Review*). "FAQ" is shorthand for Frequently Asked Questions. This FAQ, like many others, is also displayed as a Web Page, but Web pages that involve piracy are frequently removed by Web server Sysops.

[68] "Suppliers" provide the programs, "crackers" defeat any copy protection devices, "rippers" remove superfluous material from the programs to reduce transmission time, "packagers" divide the programs into easier to transmit portions, and "couriers" exchange these programs with couriers from other piracy groups. Finally, one or more of the couriers will post the program to Usenet, complete with installation instructions. The various groups compete among themselves for bragging rights for providing software having the most trouble free installations or for being the first to distribute a new program through files included with the pirated software. These files proudly list the aliases of the prominent members of the organization, the group's most recent successes, and invitations for new users to join. These pirate organizations typically operate one or more BBSs. Distribution may be done through either through the Internet using FTP transfers or by conventional direct computer-to-computer transfer using proprietary software. These groups often have affiliates located throughout the world. *See generally* McCandless, *supra* note 6. *See also Prepared Statement of Kevin V. DiGregory, Deputy Assistant Attorney Gen., Criminal Div., Before the House Judiciary Comm., Subcomm. on Courts and Intellectual Property, Concerning H.R. 2265, The "No Electronic Theft (NET) Act,"* Federal News Service, Sept. 11, 1997, *available in* LEXIS, Legis Library, Fednew File [hereinafter *DiGregory Testimony on H.R. 2265*].

[69] These so-called "zero-day warez" are the most highly prized commodity among Internet piracy groups. *See* McCandless, *supra* note 6, at 175.

[70] "Most of the images showcased in the binaries group [sic] are scanned from commercial adult publications, or uploaded from adult CD ROMs, many of which are copyrighted. As a result, virtually every post on alt.binaries.pictures.erotica is a copyright violation." Dennis, *supra* note 26, § 15.2. Many other images are now being taken from commercial adult Web sites. This is evident by the display of the site's URL along with the copyright information. There is even a newsgroup called "alt.binaries.pictures.erotica.commercial-websites."

[71] *See* Brown, *supra* note 8 (describing extent and methods of MP3 piracy).

Usenet has several features that make it an ideal medium for the mass exchange of pirated works. First, Usenet messages may be posted with a reasonable degree of anonymity.[72] Second, each message is propagated to thousands of news servers around the world within minutes, thereby making its contents available to millions of users. Finally, in contrast with FTP sites or Web pages, newsgroups provide a centralized shared source for pirated works. Trading is done on a quid pro quo system; if a user desires a specific work, he simply follows the procedure for posting a request and other users will typically respond by posting the desired material. That user is then implicitly obligated to post works that he possesses.

Unlike the other primary Internet services, Usenet does have a sort of central authority, generically called "the administrators," a voluntary association of individual Usenet server Sysops. Although Usenet administrators are empowered to a certain extent to correct abuses, "abuse" in this context means abuse of the Usenet *system* itself; it does not refer to the legality or appropriateness of the *content* of messages.[73]

Usenet is extremely difficult for Sysops to monitor. Although Usenet messages are identified by descriptive subject headers, the contents of any given message can only be accurately determined by retrieving (and in the case of binary files, decoding) the actual message. The massive number of messages flowing through Usenet servers each day, however, makes any such monitoring system practically impossible.

Likewise, a Usenet Sysop has few weapons with which to fight abuse. Since the content resident on any Usenet server is predominantly from

[72] Although users may assume any name, each Usenet message contains certain information that can be used to help track down an uploading user's identity. Sophisticated software pirates use a "patch" that strips away much of this information. *See* McCandless, *supra* note 6, at 175. Further, a few news server Sysops (understandably popular with software pirates) refuse to attach identifying information to messages originating from their servers. *See, e.g., Altopia Frequently Asked Questions* (last modified Nov. 14, 1997) <http://www.altopia.com/polfaq.htm>.

[73] "'Abuse' in the Usenet administrator context means forging messages or mass commercial postings to many different groups at once; actions will only be taken for abuse *of* the net, NOT abuse *on* the net. . . . To qualify as a true panic-inspiring net-abuse, an act must interfere with the net-use of a large number of people." *The Net Abuse FAQ* § 1.3 (Scott Southwick & J. D. Falk, eds.) (last modified Sept. 1, 1997) <http://www.cybernothing.org/faqs/net-abuse-faq.html>. Mass postings are known as "spam." "The term 'spam,' . . . means 'the same article (or essentially the same article) posted an unacceptably high number of times to one or more newsgroups.' CONTENT IS IRRELEVANT." *Id.* § 2.1.

other users outside the control of its Sysop,[74] denial of service to a Sysop's subscribers is not an effective weapon. Even if a Sysop were to terminate the posting privileges of every one of its subscribers, it would obviously have only a marginal effect on the content on its news server. Since a Sysop cannot discriminate among the incoming messages within any particular newsgroup, the only practical method of controlling the content resident on its server is to filter out those newsgroups that have a high level of abuse.[75] This may not be an attractive option, however, because many potential subscribers may be hesitant to establish service with a provider that exercises censorship.[76] Further, this would not be an effective long-term solution, as the pirates would merely invade other groups or establish new groups. In addition, once a harmful message is propagated out across the Usenet system, the harm cannot be easily undone. The continued propagation of a Usenet message can be stopped, or "cancelled," only from the originating server.[77] Even if a message is quickly cancelled, it will have already been made available to millions of users.

5. *The World Wide Web*

The most popular Internet service is the World Wide Web, a collection of documents, or "pages," stored on computers located throughout the

[74] Usenet's distributed messaging system dictates that vast majority of incoming content originates not from subscribers of any given server, but rather by subscribers of other Usenet servers. As an example, assuming that there are only 100 news servers, that each server has an equal number of subscribers, and that each subscriber posts exactly the same number of messages, then 99% of the messages on each individual server would have originated from subscribers of other servers. Recall, however, that there are some 200,000 news servers.

[75] There are several other reasons why Usenet server Sysops may choose not to carry all of the available groups. Carrying the "full feed" of all newsgroups requires tremendous mass storage space and the massive data flow required to keep the groups current requires expensive connections. *See* Dennis, *supra* note 26, §§ 4.2-4.5, 6.16, 6.24-6.28, 9.3. News server Sysops may decide to censor some groups due to content that they consider inappropriate or illegal. *See id.* § 6.16 (noting that "[m]any newsgroups contain blatant violations of copyright law"). Businesses that maintain news servers may carry only newsgroups relevant to their industry.

[76] Since most standalone Usenet providers advertise that they have a "no-censorship" policy, it seems reasonable to infer that censorship is an important customer criteria. *See, e.g., Altopia Frequently Asked Questions, supra* note 72 (last modified Nov. 14, 1997) <http://www.altopia.com/polfaq.htm> (first section on page entitled "Q: Do You Censor?" answered in the negative).

[77] A cancel message must be sent out by either the user who originally posted the message or by the Sysop of the originating server. An individual Usenet Sysop cannot unilaterally cancel a message. *See* McCandless, *supra* note 6, at 178. Further, many Usenet Sysops refuse to honor cancel messages. *Id.*

world.[78] Web pages are written in HTML, a powerful text-based computer language that allows an author to incorporate "objects" such as graphics, sounds, or "hyperlinks" within the text of a page.[79] When a visitor selects a hyperlink, the associated object or action is executed. For example, hyperlinks can automatically initiate the creation of an e-mail message, start an FTP file transfer, or display messages from a Usenet newsgroup. If, as is more common, the selected hyperlink refers to another Web page, the user's software, or "browser," is instructed to seek out and display that document. Even though the linked page may actually reside on another Web server located halfway around the globe, hyperlinks allow the visitor to "surf the Web," transparently moving from site to site by simply clicking on the hyperlinks.

The potential for abuse associated with Web pages is great. Although Web site space is usually limited,[80] thus providing insufficient storage space for stockpiles of pirated works, Web pages are frequently used to provide links to works located on FTP drop sites. Other Web pages help the visitor obtain pirated works by providing tools to defeat copy protection systems[81] or by providing instructions for obtaining pirated software from other Internet services like Usenet, FTP, and IRC.

Despite this potential for abuse, Web sites are relatively easy to monitor. Since the pages are relatively fixed in time and are encoded in a standard text-based format, Web server Sysops can inspect the pages with a simple visual scan. The identity of a Web page author is usually known to the server Sysop[82] and Web servers are configured so that

[78] *See generally* Kevin Hughes, *Entering the World-Wide Web: A Guide to Cyberspace* (last modified Oct. 1993) <http://www.hcc.hawaii.edu/guide/www.guide.html>.

Although most Web pages exist on a single server, some sites are "mirrored," meaning that they are simultaneously housed on several servers. Additionally, many ISPs "cache" (temporarily copy to local mass storage devices) Web pages as they are retrieved in order to speed up subsequent subscriber requests for that page.

[79] HTML stands for Hypertext Markup Language. *See generally* National Center for Supercomputing Applications, *A Beginner's Guide to HTML* (last modified Jan. 16, 1998) <http://www.ncsa.uiuc.edu/General/Internet/WWW/HTMLPrimer.html>.

[80] Most ISPs provide their subscribers with a limited amount of space on a Web server, thus enabling them to set up their own Web pages.

[81] *See supra* text accompanying note 7.

[82] Some Web servers allow virtually anonymous Web page creation by allowing for a quick and free signup, which the author can get by providing false personal information. For example, there are several popular Web site hosting companies that allow users to upload Web pages onto their servers with no verification of identity other

Web pages may only be modified by their author, thus making the author solely responsible for the content of the page. This accountability deters the subscriber from posting illegal material, which in turn makes the Sysop's monitoring easier.

6. *Summary*

Although each Internet service operates in a unique way and therefore each has its own distinct potential for copyright abuse, these services can be grouped and distinguished according to certain common features. First, for each of these services, the user must gain access to a server before he can upload infringing material. Services like FTP, IRC, and Usenet allow some measure of anonymity and thus present a much greater potential for abuse than services like e-mail and the World Wide Web, where users who provide infringing material can generally be identified. Second, as opposed to one-to-one services like e-mail, the other services are one-to-many, thus providing for much greater potential losses to copyright holders. Likewise, e-mail's private nature restricts a Sysop's ability, ethically and legally, to monitor one-to-one communications. Third, real-time services like IRC present a distinct challenge to any monitoring efforts, since the content remains on the servers only long enough to be transmitted to other servers. Fourth, whereas the content of a Web page is relatively easy to visually determine, other services present much greater content identification problems. Finally, distributed services like Usenet and IRC present much greater challenges to Sysop monitoring than non-distributed services like FTP and World Wide Web. The majority of the content on servers offering distributed services is not provided by a subscriber, but rather automatically supplied by other servers on the network. Further, and most importantly, the distributed services have a much greater daily data flow, presenting problems of scale to their Sysops.

Unfortunately, most of the cases and commentary regarding ISP liability have failed to clearly distinguish the differing role that ISPs play

an e-mail address, which itself may be either false or obtained from a free e-mail service with equally inadequate verification procedures. *See* Robischon, *supra* note 53 (describing the abuse of anonymous Web sites and FTP drop sites by software and music pirates).

> For the lay web user, five minutes and an e-mail address are all that's required for a free web site that provides a sort of soft-core anonymity courtesy of Geocities [a no-charge Web site hosting company]. It's protection enough for posting copyright-infringing software. Shutting the pages down requires a subpoena—an expensive and time-consuming process for a site that could disappear overnight.

Id.

in connection with each of the different Internet services. This is an understandable oversight, given the newness and complexity of the Internet. Application of this overly simplistic view of the role of ISPs and Internet Sysops, however, will lead lawmakers and courts to unfair, inconsistent and ineffective policies. As noted by one service provider association:

> Although there are no Internet-specific laws at present, it is conceivable that each different service provided by Internet access and technology suppliers may attract a differing policy or legal regime. For instance, point to point communication such as email and file transfers might be treated differently by legislators and courts than services for the creation or hosting of Web sites, or for the storage and retransmission of content such as newsgroups, and on-line video or audio services.[83]

III. WHEN WILL A SERVICE PROVIDER BE LIABLE?

The rapid expansion of the Internet has understandably challenged the courts, which have been increasingly required to apply old laws to new technology. In applying copyright law to the unfamiliar environment of computers and cyberspace, courts must first determine if a violation has occurred. This involves, among other things, unsettled questions of what constitutes a "copy," a "display," or a "distribution" in the computer context. Next, it must be determined if that copy or display violates one of the exclusive rights granted to the copyright owner by the Copyright Act.[84] Finally, courts must determine the even more challenging question of who may properly be held liable for the violation.[85]

In applying copyright law to online service providers, the central issue is whether the service provider can be held directly liable for the infringing acts of its subscribers. If the service provider is found directly liable, the Copyright Act dictates that the provider is strictly liable, since knowledge is not an element of direct liability.[86] Even if

[83] *The Canadian Association of Internet Providers (CAIP) "Code of Conduct"* (visited Apr. 4, 1997) <http://www.caip.ca/caipcode.htm>.

[84] The Copyright Act grants owners of a work, among other things, the exclusive right to control the work's reproduction and distribution, its public display or performance, and the preparation of any derivative works. 17 U.S.C. § 106 (1997).

[85] Although beyond the scope of this Comment, yet another substantial question to be resolved is where jurisdiction may properly be exercised in cyberspace.

[86] The Copyright Act imposes strict liability on infringers; a defendant's intent or knowledge is not an element of infringement. *See, e.g.*, Playboy Enters., Inc. v.

the service provider is not directly liable, the court still must consider whether the service provider may properly be held indirectly liable for its subscribers' actions under a theory of contributory infringement or vicarious liability.[87]

Since online communications is still in its infancy, only a handful of cases have required the courts to apply copyright law to the online world. Fewer yet have been asked to consider the secondary liability of service providers for subscriber-provided infringing content. As the following cases show, the courts have experienced considerable difficulty in articulating consistent principles.

A. *Recent Court Decisions*

1. Cubby v. CompuServe (Oct. 29, 1991)

In *Cubby, Inc. v. CompuServe, Inc.*,[88] CompuServe, a pioneer national online service, was sued for defamatory statements posted to one of its real-time "chat rooms" (the BBS equivalent of Internet Relay Chat). *Cubby* is considered a watershed decision because it was one of the first reported cases involving potential liability for an online service provider.

Although *Cubby* involved defamation rather than copyright infringement, the considerations involved are roughly parallel. If the court found CompuServe to have been a "publisher" of the defamatory statements, it would be held strictly liable. On the other hand, if the court found CompuServe to have been merely a "distributor" of the statements, it would only be liable if it knew or had reason to know of the presence of the statements. Thus, the distinction in the defamation

Frena, 839 F. Supp. 1552, 1556 (M.D. Fla. 1993); Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 907 F. Supp 1361, 1367 (N.D. Cal. 1995) ("Direct infringement does not require intent or any particular state of mind, although willfulness is relevant to the award of statutory damages").

[87] Indirect liability may be imposed upon others who are shown to have either benefited from or contributed to the infringement. Since the Copyright Act does not address indirect liability, these theories of recovery for indirect infringement have been inferred from the Act by the courts. As the Supreme Court has stated:

> The absence of such express language in the copyright statute does not preclude the imposition of liability for copyright infringement on certain parties who have not themselves engaged in the infringing activity. For vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another.

Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 435 (1984).

[88] 776 F. Supp. 135 (S.D.N.Y. 1991).

doctrine between "publisher" and "distributor" is a rough analog of the distinction in copyright doctrine between direct liability and contributory infringement.

The court refused to hold CompuServe strictly liable as a publisher, finding that:

> CompuServe has no more editorial control over such a publication than does a public library, book store, or newsstand, and it would be no more feasible for CompuServe to examine every publication it carries for potentially defamatory statements than it would be for any other distributor to do so. "First Amendment guarantees have long been recognized as protecting distributors of publications. . . . Obviously, the national distributor of hundreds of periodicals has no duty to monitor each issue of every periodical it distributes. Such a rule would be an impermissible burden on the First Amendment."[89]

After finding that CompuServe did not have knowledge of the defamatory statements, an essential element of distributor liability, the court granted summary judgment for CompuServe. It is important to note, however, that, since the chat room was actually operated by a subcontractor, Cubby conceded that CompuServe did not control the content in the chat room.[90]

2. *Playboy v. Frena* (Dec. 9, 1993)

Playboy Enterprises, Inc. v. Frena,[91] was the first major case to deal with the liability of an online service provider for the copyright infringement of a subscriber. Playboy magazine brought suit against George Frena, the operator of a BBS that contained over 170 of Playboy's copyrighted images. BBS subscribers were able to preview these images and select those that they wished to download. Frena claimed that subscribers had uploaded the images and that he removed them as soon as he was made aware of their existence. Since the case was before the court on Playboy's motion for summary judgment, Frena's claims were accepted as true.

[89] *Id.* at 140 (quoting Lerman v. Flynt Distrib. Co., 745 F.2d 123, 139 (2d Cir.1984), *cert. denied*, 471 U.S. 1054 (1985)).

[90] *See Cubby*, 776 F. Supp. at 140 n.1. The court also held that CompuServe, since it was not an agent of the subcontractor, could not be held vicariously liable. *Id.* at 142-43. There was a rather complicated business arrangement between CompuServe, the lessor, and another company that provided the actual content to the lessor. *Id.*

[91] 839 F. Supp. 1552 (M.D. Fla. 1993).

The court held Frena liable for direct infringement. The court found that Frena had "implicated" Playboy's exclusive right to distribute copies of its protected works and thus held Frena strictly liable, finding that "[i]t does not matter that Defendant Frena claims he did not make the copies himself."[92] It was sufficient that Frena "supplied a product containing unauthorized copies of a copyrighted work."[93] The court further held that Frena had violated Playboy's public display right, finding that Frena's subscribers constituted a sufficient audience as to render the display of the images a "public" display.[94]

3. *Stratton Oakmont v. PRODIGY* (May 25, 1995)

Stratton Oakmont, Inc. v. PRODIGY Services Co.,[95] a New York state court decision, demonstrates the unreliability of *Cubby* as precedent. The *Stratton Oakmont* court applied *Cubby* to a very similar set of facts and reached an opposite result, finding the defendant to be a publisher and thus subject to strict liability for defamatory communications posted on its system. The *Stratton Oakmont* court distinguished *Cubby* in two ways. First, the court found that PRODIGY had "held itself out to the public and its members as controlling the content of its computer bulletin boards."[96] Second, the court held that PRODIGY actually exercised this control, stating that:

> PRODIGY implemented this control through its automatic software screening program, and the Guidelines which Board Leaders are required to enforce. By actively utilizing technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and "bad taste," for example, PRODIGY is clearly making decisions as to content and such decisions constitute editorial control.[97]

The court conceded that "PRODIGY's conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than CompuServe and other computer networks that make no such choice," but dismissed the notion that its decision would "compel all computer networks to abdicate control of their bulletin boards," suggesting that the increased profits from attracting "family-oriented" users would compensate service providers for their increased exposure to liability.[98]

[92] *Id.* at 1556.

[93] *Id.*

[94] *Id.* at 1556-57.

[95] 1995 WL 323710, at *1 (N.Y. Sup. May 24, 1995).

[96] *Id.* at *4.

[97] *Id.* (citation omitted).

[98] *Id.*

4. *RTC v. Netcom* (Nov. 21, 1995)

Religious Technology Center v. Netcom On-Line Communication Services, Inc.,[99] which the Copyright Office has characterized as "[t]he most extensive judicial analysis of the issues to date,"[100] has been extremely influential, both because it has inspired considerable debate and because it has been extensively cited by subsequent courts. Religious Technology Center (RTC), a corporate entity affiliated with the Church of Scientology, brought suit against Netcom, a national ISP, Tom Klemesrud, the owner of a BBS, and Dennis Erlich, one of Klemesrud's subscribers. Klemesrud contracted with Netcom to allow his BBS subscribers to gain access to Usenet news. Using Klemesrud's BBS, Erlich posted excerpts from copyrighted Scientology literature to a scientology-related newsgroup on Netcom's Usenet server, which then propagated the messages throughout the Usenet system. Although the exact relationship between the BBS server and Netcom's Usenet server was not made clear in the opinion, the facts suggest that Klemesrud's BBS server also functioned as a Usenet server.[101] Klemesrud apparently contracted with Netcom for the limited purpose of fulfilling the requirement inherent in Usenet that each server be connected to at least one other server. The BBS subscribers apparently posted and downloaded Usenet messages using the BBS server, which would in turn

[99] 907 F. Supp. 1361 (N.D. Cal. 1995).

[100] *Prepared Statement Of Marybeth Peters, Register Of Copyrights, Before the House Judiciary Comm., Subcomm. on Courts and Intellectual Property, On H.R. 2180 And H.R. 2281*, Federal News Service, Sept. 16, 1997, *available in* LEXIS, Legis Library, Fednew File [hereinafter *Peters Statement on H.R. 2180 & H.R. 2281*].

[101] Some sections of the opinion indicate that Klemesrud's BBS was configured as a Usenet server:

> Erlich then transmits his messages to Klemesrud's computer, where they are automatically briefly stored. According to a prearranged pattern established by Netcom's software, Erlich's initial act of posting a message to the Usenet results in the automatic copying of Erlich's message from Klemesrud's computer onto Netcom's computer and onto other computers on the Usenet. In order to ease transmission and for the convenience of Usenet users, Usenet servers maintain postings from newsgroups for a short period of time—eleven days for Netcom's system and three days for Klemesrud's system. Once on Netcom's computers, messages are available to Netcom's customers and Usenet neighbors, who may then download the messages to their own computers.

Netcom, 907 F. Supp. at 1367-68.

periodically exchange messages with Netcom's Usenet server.[102] In an action for summary judgment, RTC charged that, even though Netcom was not the point of origin of the infringing materials, it should nevertheless be held liable under theories of direct infringement, contributory infringement, and vicarious liability.

The court held that Netcom did not directly infringe RTC's reproduction right, reasoning that, although the Copyright Act imposes strict liability for unauthorized copying, "there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party."[103] The court reasoned that:

> Netcom did not take any affirmative action that directly resulted in copying plaintiffs' works other than by installing and maintaining a system whereby software automatically forwards messages received from subscribers onto the Usenet, and temporarily stores copies on its system. Netcom's actions, to the extent that they created a copy of plaintiffs' works, were necessary to having a working system for transmitting Usenet postings to and from the Internet.[104]

Since Netcom's system "can operate without any human intervention" and "neither Netcom nor Klemesrud initiated the copying," "the mere fact that Netcom's system incidentally makes temporary copies of plaintiffs' works does not mean Netcom has *caused* the copying."[105]

The *Netcom* court distinguished the seemingly contrary holding in the *Frena* case by explaining that the plaintiff's reproduction right was not addressed in the *Frena* decision. The *Frena* court, it explained, held only that the defendant BBS violated the plaintiff's *distribution* and *public display* rights.[106] Nonetheless, the court took the opportunity to directly address the reasoning of the *Frena* decision:

> The court is not entirely convinced that the mere possession of a digital copy on a BBS that is accessible to some members of the public constitutes direct

[102] The court seemed to acknowledge its understanding of this fact by placing the following footnote in its opinion:

> The Usenet has been described as a worldwide community of electronic BBSs that is closely associated with the Internet and with the Internet community. . . . As a Usenet user, you read and contribute ("post") to your local Usenet site. Each Usenet site distributes its users' postings to other Usenet sites based on various implicit and explicit configuration settings, and in turn receives postings from other sites. . . . There is no specific network that is the Usenet. Usenet traffic flows over a wide range of networks, including the Internet and dial-up phone links.

Id. at 1366 n.4 (quoting DANIEL P. DERN, THE INTERNET GUIDE FOR NEW USERS 196-97 (1994)). *See also supra* Part II.C.4 (describing Usenet in more detail).

[103] *Netcom*, 907 F. Supp. at 1370.

[104] *Id.* at 1368.

[105] *Id.* at 1368-69 (emphasis added).

[106] *Id.* at 1370-71.

> infringement by the BBS operator. Such a holding suffers from the same problem of causation as the reproduction argument. Only the subscriber should be liable for causing the distribution of plaintiffs' work, as the contributing actions of the BBS provider are *automatic and indiscriminate*. Erlich could have posted his messages through countless access providers and the outcome would be the same: anyone with access to Usenet newsgroups would be able to read his messages. There is no logical reason to draw a line around Netcom and Klemesrud and say that they are uniquely responsible for distributing Erlich's messages. Netcom is not even the first link in the chain of distribution — Erlich had no direct relationship with Netcom but dealt solely with Klemesrud's BBS, which used Netcom to gain its Internet access. Every Usenet server has a role in the distribution, so *plaintiffs' argument would create unreasonable liability*. Where the BBS merely stores and passes along all messages sent by its subscribers and others, the BBS should not be seen as causing these works to be publicly distributed or displayed.[107]

Further, the court held that even if the *Frena* holding is accepted, *Frena* was "factually distinguishable" because the "[u]nlike the BBS in [*Frena*], Netcom does not maintain an archive of files for its users. . . . it merely provides access to the Internet, whose content is controlled by no single entity."[108] Again, the court refused to apply *Frena* for policy reasons:

> It would be especially inappropriate to hold liable a service that acts more like a conduit, in other words, one that does not itself keep an archive of files for more than a short duration. Finding such a service liable would involve an unreasonably broad construction of public distribution and display rights. *No purpose would be served* by holding liable those who have no ability to control the information to which their subscribers have access, even though they might be in some sense helping to achieve the Internet's automatic "public distribution" and the users' "public" display of files.[109]

The court concluded that it "does not find workable a theory of infringement that would hold the entire Internet liable for activities that cannot reasonably be deterred."[110]

Likewise, the court found that Netcom could not be held vicariously liable for Erlich's infringing actions. The court applied the *Shapiro*,

[107] *Id.* at 1372 (emphasis added).

[108] *Id.* Perhaps the court should have left well enough alone. This distinction is highly questionable, as the distinction between a bulletin board and a Usenet server is a fine one indeed. Every Usenet server contains "an archive of files." The main distinction in this case would be that, whereas a BBS server typically only stores files uploaded by its subscribers, a Usenet server theoretically stores files uploaded by every single Usenet subscriber in the world. Perhaps this is the difference between merely having "an archive of files" and *maintaining* that archive.

[109] *Id.* (emphasis added).

[110] *Id.*

Bernstein test, which provides that the defendant will be vicariously liable for the actions of a direct infringer if (1) it has the right and ability to control the infringer's acts, and (2) receives a direct financial benefit from the infringing activity.[111] The court found that, on balance, the plaintiffs had raised a genuine issue of fact as to Netcom's right and ability to control its subscribers' actions. Netcom acquired the right to control when it required its subscribers to agree to refrain from posting copyrighted materials and to indemnify Netcom from any damages to third parties. Additionally, Netcom had the ability to terminate Erlich's access, even though that would entail shutting out all of Klemesrud's subscribers. Nonetheless, because Netcom charged a flat fee to its subscribers, the court held that it could not be held vicariously liable since it received no direct financial benefit from the infringing activities. Although RTC claimed that Netcom received a direct financial benefit from its reputation as a provider that did not take action against infringing subscribers, the court found this argument to be unsupported by any evidence and would constitute an insufficient benefit even if true.[112]

Although it refused to impose direct or vicarious liability, the court held that Netcom might be liable for contributory infringement under the *Gershwin Publishing* test, where liability is found when the defendant, "with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another."[113] The court concluded that the fact that Netcom allowed "infringing messages to *remain on its system* and be further distributed to other Usenet servers worldwide" constituted "substantial," not just "material" participation.[114] Thus, since Netcom had notice of the infringing posts, the key question to be resolved at trial becomes whether Netcom "knew of any infringement by Erlich before it was before it was too late to do anything about it."[115]

In considering Klemesrud's motion for judgment on the pleadings, the court also found that he could not be held directly liable: "There are no allegations in the complaint to overcome the missing volitional or causal elements necessary to hold a BBS operator directly liable for copying that is automatic and caused by a subscriber."[116] Also consistent with

[111] *Id.* at 1375 (citing Shapiro, Bernstein, & Co. v. H. L. Green Co., 316 F.2d 304, 306 (2nd Cir. 1963)).

[112] *Id.* at 1377.

[113] *Id.* at 1373 (quoting Gershwin Publ'g Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2nd Cir. 1971)).

[114] *Id.* at 1375 (emphasis added).

[115] *Id.* at 1374.

[116] *Id.* at 1381-82.

its analysis of Netcom's liability, the court held that Klemesrud could not be held vicariously liable since RTC had not shown a direct financial benefit, but that there was a genuine issue of material fact as to whether Klemesrud's knowledge was sufficient to support a finding of contributory infringement.

In summary, although the court found that both Netcom and Klemesrud might ultimately be found liable on a contributory infringement theory, the court denied RTC's motion for a preliminary injunction:

> The court finds that plaintiffs have not met their burden of showing a likelihood of success on the merits as to either Netcom or Klemesrud. The only viable theory of infringement is contributory infringement, and there is little evidence that Netcom or Klemesrud knew or should have known that Erlich was engaged in copyright infringement of plaintiffs' works and was not entitled to a fair use defense, especially as they did not receive notice of the alleged infringement until after all but one of the postings were completed. Further, their participation in the infringement was not substantial. Accordingly, plaintiffs will not likely prevail on their claims.[117]

Netcom and RTC later settled on undisclosed terms.[118] The outcome of the case against Klemesrud is unknown.

As shall be seen in the following cases, although *Netcom* has been frequently cited for the proposition that an ISP that only provides *access to the Internet* should not be held directly liable for its subscribers' infringement, this is somewhat of a mischaracterization of its holding. Although the *Netcom* opinion in its opening paragraphs described Netcom's role as the "Internet access provider that allow[ed] [Klemesrud's BBS] to reach the Internet," and that "Klemesrud's BBS is not directly linked to the Internet, but gains its connection through the facilities of defendant Netcom,"[119] this is a somewhat imprecise characterization of the relationship between the BBS and Netcom. Netcom did *not* allow Klemesrud's subscribers to "reach the Internet." Netcom merely contracted with Klemesrud to provide a peer-to-peer

[117] *Id.* at 1383.

[118] *See* Rose Aguilar, *No Answers in Scientology Case* (last modified Aug. 5, 1996) <http://www.news.com/News/Item/0,4,2055,00.html> (noting that "Many Internet legal analysts are disappointed by an out-of-court settlement between Netcom and the Church of Scientology because now they'll have to wait for another case to come to light before a court sets a firm precedent on Internet access providers' liability for online copyright infringement"). In the days following the settlement, Netcom posted new rules regarding its handling of material claimed to be infringing. *See Netcom and Scientology Settle* (last modified Aug. 4, 1996) <http://www.news.com/News/Item/0,4,2040,00.html>.

[119] *Netcom,* 907 F. Supp. at 1365-66.

connection with the BBS's Usenet server; at no time did the Netcom connection allow Klemesrud's subscribers to actually *access* any other computer on the Internet. Any "access to the Internet" was indirect and strictly limited to providing a Usenet news feed. Further, Klemesrud (and, *a fortiori*, Erlich) was not, in the conventional Internet access provider use of the term, a "subscriber" of Netcom.[120]

The more precise holding of *Netcom* is that a system that "incidentally makes temporary copies" should not subject its operator to liability for copyright infringement, since the operator does not "cause" the copying. In fact, it is far more significant that the court used this reasoning to support its refusal to hold *Klemesrud* directly liable. Although the court was correct in its observation that there was no "meaningful distinction . . . between what Netcom did and what every other Usenet server does,"[121] the same cannot be said for Klemesrud, since the infringing works were directly posted to *his* Usenet server by one of *his* subscribers. All other news servers, including Netcom's, merely accepted content "automatically and indiscriminately" provided by another server in the periodic mass exchanges of data between peers. Despite this fact, most courts and commentators have virtually ignored Klemesrud and focused exclusively on Netcom as "the" defendant in the case. Thus, although one can easily *extend* the *Netcom* holding to encompass a service that merely provides Internet *access* to its *subscribers*, it is noteworthy that this was not the issue before the court and it did not so hold.

5. *Fonovisa v. Cherry Auction* (Jan. 25, 1996)

Although *Fonovisa, Inc., v. Cherry Auction, Inc.*[122] did not involve online communications, it is an important case because several subsequent courts have cited *Fonovisa* when considering indirect liability for online service providers. Cherry Auction operated a swap meet where

[120] Although the relationship between Usenet servers is described as a "peer" relationship, this is somewhat inaccurate. Some Usenet servers are "better connected" than others, meaning that they have more or faster peer connections and therefore contain more messages. When a peer connection is established between Usenet sysops, the less "well connected" server is said to "slurp" the news from the better connected server and thus the better connected server typically charges a fee for the connection. *See, e.g., Public Data Network: A Full Newsfeed - For Less!* (visited Mar. 11, 1998) <http://www.budget.net/news/> (home page of Usenet provider offering a peer feed). This was presumably the "subscriber" relationship between Netcom and Klemesrud, which is significantly different from the relationship between an ISP and its dial-up customers.

[121] *Netcom,* 907 F. Supp. at 1373.

[122] 76 F.3d 259 (9th Cir. 1996).

counterfeited music recordings were frequently sold. Fonovisa alleged that Cherry Auction was liable under vicarious liability and contributory infringement. Fonovisa lost in District Court[123] and appealed to the Ninth Circuit Court of Appeals.

Applying the *Shapiro, Bernstein* test (right and ability to supervise and direct financial interest), the appellate court held Cherry Auction vicariously liable. The court found that Cherry Auction had the right and ability to supervise the infringing activities because it required its concessionaires to sign an agreement whereby they agreed to abide by Cherry's rules and regulations, it patrolled the premises, and it "promoted the swap meet and controlled the access of customers to the swap meet area."[124] The court also found a direct financial benefit from the infringing activities since Cherry derived "*substantial* financial benefits from admission fees, concession stand sales and parking fees, all of which flow directly from customers who want to buy the counterfeit recordings at bargain basement prices."[125]

Applying the *Gershwin Publishing* test (where liability will be found where "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another"),[126] the appellate court also found Cherry Auction liable for contributory infringement. After finding "no question" about Cherry's knowledge,[127] the court held that "*providing the site and facilities* for known infringing activity is sufficient to establish contributory liability."[128]

[123] Fonovisa, Inc., v. Cherry Auction, Inc., 847 F. Supp. 1492 (E.D. Cal. 1994).

[124] *Fonovisa*, 76 F.3d at 262.

[125] *Id.* at 263 (emphasis added).

[126] *Id.* at 264 (quoting Gershwin Publ'g Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2nd Cir. 1971)).

[127] *Id.* Perhaps the most compelling evidence was the activities of local law enforcement. In 1991, the Fresno County Sheriff's Department staged a raid on Cherry Auction and seized over 38,000 counterfeit recordings. In 1992, the Sheriff's Department sent a letter to Cherry Auction after finding that Cherry Auction vendors were still selling counterfeit recordings. Further, in 1993, the plaintiff sent out its own investigator and found that counterfeit recordings were still being sold. *Id.* at 261.

[128] *Id.* (citing Columbia Pictures Indus., Inc. v. Aveco, Inc., 800 F.2d 59 (3rd Cir.1986) and 2 WILLIAM F. PATRY, COPYRIGHT LAW & PRACTICE 1147 (BNA 1994)) (emphasis added).

6. *Sega v. MAPHIA* and *Sega v. Sabella* (Dec. 18, 1996)

Sega Enterprises, Ltd. v. MAPHIA[129] and *Sega Enterprises Ltd. v. Sabella*[130] are remarkably similar and will therefore be considered together. Although unrelated, both were decided by the same court, on the same day, and involved remarkably similar facts. These two cases are most notable for their application of the *Netcom* approach, even though the cases had factual circumstances more similar to *Frena*. Chad Sherman (a.k.a. "Brujjo Digital") Sharon Sabella (a.k.a. "Dirty Scum") operated, respectively, the "MAPHIA" and "SEWER LINE" BBSs from their homes. Evidence strongly suggested that both Sherman and Sabella had not only known about the presence of infringing copies of Sega's games on the BBSs, but also had actually encouraged its subscribers to upload the infringing copies.[131] In each case, Sega alleged liability under direct, contributory, and vicarious liability theories.

Expressly following *Netcom* and using identical language in both cases, the court refused to hold either defendant directly liable. "While [Sherman's/Sabella's] actions in this case are more participatory than those of the defendants in *Netcom*, . . . whether [Sherman/Sabella] knew [his/her] BBS users were infringing on Sega's copyright, or encouraged them to do so, has no bearing on whether [Sherman/Sabella] directly *caused* the copying to occur."[132] Also, in each case the court, consistent with *Netcom*, concluded that "[Sherman's/Sabella's] actions as a BBS operator and copier seller are more appropriately analyzed under contributory or vicarious liability theories."[133]

Using the *Gershwin Publishing* test (knowledge and material participation), the court found no real issue with either defendants' knowledge, thereby leaving "material contribution" as the only factor to be decided. In each case, the court found sufficient participation,

[129] 948 F. Supp. 923 (N.D. Cal. 1996).

[130] No. C93-04260, 1996 U.S. Dist. LEXIS 20740 (N.D. Cal. 1996).

[131] Sabella's BBS, for instance, contained a directory called "Genesis," the name of a proprietary cartridge-based video game system produced by the plaintiff. *Id.* at *6. The "Genesis" directory contained approximately 20 files with user-supplied descriptions clearly indicating that they were copies of Sega software. *Id.*

Sabella provided different levels of access to the BBS. Users could increase the amount of information that they downloaded by either paying a fee, by gaining download credit based upon the amount of information that they uploaded, or by purchasing one of her copying machines. *Id.* at *6-10. She also urged users to contribute to her operation by proclaiming that: "You are giving very little to have HUNDRED's [sic] of $$$$$$$$ worth of games!" *Id.* at *8.

[132] *MAPHIA*, 948 F. Supp. at 932; *Sabella*, 1996 U.S. Dist. LEXIS 20740, at *19-20 (emphasis added).

[133] *MAPHIA*, 948 F. Supp. at 932; *Sabella*, 1996 U.S. Dist. LEXIS 20740, at *20.

suggesting that using either the "provision of site and facilities" test from *Fonovisa*, or what it called "an alternative and higher standard of 'substantial participation'" (citing *Netcom* as authority), both defendants would be liable since each had not only participated in, but also encouraged, the infringing activity.[134] Since the court found each defendant liable under contributory infringement, it did not consider Sega's vicarious liability claims.

7. *Playboy v. Webbworld* (June 27, 1997)

In *Playboy Enterprises, Inc. v. Webbworld, Inc.*,[135] the defendants operated the "Netpics" Web site and allowed its subscribers, for a fixed monthly fee, to access adult images stored on its Web servers. The images were first collected on a Usenet news server that the Netpics Sysops programmed to only accept messages from newsgroups that contained adult images. The Sysops developed a program called "ScanPics" that would constantly scan the downloaded Usenet messages, extract the images, discard any text, and then automatically copy the extracted images to thirteen other computers that they used as Web servers.[136] The ScanPics program would also create smaller "thumbnail" copies of the images, which enabled subscribers to preview the images and select only those that they wished to download. The Netpics Web servers each contained between 40,000 and 70,000 images at any given time.

Playboy filed suit after its "Electronic Infringement Research Assistant" obtained a subscription to the Netpics site and subsequently discovered that many of Playboy's copyrighted magazine images were

[134] *MAPHIA*, 948 F. Supp. at 932; *Sabella*, 1996 U.S. Dist. LEXIS 20740, at *24-25.

[135] No. 3-96-CV-3222-H, 1997 U.S. Dist. LEXIS 21264 (N.D. Tex. Dec. 11, 1997).

[136] *Id.* at *7-8. It is unclear from the opinion what "text" was discarded from the Usenet messages. This might mean any one of three things: (1) that the ScanPics program discarded most messages consisting only of text, (2) that the program merely separated the file attachments from their identifying "header" text, a normal part of decoding any Usenet message that has an attached file, or (3) that the program actually examined each image after it was decoded and removed text that was present in the image itself (e.g., copyright information).

contained in the "Centerfolds" directory of the Netpics Web servers.[137] Playboy named as defendants Webbworld, the corporate entity that owned the Netpics site, Webbworld's sole shareholder, and two other profit-sharing Webbworld employees. After obtaining a temporary restraining order, Playboy moved for summary judgment on theories of direct infringement and vicarious liability.[138]

With little discussion, the court found Webbworld directly liable, flatly holding that "[t]he evidence unequivocally shows that Webbworld electronically reproduced, distributed, and displayed [Playboy's] protected images."[139] The court rejected the defendants' argument, based on *Netcom*, that "it served as a mere conduit between its subscribers and adult-oriented newsgroups" and that "the infringing images would have existed on the Usenet whether or not Webbworld provided access to them or not."[140] The court distinguished *Netcom*:

> Unlike the defendant service provider in *RTC* [*v. Netcom*], Webbworld did not function as a mere provider of access. To visit the Netpics site, a subscriber first was required to gain access to the Internet itself by using an Internet service provider such as the defendant in *RTC*. Webbworld did not sell access; it sold adult images.
>
> Also unlike the Defendant in *RTC*, Webbworld did not function as a passive conduit of unaltered information. Instead, Webbworld functioned primarily as a store, a commercial destination within the Internet. Just as a merchant might re-package and sell merchandise from a wholesaler, so did Webbworld re-package (by deleting text and creating thumbnails) and sell images it obtained from the various newsgroups. In contrast to the defendants in *RTC*, Webbworld took "affirmative steps to cause the copies to be made." Such steps included using the ScanNews software to troll the Usenet for Webbworld's product.
>
> . . . .
>
> Webbworld contends that it had no control over the information its software retrieved from the Usenet and no control over the images posted therein. *See RTC* (finding no liability because the defendant access provider "does not create or control the content of the information available to its subscribers"). On the contrary, Webbworld exercised total dominion over the content of its site and the product it offered its clientele. As a shop owner may choose from what sources he or she contracts to buy merchandise, so, too, did Webbworld have the ability to choose its newsgroup sources. Clearly, a newsgroup named, for example, "alt.sex.playboy" or "alt.mag.playboy" might instantly be perceived as problematic from the standpoint of federal copyright law. Alternatively, Webbworld might simply have refrained from conducting business until it had developed software or a manual system of oversight to prevent, or at least to minimize the possibility of, copyright infringement. In any event, having

[137] These facts were only described in an earlier decision on Playboy's motion for partial summary judgment. Playboy Enters., Inc. v. Webbworld, Inc., 968 F. Supp. 1171, 1174, 76 (N.D. Tex. 1997).

[138] Playboy apparently did not allege contributory infringement. Playboy also moved for summary judgment on its trademark infringement, trademark dilution, and unfair competition claims, but these discussions have been omitted.

[139] *Webbworld*, 1997 U.S. Dist. LEXIS 21264, at *15-16.

[140] *Id.* at *16.

> developed and launched the ScanNews software for commercial use, Webbworld cannot now evade liability by claiming helplessness in the face of its "automatic" operation.[141]

The court also held two of the three individual defendants vicariously liable.[142] After finding that the infringements were willful, the court assessed joint and several liability for statutory damages of $439,000 and plaintiff's attorney's fees.[143]

Although the *Webbworld* court arguably came to the right conclusion, its analysis of the direct liability issue was somewhat flawed. First, although the court correctly distinguished *Netcom*, the implication that Netcom only provides Internet access is incorrect. As previously noted, Netcom did not provide Internet access to the codefendant BBS's subscribers, it merely provided a Usenet news peer feed. Although it may be true that Netcom was more of a "passive conduit," Netcom's actual role eluded the *Webbworld* court, which is understandable given the *Netcom* opinion's confusing treatment of the subject. Further, and perhaps more importantly, the court failed to adequately note that the defendants, in addition to creating and copying the thumbnail images, also copied *the images themselves* to their Web servers, an additional "volitional act" that would have further distinguished *Netcom* and added more support to its holding.

8. *Marobie-FL v. NAFED* (Nov. 18, 1997)

In *Marobie-FL, Inc. v. National Association of Fire Equipment Distributors* ("NAFED"),[144] NAFED created a Web page that included certain clip art files (simplified images typically used in publications like newsletters) copyrighted by Marobie-FL. The case was before the court on Marobie's motion for summary judgment for direct infringement against both NAFED and Northwest Nexis, the ISP that provided NAFED with space on its Web server. Although Marobie did not allege vicarious liability, Northwest sought summary judgment on that issue.

Citing *MAPHIA* and *Frena*, the court held that NAFED violated Marobie's reproduction right when it copied the clip art to the hard drive

[141] *Id.* at *17-18 (citations omitted).

[142] The third individual defendant was not entitled to receive a profit share until a time after most of the infringing acts occurred. *Id.* at *24-25.

[143] *Id.* at *18-22, 48, 53-54.

[144] No. 96C2966, 1997 U.S. Dist. LEXIS 18764 (N.D. Ill. Nov. 18, 1997).

on the Northwest Web server.[145] Relying on *Frena*, the court also held that NAFED violated Marobie's distribution right when it made the clip art available for downloading, irrespective of whether anyone actually downloaded the images. The court also indicated in a footnote that, although Marobie did not allege violation of its right to public display the works, "NAFED appears liable for violating this right as well."[146]

The court did not, however, find Northwest directly liable. Relying on *Netcom*, Northwest argued that "it cannot be held liable for direct infringement because if any copying, distribution or display of plaintiff's work occurred, it was caused not by Northwest, but by Internet users."[147] The court found this argument "persuasive" and rejected Marobie's attempt to distinguish *Netcom*:

> Plaintiff argues that Northwest, unlike the Internet access provider in *Religious Technology Center*, serves as more than just a gateway to the Internet because Northwest actually stores the files in NAFED's Web Page in its hard drive. Although plaintiff correctly points out that Northwest provides a service somewhat broader than the service provided by the Internet access provider in *Religious Technology Center*, the court nevertheless finds that Northwest only provided the means to copy, distribute or display plaintiff's works, much like the owner of a public copying machine used by a third party to copy protected material. Like a copying machine owner, Northwest did not actually engage in any of these activities itself. Accordingly, Northwest may not be held liable for direct infringement.[148]

Next, the court, citing *Fonovisa*, held that it could not grant Marobie's motion for summary judgment on its contributory infringement claim, since there were genuine issues of material fact as to Northwest's knowledge of the infringing material and as to "[t]he degree to which Northwest monitored, controlled, or had the ability to monitor or control the contents of NAFED's Web Page."[149] The court did, however, grant Northwest's motion for summary judgment on the issue of its vicarious liability. Citing *Netcom*, the court held that, since Northwest charged a flat fee for its hosting services, Marobie could not prove that Northwest received any direct financial benefit from NAFED's infringing activities.[150]

[145] *Id.* at *10-11. Note that this is in variance with the *Netcom* court's interpretation of the *Frena* decision. The *Netcom* court held that *Frena* did not address the reproduction right. *See supra* note 106 and accompanying text.

[146] *Id.* at *11 n.4.

[147] *Id.* at *29.

[148] *Id.*

[149] *Id.* at *30.

[150] *Id.* at *31-31.

The *Marobie* decision contains notable errors. It was factually incorrect when, as in *Webbworld*, the court incorrectly asserted that Netcom served only as an "Internet access provider" in the *RTC* case. It was legally incorrect in its consideration of Northwest's contributory infringement. Rather than evaluating Northwest's *participation* in the infringing activities, the court considered its *control or ability to control*, an element that is only relevant to a vicarious liability analysis.[151]

9. *Playboy v. Hardenburgh* (Nov. 25, 1997)

In *Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.*,[152] the defendant operated a BBS containing over 40,000 adult images. The BBS granted its subscribers additional download privileges in exchange for their uploads. Each file uploaded by a subscriber was briefly examined by the Sysops "to ascertain whether they were 'acceptable,' meaning, not pornographic, and not blatantly protected by copy-

[151] The court was also inaccurate in its analysis of Northwest's direct liability. The plaintiff, in what may have simply been unartful drafting, failed to allege that the copies on the Northwest Web server's storage devices were infringing. It instead alleged that Northwest directly infringed whenever its server made temporary copies in its RAM incidental to the process of transmitting the information to a visitor to the page. *Id.* at *6. Northwest therefore tendered the defense that the works were not sufficiently "fixed" since the images were sent out in individual packets, with the entire work never being simultaneously present in the server's RAM. *Id.* at *26. The court analyzed this argument as follows:

> Northwest argues that this copy is not a "copy" under the Act because it is not "fixed." Northwest argues that it is not "fixed" because the information is transmitted "through" RAM and over the Internet at high speed in the electronic form of bytes. According to Northwest, this process of duplication and transmission happens so quickly that "typically only a portion of a file is in RAM at any one time."
>
> "A work is 'fixed' in a tangible medium of expression when its embodiment in a copy . . . is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." 17 U.S.C. § 101. Yet, a "copy" under the Act need not be potentially perceptible with the naked eye. On the contrary, a "copy" is a "material object[] . . . in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." 17 U.S.C. § 101. In the instant case, the copy created by Northwest's computer can be perceived with the aid of a machine or device, namely, the Internet user's computer.

Id. at *26-27. The court clearly confused "fixation" with "perception."

[152] No. 1:93CV0546, 1997 U.S. Dist. LEXIS 19310 (N.D. Ohio Nov. 25, 1997).

right."[153] After a Playboy investigator subscribed to the BBS and discovered that it contained 412 of its copyrighted images, Playboy brought suit and then moved for summary judgment on the issues of direct and contributory infringement.

Noting that "the differences between *Frena* and this case are few,"[154] the court held Hardenburgh liable for direct infringement. Although in dicta the court noted its approval of the *Netcom* decision, it held that *Netcom* did not apply to this case:

> [T]he facts in this case, unlike *Frena*, *Sega*, and *Netcom*, are sufficient to establish that Defendants themselves engaged in two of the activities reserved to copyright owners under 17 U.S.C. § 106. The court finds that Defendants distributed and displayed copies of [Playboy's] photographs in derogation of [its] copyrights. This finding hinges on two crucial facts: (1) Defendants' policy of encouraging subscribers to upload files, including adult photographs, onto the system, and (2) Defendants' policy of using a screening procedure in which [BBS] employees viewed all files in the upload file and moved them into the generally available files for subscribers.
>
> These two facts transform Defendants from passive providers of a space in which infringing activities happened to occur to active participants in the process of copyright infringement.[155]

The court held that the defendants' actions violated Playboy's distribution and public display rights but, curiously, as in the *Frena* decision, failed to address its reproduction right. The court also granted Playboy's motion for summary judgment on its contributory infringement. Citing *Fonovisa*, the court found that the defendants "clearly induced, caused, and materially contributed" to the infringing activity and found that the defendants "had at least *constructive knowledge*" of the infringing activity, stating that it was "disingenuous" for the defendants to deny that they were aware that images from "one of the most famous and widely distributed adult publications in the world" "were likely to find their way onto the BBS."[156]

B. Analysis

Firm rules defining the current limits of Internet service provider liability are obviously difficult to state with any accuracy. There have been few cases to directly address the issue and those that have addressed it have often come to apparently inconsistent conclusions.

[153] *Id.* at *6.

[154] *Id.* at *23.

[155] *Id.* at *29-30.

[156] *Id.* at *35-36 (emphasis added).

Further, since the reported decisions have often stated incorrect facts,[157] offered ambiguous legal conclusions,[158] or inadequately reported perhaps crucial facts,[159] it is unclear how those cases might be decided before a better informed court. As demonstrated by the following list, this uncertainty presents service providers with a great challenge in setting operating policies and procedures that limit their potential liability.

[157] *E.g.*, the incorrect assertion that Netcom only provided access to the Internet in *Playboy Enterprises, Inc. v. Webbworld, Inc.*, No. 3-96-CV-3222-H, 1997 U.S. Dist. LEXIS 21264, at *16-18 (N.D. Tex. Dec. 11, 1997) (*see supra* text accompanying notes 140-41) and *Marobie-FL, Inc. v. National Association of Fire Equipment Distributors, Inc.*, No. 96C2966, 1997 U.S. Dist. LEXIS 18764, at *29 (N.D. Ill. Nov. 18, 1997) (*see supra* text accompanying note 148).

[158] *E.g.*, the cursory treatment of the exclusive rights in *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552, 1556 (M.D. Fla. 1993) (*see supra* text accompanying notes 92, 94) and *Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.*, No. 1:93CV0546, 1997 U.S. Dist. LEXIS 19310, at *26-30 (N.D. Ohio Nov. 25, 1997) (*see supra* text accompanying note 155) and the incorrect treatment of Northwest's "fixation" argument in *Marobie* (*see supra* note 151). *See also Case Law on Online Transmissions of Copyrighted Works, U.S. Copyright Office, June 1997* (appended to *Statement of Marybeth Peters, Register of Copyrights, Before the House Subcomm. on Courts And Intellectual Property, on H.R. 2180 and H.R. 2281, 105th Congress, 1st Session* (last modified Sept. 16, 1997) <http://lcweb.loc.gov/copyright/cpypub/2180_stat.html>).

> In a number of these cases, the question of which rights were infringed is less than clear. The courts often fail to differentiate among the rights, or to conduct a thorough analysis of each separately. Thus, they may simply find "copying" in its plain English meaning, or use words like "transmitted," "posted," "distributed," "uploaded," or "downloaded" without clearly indicating what actions were sufficient to constitute a prima facie infringement, and of which right.

Id.

[159] *E.g.*, the court's failure to completely describe the nature of the "subscriber" relationship between Klemesrud's BBS and Netcom's news server in *Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc.*, 907 F. Supp 1361 (N.D. Cal. 1995) (*see supra* text accompanying notes 101-02, 119-21) and the court's failure to elaborate on the "discarding" of text in the collected Usenet messages in *Webbworld* (*see supra* note 136).

(1) The *right* to control subscriber activities may increase an ISP's exposure to liability.[160] Therefore, more power that an ISP retains in a subscriber's contract, the greater its potential liability.

(2) The *ability* to control subscriber activities may increase an ISP's exposure to liability.[161] The longer that content is resident upon the servers, the greater the ability to control that content, thereby encouraging ISPs to provide only more transient, and therefore less useful, services.[162] Similarly, the hosting of content able to be displayed, such as Web page hosting, may expose an ISP to strict liability for direct infringement of the author's public display, distribution, or public performance rights.[163]

(3) The *actual exercise* of control over subscriber activities may increase an ISP's exposure to liability.[164] If an ISP selectively filters

[160] *See Fonovisa,* Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262 (9th Cir. 1996) (Cherry Auction concessionaires were required to sign an agreement pledging that they would obey Cherry's rules and regulations) (*see supra* text accompanying note 124); *Webbworld,* 1997 U.S. Dist. LEXIS 21264, at *18 (Webbworld "exercised total dominion over the content of its site"); *compare Cubby, Inc. v. CompuServe, Inc.,* 776 F. Supp. 135, 142-43 (S.D.N.Y. 1991) (CompuServe not liable because there was no agency relationship with company that operated chat room) *with Stratton Oakmont, Inc. v. PRODIGY Services Co.,* 1995 WL 323710, at *6-7 (N.Y. Sup. May 24, 1995) (PRODIGY liable because there was an agency relationship).

Service providers have argued that the reservation of removal rights by an ISP should not be seen as an admission that it actually has the *ability* to monitor its systems.

> [M]ost providers expressly reserve a contractual right to remove any content uploaded by any party for any reason. They do not, however, undertake to monitor all content actively and on a real-time basis, which both is impossible and would destroy the speed and effectiveness of the communications tools that they provide. However, this reservation of rights permits the service provider to take actions that may be necessary under unexpected circumstances, such as flagrant and obvious violation of copyright rules.

NII Copyright Protection Act of 1995 (Part 2), Hearings on H.R. 2441 Before the Subcomm. on Courts and Intellectual Property of the House Comm. on the Judiciary, 105th Cong. 248 (1996) [hereinafter *Hearings on H.R. 2441*] (statement of Stephen M. Heaton, Gen. Counsel and Sec., CompuServe Inc.).

[161] *See Stratton Oakmont,* 1995 WL 323710, at *2-3 (proof of past exercise of editorial control central to the finding that PRODIGY was a publisher and thus strictly liable).

[162] *See Netcom,* 907 F. Supp at 1361 (that Usenet server retained messages for at most 11 days "may be relevant to contributory infringement, where knowledge is an element").

[163] *See* Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1556-57 (M.D. Fla. 1993); Marobie-FL, Inc. v. Nat'l Ass'n of Fire Equip. Distribs., Inc., No. 96C2966, 1997 U.S. Dist. LEXIS 18764, at *11 n.4 (N.D. Ill. Nov. 18, 1997); Playboy Enters., Inc. v. Russ Hardenburgh, Inc., No. 1:93CV0546, 1997 U.S. Dist. LEXIS 19310, at *29-30 (N.D. Ohio Nov. 25, 1997) (ability of subscribers to browse files on server violates plaintiff's public display and distribution rights); *Webbworld,* 1997 U.S. Dist. LEXIS 21264, at *15-16 (display, distribution *and* reproduction).

[164] *See Stratton Oakmont,* 1995 WL 323710 at *4 (preparing guidelines for message removal and creating an automatic system to remove messages); *compare*

incoming content, even using automated systems, this editorial control may increase its exposure to liability.[165] Although this increased exposure to liability is, of course, offset by a decreased exposure to liability for the content removed or blocked, there seems to be a clear disincentive for ISPs to exercise editorial control.

(5) If an ISP presents itself as a concerned provider that exercises editorial control, the corresponding commercial benefit may increase its exposure to liability.[166] Yet, if an ISP presents itself as a provider that does *not* exercise editorial control, the corresponding commercial benefit may also increase its exposure to liability.[167]

(6) An ISP may be charged with constructive knowledge of the information resident on its servers.[168]

Despite the fact that these liability-increasing factors are often in conflict with subscriber desires, with public policy, and even in apparent conflict with each other, some commentators have attempted to minimize the concerns of ISPs by noting that no truly blameless providers have yet to be found liable: "While the legal analysis has not always been consistent, the outcomes have been appropriate, imposing liability only on parties who clearly should have been held responsible."[169] Unfortu-

Netcom, 907 F. Supp at 1368-69 (programming Usenet server accept messages from all newsgroups) *with Webbworld*, 1997 U.S. Dist. LEXIS 21264, at *7 (programming Usenet server to accept messages only from selected newsgroups) and *Hardenburgh*, 1997 U.S. Dist. LEXIS 19310, at *6, 29-30 (visually screening images to filter out blatantly infringing images). *But see Netcom*, 907 F. Supp. at 1375 n.21 ("[Departure from a] policy and practice of acting to stop postings where there is inadequate knowledge of infringement in no way creates a higher standard of care under the Copyright Act as to subsequent claims of user infringement").

[165] *Compare Netcom*, 907 F. Supp at 1368-69 (Usenet server programmed to accept messages from all newsgroups) *with Webbworld*, 1997 U.S. Dist. LEXIS 21264, at *7, 17-18 (Usenet server programmed to accept messages only from selected newsgroups provides commercial advantage to Sysops).

[166] *See Stratton Oakmont*, 1995 WL 323710 at *5 (PRODIGY's advertisement of itself as a concerned provider increased revenues from "family-oriented" users).

[167] *See Netcom*, 907 F. Supp. at 1377 (reputation as a "hands-off" provider might prove direct financial benefit from infringing activities).

[168] *See Hardenburgh*, 1997 U.S. Dist. LEXIS 19310 at *17 (Sysops charged with constructive knowledge that adult newsgroups would contain images from famous magazine).

[169] *Peters Statement on H.R. 2180 & H.R. 2281*, *supra* note 100. *See also Valenti Testimony on H.R. 2180 & H.R. 2281*, *supra* note 8.

> Of those few cases that have gone to court, none has resulted in the imposition of debilitating damage awards on an "innocent" [service provider] that had no involvement, other than providing network services, in infringing activity.

nately, decisions involving "bad actors" provide little guidance for more responsible providers attempting to set policies and procedures that limit their potential liability. The *Netcom* court's holding that "mere conduit" services do not "cause" copying and thus should be held to a contributory infringement standard seems to be the closest thing to a "bright-line test" to have emerged from the cases.[170] *Netcom*, however, was only a District Court decision, and thus not binding authority for any other court. Further, even if courts attempt to follow the *Netcom* reasoning, the Webbworld decision illustrates that the precise contours of when an ISP is a "mere conduit" are far from being defined.

Although *Webbworld* and *Netcom* were each arguably correctly decided, it is difficult to articulate a rule separating them. Netcom was not directly liable because it acted as a "mere conduit" when it configured its news servers to automatically make copies of *all* messages from *all* newsgroups. Webbworld, on the other hand, was directly liable because it "functioned primarily as a store" when it "repackaged" and "sold" the images automatically obtained from its news server.[171] It is unclear, however, which action or actions were sufficient to transform Webbworld from a "conduit" to a "store." Was Webbworld's configuring of its news server to only accept images from certain groups, it's filtering of these messages to remove text, it's copying of these filtered images to its Web servers, or it's creation of the thumbnail images that was the transforming action or actions? What if a provider configured a news server to accept only images from the adult newsgroups and offered access to these unaltered images as a standalone service? What if it filtered out text messages and offered only the images? What if automatically copied these filtered pictures to its Web servers without creating thumbnails?

Even assuming that the *Netcom* contributory infringement approach is followed by all courts, a dubious assumption at best, the application of

> Where providers have been held liable, it's quite clear from the facts of specific cases that they were well aware of, or were even active participants in, the violations enabled by their services.

Id.

[170] The *Netcom* court found contributory infringement to be the only "viable theory" of recovery. Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 907 F. Supp 1361, 1383 (N.D. Cal. 1995). In *Sega v. MAPHIA* 948 F. Supp. 923, 933 (N.D. Cal. 1996) and *Sega v. Sabella*, No. C93-04260, 1996 U.S. Dist. LEXIS 20740, at *25 (N.D. Cal. 1996), while the court did not find that contributory infringement is the *only* viable theory, it did not address the defendants' vicarious liability, halting the inquiry after finding contributory liability. This can be fairly seen as an implied assertion by the court that contributory infringement was the most suitable theory.

[171] *See supra* text accompanying note 141.

the doctrine to the complex fact patterns that will undoubtedly continue to present themselves will be a persistent problem. For example, what is proper notice? Is actual notice required? If actual notice, how specific must the notice be? This technological slippery slope is presented by *Hardenburgh*, where the defendant was charged with "at least constructive knowledge" that Playboy's images "were likely to find their way onto the BBS."[172] Couldn't the same thing be said of every Usenet server Sysop? Any news server that accepts the full news feed will contain *far* more than 412 of Playboy's copyrighted images.

What if a service provider did the opposite, configuring its news server to filter out those groups that have a high level of copyright abuse? Might it also thereby increase its liability for infringing content in the remaining groups, since it has now ceased to be a "mere conduit" and has undertaken to exercise editorial control? The defendants in Hardenburgh claimed to have made a good faith effort to screen out obviously infringing content, yet the court held that fact *against* them by using it to establish their knowledge.

The inability of the courts to articulate consistent rules is undoubtedly due in part to the fact that they have been required to carry out the objectives of copyright in an unfamiliar, complex, and often confusing factual setting. In addition to raising difficult legal and factual issues, the question of ISP liability inherently implicates important social, economic, and constitutional policy considerations. Further, although courts must necessarily consider these policy issues, copyright is statutory in nature, thereby forcing the courts to render decisions that are not only fair, but also simultaneously consistent with both the express provisions of the Copyright Act and its underlying policy goals.

Because of these practical difficulties and inherent policy implications, many commentators reason that service providers should be held strictly liable. In addition to removing the judgment of the courts, it is argued that strict liability is most consistent with the policy goals of copyright. The following section examines some of these policy arguments.

IV. THE STRICT LIABILITY OPTION

In September 1995, the Clinton administration's Information Infrastructure Task Force (IITF) issued *Intellectual Property and the National*

[172] *See supra* text accompanying note 156.

Information Infrastructure (commonly referred to as "the White Paper"), a controversial report recommending changes to American policy in response to "[t]he special intellectual property concerns and issues raised by the development and use of the NII [national information infrastructure]."[173] The report concludes that ISPs should be subjected to strict liability for infringing material transmitted through or resident upon their computers.[174]

The White Paper is significant in the discussion of online service provider liability for several reasons. First, although it was disappointingly cursory in its specific examination of ISP liability, it is one of the most comprehensive studies yet produced regarding the application of intellectual property doctrines to cyberspace. Second, it is more than just a study; the White Paper makes specific recommendations about future policy for the Internet, including ISP-related issues, and these recommendations carry with them the implicit endorsement of the Oval Office, thus giving them inherent credibility. These recommendations were, in fact, without significant change, quickly codified and introduced

[173] INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE, at 1 (1995) [hereinafter IITF WHITE PAPER]. Some authors have supported the White Paper as a balanced treatment of the issues. *See, e.g.*, Mark C. Morril & Sarah E. Eaton, *Protecting Copyrights On-Line: Copyright Liability for On-Line Service Providers*, 8 NO. 4 J. PROPRIETARY RTS. 2, 3 (Apr. 1996) ("Its conclusions and recommendations . . . represent a serious attempt to balance potentially conflicting interests and to develop sound public policy in connection with the NII.").

Other commentators have been critical of the report. *See, e.g.*, *Hearings on H.R. 2441*, *supra* note 160, at 258 (statement of Stephen M. Heaton, Gen. Counsel and Sec., CompuServe Inc.).

> [The White Paper] appears to reflect only considerations of copyright owners, without due consideration of the needs of the infrastructure that is to constitute the [national information infrastructure]. Indeed, [the *Netcom* court] has already taken issue with the failure of the White Paper to appreciate the significance of the issues raised by the online industry and other persons concerned about the free flow of ideas.

Id. One news article even suggested that the report was the product of pro-content provider bias on the part of Bruce Lehman, the administration official primarily responsible for the White Paper's preparation. Characterizing the Clinton administration's policies as a "dogged pursuit of restrictive copyright legislation for the digital age," the article noted that "[b]efore joining the Patent Office [as its Commissioner] in 1993, Lehman, a lawyer, represented the motion picture, telecommunications, computer software and broadcasting industries" and that the White Paper "was widely criticized as too restrictive and favorable to the interests of Lehman's former clients." Denise Caruso, *A Tough Stance on Cyberspace Copyrights*, NEW YORK TIMES CYBERTIMES (last modified Jan. 19, 1998) <http://www.nytimes.com/library/cyber/digicom/011998digicom.html>

[174] The White Paper devoted a separate section to ISP liability. IITF WHITE PAPER, *supra* note 173, at 114-23.

as bills in both the House and the Senate.[175] The White Paper's endorsement of strict liability for online service providers has understandably generated tremendous controversy, with the White Paper serving as a focal point for debate over the policy issues surrounding service provider liability.

The White Paper asserts that strict liability for service providers is mandated by the Copyright Act and concludes that "[t]he Working Group believes it is – at best – premature to reduce the liability of any type of service provider in the NII environment."[176] Although the White Paper was, in essence, arguing for the status quo,[177] the status quo has apparently changed since its publication. The landmark *Netcom* case, pending when the White Paper was released,[178] explicitly rejected White Paper's conclusions. The *Netcom* view seems to have taken root, relegating the White Paper's recommendation of strict liability to an apparent minority view. This is appropriate, as liability without fault is a harsh doctrine and should be imposed only after careful consideration and when absolutely necessary to further important policy goals.[179]

The White Paper and its supporters do, however, articulate many important policy goals that they claim would be advanced by the imposition of strict liability on service providers. The White Paper first identified the "arguments made by service providers wishing exemption

[175] Both bills were entitled "the National Information Infrastructure Copyright Protection Act of 1995." S. 1284 was authored by Senators Orrin Hatch (R-Utah) and Patrick Leahy (D-Vermont) and H.R. 2441 was authored by Representatives Carlos Moorhead (R-California), Patricia Schroeder (D-Colorado), and Howard Coble (R-North Carolina).

[176] IITF WHITE PAPER, *supra* note 173, at 122.

[177] "Simply put, the White Paper recommends that the Copyright Act maintain traditional standards of liability for online service providers in today's emerging, nontraditional environment. In other words, the White Paper suggests that the law maintain the status quo." John Carmichael, *Comment, In Support of the White Paper: Why Online Service Providers Should Not Receive Immunity From Traditional Notions of Vicarious and Contributory Liability for Copyright Infringement*, 16 LOY. L.A. ENT. L.J. 759, 763-64 (1996).

[178] The White Paper identified *Netcom* as a pending "relevant case." IITF WHITE PAPER, *supra* note 173, at 119-20.

[179] Some authors have argued the opposite, that strict liability should be the default standard for new technologies. *See, e.g.*, Morril & Eaton, *supra* note 173, at 5.

> As the law tends to hold new activities, whose safety is not well understood, to strict liability until more is known about them, on-line services should be held to a strict liability standard at least until we discover how best to mitigate and prevent on-line copyright infringement through technological solutions.

Id.

or a higher standard of liability"[180] and then addressed them in turn, thus implicitly placing the burden of proof upon those challenging what it perceived as the current state of the law. Since it now appears that the status quo has changed, the following analysis of the strict liability option will identify and examine the justifications for strict liability advanced by the White Paper and its supporters.

A. *The Products Liability Analogy*

One central theme advanced by proponents of strict liability for service providers is that it is necessary to provide proper internalization of the costs of infringement. This argument is premised on the classic products liability tort doctrine that those who produce injurious or defective products should be held strictly liable for any resultant harm. As Mark Morril and Sarah Eaton, attorneys for publisher Simon & Schuster, argued in a forceful defense of the White Paper:

> While the hazard at issue in the context of on-line service copyright infringement is injury to intellectual property and not personal injury, the traditional justifications for the application of strict liability are present here. The commercial on-line service provider is in a position analogous to the manufacturer as it launches into commerce a product or service with the potential to do harm to others and the provider is best situated to prevent, or to allocate the cost of, that harm. . . .
>
> . . . .
>
> Manufacturers are held liable for injuries caused by their products in a foreseeable manner. By analogy, on-line service providers provide services which foreseeably lead to copyright infringement of unprecedented magnitude — the destruction of the entire commercial value of a work through the click of a mouse.[181]

While strict liability for products manufacturers is well-settled law, it is a flawed proposition to import products liability doctrine into the discussion of service provider liability. Strict liability is typically applied to force manufacturers to internalize the costs from products that create injury because they are either inherently dangerous or defective.[182] Unlike the costs properly imposed on the manufacturer of a product "unsafe in its intended use," however, the "product" that an ISP supplies (the provision of transmission or storage facilities) has no "defect;" it is the *intentional misconduct* of a minority of the consumers

[180] IITF WHITE PAPER, *supra* note 173, at 115.

[181] Morril & Eaton, *supra* note 173, at 5.

[182] *See* WILLIAM L. PROSSER, HANDBOOK OF THE LAW ON TORTS 659-60 (4th ed. 1971).

of that product that creates the injury.[183] Unlike a defective automobile, unsafe power tool, or even explosives, online services do not "cause" the risk of injury. In tort terms, the intentional act of the infringer, even if "foreseeable," constitutes a superseding cause, thereby breaking the chain of causation.[184] Holding ISPs strictly liable on these grounds makes no more sense than holding an automobile manufacturer liable for injuries caused when an automobile is "foreseeably" used as the getaway vehicle in a bank robbery.[185]

However, the White Paper asserts that, since ISPs reap some economic benefit from the foreseeable misconduct of their subscribers, fairness dictates that they should nevertheless be held strictly liable:

> The on-line services provide subscribers with the capability of uploading works because it attracts subscribers and increases usage—for which they are paid. Service providers reap rewards for infringing activity. It is difficult to argue that they should not bear the responsibilities. . . . The risk of infringement liability is a legitimate cost of engaging in a business that causes harm to others . . .[186]

[183] Even those supporting increased liability for service providers cannot dispute that the vast majority of Internet users are not infringers. *See, e.g., Valenti Testimony on H.R. 2180 & H.R. 2281, supra* note 8.

> Let's be clear right up front. Most of the millions of customers of OSP's and Internet service providers (ISP's) are law-abiding and ethical. They use these services to reach the Net for perfectly legitimate purposes: to communicate by electronic mail; to participate in online communities of shared interests; to access news and information; and to reach the mushrooming number of legitimate, authorized sites that offer entertainment, including sites affiliated with all of our studios.

Id.

[184] *See* PROSSER, *supra* note 182, at 667.

[185] As noted by one service provider:

> Where a third party has not itself done anything to infringe a copyright, . . . it is contrary to fundamental notions of fairness to hold him responsible for that infringement. . . .
>
> . . . .
>
> [W]here a device, system, product or service has substantial purposes and uses that are in no way illegal or even inappropriate, and that in fact have tremendous positive, non-infringing value, those same facilities should not be treated as if they were in conspiracy with infringers simply because some users of these tools decide to abuse them. And this is especially true when the service at issue—such as an online service—actually supports one of the fundamental objectives of the Copyright Act itself: the advancement of the useful arts through the free exchange of ideas and information.

Hearings on H.R. 2441, supra note 160, at 255 (statement of Stephen M. Heaton, Gen. Counsel and Sec., CompuServe Inc.).

[186] IITF WHITE PAPER, *supra* note 173, at 117-18.

This view has some intuitive appeal since, after all, at least some portion of an ISP's revenues, by definition, must be derived from its subscribers' infringing activities. It is precisely this intuitive appeal that has resulted in increased scrutiny for products capable of reproducing intellectual property.[187] There are, however, many other products besides an ISP's facilities that are essential to complete an act of online infringement—the most obvious being modems, computers, and disk storage devices. Since the manufacturers of these products also reap at least *some* benefit from their use in acts of infringement, doesn't a consistent application of strict liability require that they also be held strictly liable? The answer to this question was supplied by the U.S. Supreme Court in *Sony Corp. v. Universal City Studios, Inc.*: "[T]he sale of copying equipment [in this case, videocassette recorders], like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, nonobjectionable purposes. Indeed, it need merely be capable of substantial non-infringing uses."[188] Since only a small percentage of the data that flows through an ISP's system is infringing, its facilities are clearly capable of substantial non-infringing uses.[189] If ISPs are viewed as producers of "products" that may cause harm because of their foreseeable use to infringe, they must also be released from liability by the additional doctrine supplied by *Sony*.

Fairness-based strict liability arguments, when applied to the supplier of a "product" that is neither inherently dangerous, defective, nor specifically intended to facilitate infringement, are, at bottom, merely distributive arguments for the imposition of liability on the most convenient deep-pockets defendant.[190] Irrespective of one's views

[187] *See, e.g.*, Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 430 (1984) ("From its beginning, the law of copyright has developed in response to significant changes in technology. Indeed, it was the invention of a new form of copying equipment—the printing press—that gave rise to the original need for copyright protection.")

[188] *Id.* at 442.

[189] *But see* A&M Records, Inc. v. Abdullah, 948 F. Supp. 1449, 1456 (C.D. Cal. 1996) (reasoning that *Sony* should be limited to "staple articles or commodities of commerce" since the *Sony* Court relied on patent principles in arriving at its decision).

[190] *See, e.g.*, Morril & Eaton, *supra* note 173, at 5.

> Elimination of the strict liability standard for on-line service and Internet access providers would not eliminate the potential devastation of the value of the rights holder's creation. Rather, it merely would shift the ultimate economic loss to a partly less well-situated to bear or apportion it—generally the author, composer, screen-writer, or other creator.

Id. Note, however, that there is virtual economic parity between the ISP industry and the software industry, which is the most common litigant in an online infringement case. One study found that 64% of American ISPs have annual revenues of $1 million or less. Commercial Internet Exchange, *CIX FCC Filing on Access Charge Reform* (last about the fairness of holding a relatively blameless defendant liable simply to ensure a recovery for the plaintiff, it is disingenuous to cloak purely distributive arguments in the seemingly logical economic concept of "cost internalization."

Guido Calabresi, in *The Costs of Accidents*, his influential text on tort liability, provides much needed clarity to the subject by identifying distinct "subgoals" of the tort system's general goal of reducing the costs of injuries.[191] Calabresi distinguishes the goal of loss avoidance, which is accomplished by distributing economic incentives where they will best prevent the injury from occurring, from the goal of "reducing the social costs" of accidents, which is accomplished through two primary methods: "the risk (or loss) spreading method and the deep pocket method."[192] Calabresi correctly observes that strict liability as a *value judgement* is quite different from strict liability as a *rational economic argument* and is thus more a moral or political question than a legal question.[193]

B. The Need to Provide Incentives to Prevent Infringement

It is the first goal identified by Calabresi, loss avoidance thorough proper distribution of economic incentives, that seems to provide the strongest support for strict liability. The White Paper and its supporters argue that strict liability is required to provide the incentives for ISPs to take measures to minimize user infringement. As stated by Morril and Eaton:

modified Mar. 24, 1997) <http://www.cix.org/noi0397.html>. Similarly, 75% of the Software Publishers Association's members have annual revenues of less than $2 million. Ken Wasch, *Statement by Ken Wasch, President of Software Publishers Association, on Congressional Hearings to Address Software Piracy* (last modified June 24, 1997) <http://www.spa.org/piracy/releases/pirusrep.htm>. The SPA's membership represents 85% of all packaged software sales from U.S. companies. *SPA Moves Against Internet Pirate; Lawsuit Is Software Industry First* (visited Feb. 21, 1997) <http://www.spa.org/piracy/releases/butler3.htm>. Thus, strict liability for service providers would typically only shift money from one deep pocket to another.

[191] GUIDO CALABRESI, THE COSTS OF ACCIDENTS 26-29 (1970).

[192] *Id.* at 28. Calabresi also identifies a third subgoal, the reduction of transaction costs associated with the first two subgoals. *Id.*

[193] "Economists, unlike lawyers, tend to treat [reducing the social costs] under the rubric of justice. . . . The reason, the same given for treating collective desires under justice, is that reduction of secondary costs usually entails interpersonal comparisons of utility and hence is not amenable to traditional economic efficiency analysis." *Id.* at 28, n.6.

> The reasoning of the *Netcom* court fails to take into account the unique ability of on-line service and Internet access providers to take measures to prevent copyright infringement on their systems and the urgent need to incent them to do so in order to ensure that the livelihoods of authors, composers, screenwriters, and other creators are not destroyed. The defendants here made an *affirmative policy decision* not to attempt to monitor or control infringing material on their systems . . .[194]

It is this theoretical "unique ability" for a service provider to "monitor or control" the infringing activities of its subscribers that makes *Sony* inapplicable. Although it may be conceptually convenient to refer to an ISP's machinery as a "product," the obvious reason why *Sony* doesn't apply to ISPs is that they do not manufacture a *product*, so much as they run a machine or provide a service, thus making *Sony* only tangentially relevant.[195] Although the *Netcom* court analogized Netcom to the operator of a photocopier,[196] it did not compare it to the *manufacturer* of a photocopier. Had it done so, *Sony* would have been controlling authority. Likewise, if ISPs were merely "wires and conduits," they would enjoy the same common carrier immunity as telephone companies.[197] ISPs, unlike VCR manufacturers and telephone companies, have, at least theoretically, the ongoing opportunity to control both how and by whom its system is used.

C. What Can Service Providers Do To "Monitor" Or "Control" Content?

Under the *Netcom* contributory infringement alternative to strict liability, an ISP's knowledge of infringing activities is the touchstone of

[194] Morril & Eaton, *supra* note 173, at 2-3 (emphasis added).

[195] *But see Hearings on H.R. 2441, supra* note 160, at 256 (statement of Stephen M. Heaton, Gen. Counsel and Sec., CompuServe Inc.) ("Inasmuch as virtually all providers offer services that, overwhelmingly, are used for 'legitimate, nonobjectionable purposes,' the sensible standard developed in the *Sony* decision for contributory liability *should be a model* for the standard that would apply to OLS companies.") (emphasis added).

[196] Religious Tech. Ctr. v. Netcom On-Line Communication Servs., 907 F. Supp. 1361, 1369 (N.D. Cal. 1995). *See also* Marobie-FL, Inc. v. Nat'l Ass'n of Fire Equip. Distribs., No. 1:93CV0546, 1997 U.S. Dist. LEXIS 19310, at *29 (N.D. Ohio Nov. 25, 1997) (also analogizing ISP to operator of photocopier).

[197] *See* 17 U.S.C. § 111 (1997). The *Netcom* court found that "[s]ince other similar carriers of information are not liable for infringement, there is some basis for exempting Internet access providers from liability for infringement by their users." *Netcom*, 907 F. Supp. at 1369 n.12. The court found, however, that ISPs do not fit under the existing statutory definitions of common carrier since, among other things, ISPs do not have to accept any customer. *Id.* "Whether a new definition should be carved out for online service providers is to be resolved by Congress, not the courts." *Id.*

liability. This knowledge requirement, it is argued, provides a disincentive for ISPs to control content on their systems, since self-discovery can provide liability-creating knowledge.[198] This disincentive is compounded by the fact that past instances of self-monitoring by an ISP might be used as proof that the ISP in fact has the ability to monitor resident content. Therefore, under any system with a knowledge element, ISPs that are diligent are subjected to greater liability than those that make an "affirmative policy decision" to remain ignorant. Although service providers argue that their need to preserve a business relationship with the content providers whose works they host supplies sufficient motivation,[199] the White Paper and its supporters maintain that strict liability is necessary to supply ISPs with the proper incentives to exercise editorial control.[200]

The argument that strict liability is required to supply economic incentives for service providers to control user activity and monitor content, however, presupposes that ISPs in fact possess significant ability to exercise editorial control. The following sections will challenge that assumption.

[198] "It would be unfair—and set a dangerous precedent—to allow one class of distributors to self-determine their liability by refusing to take responsibility. This would encourage intentional and willful ignorance." IITF WHITE PAPER, *supra* note 173, at 122.

[199] *See, e.g.*, *Hearings on H.R. 2441*, *supra* note 160, at 260 (statement of Stephen M. Heaton, Gen. Counsel and Sec., CompuServe Inc.).

> [The lack of incentives argument] ignores two fundamental truths: (1) OLS [online service] companies are copyright owners too and therefore already have this incentive; and (2) there are many practical business pressures on OLS companies for them to continue to provide the copyright assistance currently provided. OLS companies must work very closely with copyright owners of all kinds in connection with content-related alliances, ventures, licenses and other transactions that fuel the very business in which OLS companies find themselves: distributing content and providing network access to information sources. Thus the considerable and persistent anti-infringement efforts already undertaken by OLS companies are not in risk of extinction.

Id.

[200] *See, e.g.*, IITF WHITE PAPER, *supra* note 173, at 122-24; Morril & Eaton, *supra* note 173, at 4-6; Joseph V. Myers III, *Note, Speaking Frankly About Copyright Infringement on Computer Bulletin Boards: Lessons to Be Learned From Frank Music, Netcom, and the White Paper*, 49 VAND. L. REV. 439, 474-75 (1996).

1. Service Provider Control Over Resident Content

Let us assume for the purposes of discussion that an ISP has notice, actual or constructive, that infringing content may be physically resident in the mass storage of one of its servers. Unlike material in transmission, the ISP has at least some "possession" of the material and it is therefore at least theoretically possible for the ISP to exercise control over it. Several obstacles, however, severely restrict an ISP's ability to actually effectuate this potential.

First, an ISP must be able to identify a potentially infringing work. Second, even if an ISP is able to identify a potentially infringing work, it may not be able to determine if further distribution of the work would violate one of the author's exclusive rights. Finally, even if the work is identified as an unauthorized copy, an ISP may experience difficulty in judging the validity of any potential fair use defense.

a. Identification of Potentially Infringing Content

Although some file names or types may be obviously suspect as potentially infringing[201] or the files may be presented in circumstances suggesting piracy,[202] in many cases an ISP may have great difficulty simply identifying whether a file contains protected material. The disguise of a digitally encoded work, whether intentional or accidental, is a simple matter and may occur in a several ways.

Simply renaming a file, for example, can be a quite effective method of disguise. Since the only visual identification information conveyed by a file is its name, changing a file's name defeats any attempt to

[201] The distinctive file types associated with sound recordings are an example of file types that might raise suspicion:

> [I]f an IAP notices that one of the web sites it is hosting for someone who is not affiliated with the music industry is taking up a tremendous amount of server space (because sound files are large), or numerous files on this site that are known to be sound files—.WAV, .AU or .MP3—reside on that server or are evident in the IAP's activity logs, shouldn't that IAP at least notify us so we can check out whether the recordings on that site are authorized or not?

Prepared Testimony of Lawrence Kenswil, Exec. Vice Pres. of Bus. and Legal Affairs, Universal Music Group, Before the House Comm. on the Judiciary, Subcomm. on Courts and Intellectual Property, Federal News Service, Sept. 16, 1997, *available in* LEXIS, Legis Library, Fednew File [hereinafter *Kenswil Testimony on H.R. 2180*].

[202] *See, e.g., SPA Moves Against Internet Pirate; Lawsuit Is Software Industry First, supra* note 190 ("If an ISP notices that someone, particularly an anonymous user, is uploading exceedingly large files to its FTP server or the filenames are similar to those of commercially available software, that activity should raise a red flag and cause the ISP to investigate further.").

selectively filter files based on similarity of their file names to those of known protected works.

Changing a file's format (the way its data is arranged) also hinders identification. Many works distributed on the Internet, for instance, are reduced in size, or "compressed," and combined into "archives" of related files. Visual inspection of the files contained within an archive requires that the archive first be uncompressed. Further, many files are encoded in proprietary formats. There are hundreds of such formats in existence today and their number is constantly increasing. Examination of a file encoded in a proprietary format requires the use of a program capable of recognizing that format and rendering the contents of that file. Some proprietary formats can be recognized only by the particular program that was used to encode them. Further, if an ISP does not recognize a particular file format, it may not even be able to find an application capable of rendering the file's contents.

Another simple method of file disguise, frequently used with image files, is the removal of the copyright information. This is usually done not for the sake of disguise, but rather to make the image more visually appealing. The end result, however, is the same—even if an ISP were to visually examine every single image file resident on its servers, it would often be unable to determine whether the user that posted the file was not its lawful owner.

There are also many methods available to intentionally disguise files, of which the most commonly used method is encryption. The need for privacy, data security, and secure commerce on the Internet has fueled a rapid growth in encryption technology. A file is encrypted through the use of sophisticated mathematical algorithms that rearrange the file's data structure.[203] It is virtually impossible to examine the contents of

[203] The most popular encryption method is the "public key/private key" method. *See generally Pretty Good Privacy, Inc. Home Page* (visited Mar. 3, 1997) <http://www.pgp.com> (Web site of PGP, shorthand for Pretty Good Privacy, the most popular of these public key/private key systems); (visited Oct. 19, 1997) <http://www.yahoo.com/Computers/Security_and_Encryption/PGP___Pretty_Good_Privacy/> (providing hyperlinks to many other PGP-related pages). Only someone in possession of the specific "key" used to encrypt a file is able to decode it. As illustration of this process, assume user A wishes to receive encrypted communications from user B. First, A generates his own private key, which he reveals to no one. A then uses his private key to make a public key, which he then sends to B or uploads to one of many public "key servers," which are repositories of public keys. B then encrypts a message using A's public key and sends the message to A. Since A's private key is

an encrypted file without possession of the "key" used to encode it. Software pirates are quickly adopting encryption technology. Several Usenet software piracy groups have begun encrypting all of their communications and files.[204] ISPs are completely powerless to determine the contents of these files.[205]

Finally, ISPs may not even be allowed to examine some files, such as e-mail, that are inherently private. Not only would examination of these messages intrude upon the author's right to privacy, as previously described in Part II.C.1, federal law prohibits the interception or viewing of e-mail in most circumstances.

b. Determining if Distribution of the Challenged Work Would Constitute Infringement

Even assuming that an ISP has been able to successfully determine that a file on its server contains copyright-protected material, it is then faced with the challenge of determining if allowing further distribution of the material would violate one of the author's exclusive rights. In order to resolve this question, the ISP first must determine whether the person that posted the work was the owner or his agent, a determination that is possible only in exceptional circumstances.[206] Further, even if an ISP is able to determine that the work was not posted by an authorized party, it still must determine if further distribution of the work would violate the author's exclusive rights.

Many authors intend for their works to be distributed over the Internet. Many images, for instance, contain a copyright notice and advertising information, a clear sign that their authors *know* that their works will be distributed. The issue for the ISP, however, is whether the authors *intend* for the images to be distributed and have, in effect, granted an

required to decode the message, only A (or someone in possession of A's private key) can decode the message.

[204] The more popular of these groups has a membership that now exceeds 500. McCandless, *supra* note 6, at 175.

[205] The White Paper, while recommending strict liability for service providers, conceded that "an on-line service provider who unknowingly transmitted encrypted infringing material" could "have a good argument for an exemption." IITF WHITE PAPER, *supra* note 173, at 122.

[206] As noted by one commentator:

> A user could easily upload a third party's copyrighted short story, for example, claiming it as his own. How would the system administrator know whether it was the uploader's original work or not? Any number of other such files fall into a similar category, such as computer software that the uploader claims to have written, art work the uploader claims to have drawn, and so on.

Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1007 (1994).

implied license to distribute the work. An even more challenging question is presented by images that have no copyright information. Unless an image is clearly infringing, as in the case of an image that has obviously been poorly scanned from a printed work, there is virtually no way for an ISP to determine if further distribution of the material would violate the author's rights, since the ISP can not even determine the author's identity, much less the author's intent.

Similarly, many computer program authors intended for their works be distributed online. This is the increasingly popular "shareware" concept where users are encouraged to try out the product and, if they like it, to "share" it with others by distributing a copy.[207] Shareware programs are typically provided with one or more files granting the user a "limited license" to evaluate the product for some specified period of time or number of uses and defining the user's right to further distribute the product. These products are typically "crippled" in some way, either by providing limited functionality or by becoming unusable after a certain period of time. The user, if he likes the product, will send payment to the publisher, who will then typically respond by sending the user the information required to fully enable the product or defeat its time lock.

Shareware obviously presents a multitude of problems for an ISP, requiring them to exercise considerable technical expertise in determining if further distribution of any particular program would constitute infringement. First, an ISP would be required to uncompress each archive in order to examine the individual licenses contained within. Second, shareware programs frequently contain licenses that are ambiguous or are only visible after or during installation. Finally, software pirates often "crack," re-archive, and redistribute shareware programs. Even after full installation of the product, the examining ISP might be unaware that the copy protection mechanisms have been defeated.

Other programs are distributed as "freeware," meaning that their authors have relinquished all claims to copyright protection. The distinctions between retail software, shareware, and freeware, however, are often blurry. For example, Microsoft released one of its products, "FrontPage 97," as a series of freeware "betas" (products under

[207] *See generally Shareware, Freeware & Public Domain Software* (visited Feb. 3, 1998) <http://www.spa.org/piracy/share.htm>.

development), then concurrently in both limited-license shareware and retail product versions. It is quite difficult to distinguish among these versions without careful inspection and perhaps even actual installation.[208] Therefore, even a file with the seemingly clear name "FrontPage 97" conveys ambiguous copyright information to an ISP.

c. *Anticipating Fair Use Defenses*

Even after an ISP has identified a work as potentially infringing and determined that the work was likely not intended for online distribution, it is then presented with the problem of anticipating any fair use defenses which might be asserted by the putative infringer. Although for some works such as software, fair use would rarely be a defense, for others, such as literary works or images, the fair use defense must be considered. Section 107 of the Copyright Act provides that:

> [T]he fair use of a copyrighted work . . . for purposes such as criticism, comment, news reporting, teaching . . ., scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in a particular case is a fair use the factors to be considered shall include —
>
> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
> (2) the nature of the copyrighted work;
> (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
> (4) the effect of the use upon the potential market for or value of the copyrighted work.[209]

The application of these four factors requires a balancing test. As with any balancing test, the person examining the challenged work must exercise judgment in applying the factors. When applied to conventionally published materials, the application of these factors may prove quite challenging to the layperson. Application of these factors to the new types of publishing, such as digital multimedia works, may prove even more difficult.[210]

ISPs would need a certain measure of legal expertise in order to determine whether the fair use defense is applicable. When the matter presents a close call for an ISP, it would be required to consult with

[208] This difficulty is highlighted by a recent incident in the Usenet newsgroup "alt.binaries.fonts." A reader had posted a large series of fonts (computer typefaces), only to discover later that they were copyrighted. Despite subsequent apologies to the other members of the group, presumably countless persons had already downloaded the infringing material. Similarly, new users of the software piracy newsgroups are frequently chastised for mistakenly posting freeware or "uncracked" shareware programs.

[209] 17 U.S.C. § 107 (1997).

[210] *See generally* Victoria A. Cundiff, *Stop Cyber Theft: Respecting Intellectual Property Rights on the Internet*, 444 PLI/PAT 93 (1996).

legal counsel in order to make an informed decision. The best that an attorney can provide, however, is only a more educated guess to this complicated question.[211]

> [T]he difficulties associated with arriving at a conclusion of whether a set of circumstances is likely to constitute infringement are daunting. They involve questions of fair use, ownership, substantial similarity, validity of the underlying copyright, merger doctrine, distinguishing facts and ideas from expression, parody, public domain issues, license, laches, copyright misuse and various other issues—the stuff that has given courts and experts fits for years. It is simply unreasonable to tell [a service provider] to make these decisions in the ordinary course of its business day and to accept the repercussions and liability itself if it decides incorrectly or unwisely.[212]

d. Automating the Content Screening Process

The final and most daunting problem that an ISP faces in content-based screening is the sheer volume of data flowing through its servers each day. Perhaps the best example of this difficulty is an ISP's Usenet server. The Usenet data flow is crushing – for example, on one day picked at random, a Web page providing current statistics for that provider's news server showed that 262,762 messages passed through that server from midnight to noon, almost *22,000 messages per hour.*[213]

Manual content screening is not even remotely realistic, even for those files and messages that are relatively fixed in time. In order to manually inspect each item, an ISP would be required to have a huge number of employees, each equipped with a powerful multimedia computer and fully trained in the often complex subject of copyright law. An ISP would also be required to purchase software programs capable of rendering each of the hundreds of proprietary file formats.[214] Yet even after an ISP has expended these huge sums, the inherent content

[211] *See, e.g.*, Terry Carroll, *Copyright FAQ* at pt. 2 (last modified Jan. 6, 1994) <http://www.aimnet.com/~carroll/copyright/faq-home.html> ("If all this sounds like hopeless confusion, you're not too far off. Often, whether a use is a fair use is a very subjective conclusion. . . . even well-educated jurists are capable of disagreeing on the application of this doctrine.").

[212] *Hearings on H.R. 2441*, *supra* note 160, at 254-55 (statement of Stephen M. Heaton, Gen. Counsel and Sec., CompuServe Inc.).

[213] *SlurpNet DIABLO News Statistics for 'newsfeed.kcdata.com' for Sat 14 Feb 98* (visited Feb. 14, 1998) <http://www.slurp.net/stats/>.

[214] It is conceivable, however, that software producers might donate software to ISPs as part of an anti-piracy campaign.

identification problems discussed previously would still render the system ineffective.

Even for services with a lesser data flow, content screening is still not feasible. Web servers, for instance, would be easier to monitor, since the files are mostly in a standard format, relatively fixed in time, and originate from a subscriber of that server. Yet monitoring the traffic on these servers would still be virtually impossible, even for a large company. As an executive from a large Web site development and hosting company correctly noted:

> My servers regularly pass content and domain name resolution in the millions per hour. I have no knowledge or control over any of this information. To give you an analogy, asking me to know what my servers are doing at any one time is like asking the federal Department of Transportation what conversation is happening in every car on I-66 at any one time. There are many firms significantly smaller than [my company] that also provide this management of services who have far less resources.[215]

Indeed, most service providers are "significantly smaller"; two thirds of all American ISPs are very small firms serving primarily residential customers.[216] Considering that a local ISP typically has only a handful of employees but hundreds or thousands of subscribers, manual content screening this is simply not a realistic option.[217] Commentators, legislators, and judges would be wise to actually visit an ISP's facility. As part of the research for this Comment, I recently visited a local ISP.[218] This ISP had several hundred customers, yet its infrastructure was no more than a couple of terminal servers, a router, and a T-1 line leased from the local phone company. There were only three employees – the owner, a part-time salesperson, and a secretary. This is by no means atypical; according to a 1997 ISP survey, the median ISP only

[215] *Testimony of Tushar Patel, Vice Pres. and Managing Dir., US Web, Before the Subcomm. on Courts and Intellectual Property, Comm. on the Judiciary, U.S. House of Representatives* (last modified Sept. 16, 1997) <http://www.house.gov/judiciary/4024.htm> [hereinafter *Patel Testimony on H.R. 2180 & H.R. 2281*].

[216] *See supra* note 190 and accompanying text (detailing average ISP revenues). Eighty percent of a small ISP's customers are residential dial-up users. *CIX FCC Filing on Access Charge Reform*, *supra* note 190.

[217] *See* Richard Stiennon, *Starting an Internet Service Provider* (last modified Apr. 2, 1997) <http://www.knowledgetech.com/~richard/ISP/> (presenting a typical small ISP's business plan). This business plan calls for 2,000 subscribers serviced by only two full-time employees (a manager and a salesperson) and three part-time employees (two to answer telephones and a third to help with Web site design). *Id.* § 6, "*The Management Team*" and § 8, "*Growth Strategy.*"

[218] Feb. 1996 visit to IO-Online, an Internet access provider in San Diego, California.

had six employees.[219] Any content screening program would involve an exponential increase in costs for this or any other similarly situated service provider. Such a provider would have two choices: (1) pass the costs on to its customers, or (2) shut its doors. As noted by a service provider industry representative:

> The only *sure effect* of encouraging service providers to monitor the Internet is to vastly increase the cost of Internet service. Monitoring would have to be 24 hours a day since a web site can be changed at any moment. Monitors would have to be thoroughly trained since they would be asked to make legal judgements that they cannot make. The enormous costs of this program would be obviously passed on to the consumer.[220]

It is frequently suggested, without elaboration, that these costs might be minimized through the development of some automated system where, presumably, a program constantly scans the information stored on servers, examining each file to determine if it contains infringing content.[221] Even assuming that such a system could be unilaterally developed by an ISP, a large assumption indeed, it would still be prohibitively expensive.[222] An automated content screening system would still require large equipment expenditures. Although staffing costs would be less than under a manual system, the inspection process would still require a large measure of human judgment. No computer, for instance, can evaluate fair use, interpret the subtleties of a software license, or perceive written words displayed in an image.[223]

[219] December 1996 Study conducted by Web World magazine (on file with *San Diego Law Review*).

[220] *Prepared Testimony of Roy Neel, Pres. and CEO, U.S. Tel. Ass'n, Before the House Comm. on the Judiciary, Subcomm. on Courts and Intellectual Property, Concerning H.R. 2180*, Federal News Service, Sept. 16, 1997, *available in* LEXIS, Legis Library, Fednew File [hereinafter *Neel Testimony on H.R. 2180*] (emphasis added).

[221] In *Netcom*, the plaintiffs made such an unsupported assertion, but the court concluded that "plaintiffs submit no evidence indicating that Netcom, or anyone, could design software that could determine whether a posting is infringing." Religious Tech. Ctr. v. Netcom On-line Communication Servs., Inc., 907 F. Supp. 1361, 1376 n.23 (N.D. Cal. 1995).

[222] *But see infra* Part VIII.E (describing a possible system whereby content providers develop a system of embedding digital fingerprints in protected works and software recognizing that code is uniformly implemented by all ISPs).

[223] *See, e.g., Prepared Testimony of Scott Purcell, President, HLC-Internet, Inc., Irvine, California, Representing the Commercial Internet Exch. Ass'n, Before the House Comm. on the Judiciary, Subcomm. on Courts and Intellectual Property, Hearings on H.R. 2441*, Federal News Service, Feb. 8, 1996, *available in* LEXIS, Legis Library, Newfed File [hereinafter *Purcell Testimony on H.R. 2441*].

Even if these costs could somehow be reduced to acceptable levels, the screening of incoming content would impermissibly slow information transfer. The incoming data stream from an ISP's customers would have to be diverted to a temporary "quarantine" area. This would add an intolerable bottleneck for communications such as videoconferencing and chat that require real-time two-way data flow.

As summarized by one industry spokesman, "It should be self-evident that to suddenly require us to monitor this vast amount of content for copyright infringements would be technically unfeasible and economically unreasonable."[224]

2. *Service Provider Control Over Content in Transmission*

The considerable problems involved with screening content on an ISP's servers, however, are minimal when compared with the difficulty inherent in attempting to screen information that is merely passing through an ISP's access servers. As previously described in Part II.B, a subscriber's communications flow through the ISP's access server to its router, which then forwards the packets to "midstream" routers, which in turn forward the packets to other routers nearer the computer that the subscriber wishes to reach.

a. *Midstream Content Filtration*

Because of this propagation system, content in transmission cannot be filtered. Routers examine each packet for the sole purpose of determining the packet's ultimate destination. Like postal workers, routers only examine two pieces of information in the packet—the source and destination IP addresses.[225] Further, since routers process each packet individually, the entire message is never available to a router.[226] This

> It is technologically impossible to ascertain whether a certain phrase or picture infringes copyright; this determination is a legal one that must be made on a case-by-case basis. It would be equally impossible economically and in terms of response time for each service provider to hire an army of lawyers to ascertain the viability of claims of copyright infringement as they arise.

Id.

[224] Press release by Timothy D. Casey, Chief Technology Counsel, MCI Corp., as reported in INTERNET IT INFORMER (Web site no longer in existence; copy on file with *San Diego Law Review*).

[225] *See* Henry H. Perritt, *Cyberliability*, 446 PLI/PAT 173, 196 (1996); *ITAA Discussion Paper*, *supra* note 25, § 2 ("Approach 2: Packet Filtering").

[226] Routers are "stateless," meaning that they do not remember a packet once it has been processed. *See ITAA Discussion Paper*, *supra* note 25, § 2 ("The Connection"). Additionally, recall that the TCP/IP transmission protocol sends packets out virtually randomly, so that the chances are slim that any downstream router would process all of

means that, unlike a postal worker, even if there is something about a packet that were to signal that it might contain suspicious content, a router cannot "open up" the packet and reconstruct the contents of the message. Even if a router *could* examine the data in a packet, it would not be able to determine whether the content was infringing because "a bit is a bit and infringing bits are indistinguishable from authorized ones."[227]

Since routers are blind to content, the only possible method of control over content in transmission would, then, necessarily involve screening out individual packets based solely on the IP address of the originating or destination computer.[228] Such a system could only be implemented at the ISP dial-up router level. If midstream routers were programmed to reject communications to or from a particular IP address, that computer would be completely "blacked out" from all Internet communication. Such an Internet "death penalty" cannot realistically be implemented since it would be practically impossible to reach international agreement as to which IP addresses should be filtered out.[229]

b. *Dial-up Subscriber Content Filtration*

Although it would be theoretically possible to individually filter packets by IP address at the ISP level, implementation of any such address filtering system would cause serious bottlenecks.[230] ISPs would have to constantly update and monitor their routers' filtering

the individual packets that make up a message (*see supra* Part II.B).

[227] IITF WHITE PAPER, *supra* note 173, at 116. *See also* Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 907 F. Supp. 1361, 1372-73 (N.D. Cal. 1995) ("Billions of bits of data flow through the Internet and are necessarily stored on servers throughout the network and it is thus practically impossible to screen out infringing bits from noninfringing bits.").

[228] *See ITAA Discussion Paper*, *supra* note 25, § 2 ("Approach 2: Packet Filtering"). For a general discussion of packet filtering, see Perritt, *supra* note 225, at 195-98.

[229] If, for instance, only U.S.-based routers were unilaterally programmed to refuse packets coming from or going to a certain IP address, this would create chaos on the backbones as packet traffic was automatically re-routed in a path that avoids U.S. routers. Additionally, if one country were to unilaterally begin to filter out computers residing in another country, potentially serious international issues would certainly arise.

[230] A packet filtering system would theoretically impose a 50% performance penalty on all Internet traffic. Since routers currently only filter packets based on their destination, imposing an additional requirement to examine and filter packets based on their origin would effectively double their workload. *See* Perritt, *supra* note 225, at 197.

algorithms, or "router tables." These router tables would become exponentially more complex, thereby reducing system performance at a time when system throughput levels are not even keeping pace with the explosive growth of the Internet.[231] Further, since router tables are used to protect ISPs and their customers from unwanted accidental or intentional access, the quantum increase in complexity of the filtering rules would dramatically increase the frequency of security-compromising errors.[232]

An address-based filtering system could also easily be defeated. Subscribers of a packet-filtering ISP could simply communicate with the banned computer using "proxy servers," computers that serve as intermediaries between the remote server and the end user.[233] As far as the ISP's router is concerned, the subscriber is communicating with the proxy server, not the banned computer. Were an IP address-based filtering system to be implemented, the use of proxy servers would undoubtedly become routine.[234] Even if the proxy server problem could be worked around, address-based filtering would still be ineffective, since Internet content would inevitably be copied from filtered servers to non-filtered servers.[235]

[231] *See ITAA Discussion Paper*, *supra* note 25, § 2 ("Approach 2: Packet Filtering"). For a discussion of the current crisis in router throughput rates, or "bandwidth," see Jamie Murphy & Charlie Hofacker, *Explosive Growth Clogs the Internet's Backbone*, N.Y. TIMES CYBERTIMES (last modified June 30, 1996) <http://www.nytimes.com/library/cyber/week/0629backbone-money.html>; Peter H. Lewis, *An 'All You Can Eat' Price is Clogging Internet Access*, N.Y. TIMES CYBERTIMES (last modified Dec. 17, 1996) <http://search.nytimes.com/web/docsroot/library/cyber/week/1217aol.html>. A recent study showed that information retrieval speed was the number one concern of Internet users. *GVU's 5th WWW User Survey* (visited March 11, 1998) <http://www.gvu.gatech.edu/user_surveys/survey-04-1996/>.

[232] *See ITAA Discussion Paper*, *supra* note 25, § 2 ("Approach 2: Packet Filtering").

[233] A proxy server functions as an intermediary; a user communicates with a remote server by sending the information through the proxy server, which, in turn, relays the communication to the remote server. *See id.* § 2 ("Approach 3: Blocking HTTP Proxy Servers"). Proxy servers are routinely used by businesses that have multiple computers on their network, but wish to manage only a single Internet connection. Other proxy servers, for the purpose of protecting user privacy, are intentionally designed to prevent the remote server from knowing the true IP address of the user that is ultimately receiving the information that it is sending out. *See The ANONYMIZER Home Page* (visited Feb. 12, 1997) <http://anonymizer.cs.cmu.edu:8080/>.

[234] To avoid a legal battle with German authorities over pornography, CompuServe recently restricted its information feed to Germany. *See* Eric Berlin, *CompuServe Bows to Germany*, INTERNET WORLD, Apr. 1996, at 16. German users quickly discovered how to bypass the restrictions. *See* Perritt, *supra* note 225, at 198.

[235] Content does not always flow from point A to point B. Usenet servers, for instance, have a global propagation. Content from screened sites could be easily posted there. Since the Usenet server itself would not be a forbidden site, an ISP-level filtering system would be easily and automatically sidestepped. As an example, assume that an

Address-based packet filtering is also a blunt tool. If, in the ISP's judgment, the potentially filtered address contains objectionable material, it is faced with a choice – to completely black out the entire site or not. That site may, however, contain the content of hundreds or even thousands of users, yet there would be no way to discriminate among them, since they all share the same IP address.[236] Filtering out an address in such circumstances would be the equivalent of the postal service refusing to service an entire apartment building based on the misconduct of a single tenant. Further, a wrong decision might subject the ISP to liability for "wrongful filtration."

The difficulties inherent in an ISP's decision to filter any given address are compounded by the reality that, as of August 1997, there were about 1.3 million sites on the World Wide Web.[237] Even assuming that somehow an ISP could ever establish a filter database, it would have to be constantly monitored and kept current since, like physical addresses and telephone numbers, both the operators and the content associated with any given IP address will change over time.

c. *Liability for Content in Transmission*

The impossibility of midstream content filtration presents a doctrinal conundrum for advocates of strict liability. Since a "copy" is created whenever a work is duplicated in either fixed storage or RAM, infringing "copies" of the work (or pieces thereof) are made in many

ISP has programmed its router to reject information coming from a certain site. So long as any user in the world can get to the filtered site, he can simply download content from that site and then post it to any Usenet server. From there, Usenet's distributed messaging system would send that message out to every other Usenet server, including the one operated by the filtering ISP. Content posted to the World Wide Web would similarly defeat any such filtering system as content from the filtered sites is downloaded then uploaded to a non-filtered Web sites. The filtering ISP's router would then accept this content and pass it through to the subscriber, ignorant of its true origin.

[236] An increasingly popular trend is free Web site hosting. The Web site host administrator makes a profit by selling advertising, which is displayed whenever someone visits subscriber's site. All of the individual Web pages are located at one domain name (and therefore at one IP address). For instance, a Web site hosting computer may have the domain name "www.freesites.com." Subscriber Joe's page would have an address like "http://www.freesites.com/users/joe," subscriber Jane's page would have an address like "http://www.freesites.com/users/jane," and so on. Filtering out "freesites.com" because Joe's site contains infringing material would also block access to Jane's site.

[237] *See* Zakon, *supra* note 1.

locations when a protected work is transmitted through the Internet. Given the Internet's random propagation system, a single infringing message could travel through hundreds of midstream routers. Under a logically consistent application of strict liability, however, each of these midstream providers would be liable, despite the fact that they have no means of preventing their systems from passing infringing content. This result cannot be seriously advanced, as it is both unfair and impractical.

Strict liability for midstream content can only be justified using purely distributive arguments. Since such arguments are not amenable to rational analysis, the remainder of this comment will restrict the discussion of service provider liability to content that is either flowing through an ISP's access server and router or resident in the mass storage devices one of its servers. Even this restriction, however, introduces its own technological slippery slope. How "resident" is resident? At one end of this range are subscribers' Web pages resident on an ISP's Web server, which, absent intervention by the hosting ISP, will remain until removed by their authors. At the other end of this spectrum is outgoing e-mail, which is resident on an ISP's mail server only briefly while waiting to be sent. Somewhere in between these two extremes are messages on an ISP's Usenet server, which are typically kept for only a few days or weeks.[238] Although different types of content may be resident for different periods of time, it will be useful for the purposes of the remaining discussion to further define "resident" information as simply any information not in the process of transmission.

3. *Cost/Benefit Analysis of Editorial Incentives for Service Providers*

Content-based screening of content resident on an ISP's servers, although perhaps possible, is not even remotely commercially viable, either by manual or automated systems. Further, even accepting these costs, the benefits would be marginal since content providers have such a limited ability to detect and control infringing content in all but the most flagrant situations. In short, increased editorial efforts by ISPs would be either costly, ineffective, or both.

In addition to the economic costs, strict liability for service providers may also come with significant social costs. Civil rights groups and

[238] Most Usenet servers are programmed to purge binary messages in less than a week. A February 12, 1998 survey showed that the average length of time that binary messages were kept on the news servers of the four largest news providers was less than four days. *Airnews Earns Its Title as "the Premium News Service,"* (visited Feb. 14, 1998) <http://www.airnews.net/compare/study.html>. *See also Purcell Testimony on H.R. 2441*, *supra* note 223 ("[M]ost servers only maintain Usenet data for 7-10 days. The material is then automatically deleted.").

service providers believe that imposing strict liability on service providers would negatively impact free speech.[239] It is feared that the threat of liability may cause service providers to overreact, erring on the side of caution by aggressively censoring their subscribers' content, thereby removing protected content along with prohibited content.[240] This concern was a central factor that was addressed by the court in *Cubby v. CompuServe*, finding that "'[t]he constitutional guarantees of the freedom of speech and of the press stand in the way of imposing' strict liability on distributors for the contents of the reading materials they carry."[241] The *Cubby* court elaborated that:

> "Every bookseller would be placed under an obligation to make himself aware of the contents of every book in his shop. It would be altogether unreasonable to demand so near an approach to omniscience." And the bookseller's burden would become the public's burden, for by restricting him the public's access to reading matter would be restricted. If the contents of bookshops and periodical stands were restricted to material of which their proprietors had made an inspection, they might be depleted indeed.[242]

[239] As an example, the Electronic Frontier Foundation (EFF), an Internet free speech advocacy group, maintains an entire archive of documents arguing that many proposed national copyright laws and international intellectual property treaties will impermissibly interfere with free speech. *EFF Online Intellectual Property Overview* (last modified Dec. 6, 1996) <http://www.eff.org/pub/Intellectual_property/HTML/ip-overview.html>.

[240] As noted by an attorney for CompuServe:

> [Increased liability for service providers] is not only patently unfair, but because it tempts [service providers] to take the easy route of deletion of communications, it jeopardizes the very success of the [national information infrastructure] itself, it threatens to frustrate First Amendment-based expectations and it is bound to strain the relationships between the [service provider] and its customers.
>
> . . . .
>
> . . . [T]here must be maintained not only a proper preservation of the free flow of information and exchange of ideas unthreatened by all-too-easy deletions of communications, but an acknowledgment of the damage that would be imposed on the [service provider's] relationship with its customers by compelling them to consistently take on a role that inevitably (although unfairly) will be labeled "censor"—and to do so in lieu of the copyright owners themselves.

Hearings on H.R. 2441, *supra* note 160, at 254, 262 (statement of Stephen M. Heaton, Gen. Counsel and Sec., CompuServe, Inc.).

[241] Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135, 139 (S.D.N.Y. 1991) (quoting Smith v. California, 361 U.S. 147, 152-53 (1959)).

[242] *Cubby*, 776 F. Supp. at 139-40 (quoting Smith v. California, 361 U.S. 147, 153 (1959) (citation and footnote omitted)).

Civil rights groups also argue that strict liability will force service providers to impermissibly intrude upon their subscriber's rights to privacy.[243] Although the Internet is typically thought of as the most public of all forums, many Internet communications are intended to be private person-to-person communications. Subjecting ISPs to strict liability, it is argued, will force them to examine such communications (to the extent that they are legally able to do so), thereby invading their subscriber's privacy.

Although the extent of the intrusion upon free speech and privacy is uncertain, and may even be minimal, it seems clear that strict liability for ISPs would have a discernable impact and thus these social costs should be considered.[244]

4. *Summary*

Since ISPs have few realistic tools available to monitor content, their "editorial abilities," as a practical matter, are limited to the blunt tools of termination of service to known habitual infringers and removal of flagrantly infringing material. Yet even under the most lenient liability standard, there is no reason to believe that ISPs would not terminate known infringers. Although an ISP can legitimately defend that it cannot monitor all files flowing through or resident on its system, it defies logic that it would expose itself to even the possibility of liability to preserve the twenty dollars per month revenue stream from a known infringer.[245]

[243] *See, e.g.*, Mike Yamamoto, *Policing the Internet* (last modified Dec. 13, 1996) <http://www.news.com/News/Item/0,4,6193,00.html>.

[244] The White Paper correctly observed that the impacts upon free speech, standing alone, are insufficient grounds for reducing liability for service providers:

> Clearly, on-line service providers play an integral role in the development of the [national information infrastructure] and facilitate and promote the free exchange of ideas. But that has not been grounds for removing or reducing liability for copyright infringement. One can perform these functions without infringing or facilitating the infringement of the copyrighted expression of others.

IITF WHITE PAPER, *supra* note 173, at 117.

[245] In fact, Ken Wasch, President of the Software Publishers Association, the leading anti-piracy voice for the software industry, has made it clear the SPA does not expect service providers to engage in an expensive and futile program to monitor content:

> We are not asking ISPs to monitor that which is on every page that they host . . . that's too difficult. . . . What we're asking ISPs to do is . . . don't draw attention to illegal sites, . . . when you find out that you're hosting an illegal site, take appropriate action, and look for patterns of usage [on servers] that would indicate that there's a lot of [unusual download activity].

The threat of liability is not the only way to encourage ISPs to monitor content. Statutory "Good Samaritan" immunization for ISPs that take reasonable good faith measures to monitor content, would, if not provide an incentive, at least eliminate some of the disincentive provided under a knowledge-based standard.[246]

Thus, while strict liability would increase incentives for service providers to monitor content, it would produce questionable benefits. Further, those benefits could only be achieved by imposing unacceptable economic and social costs upon information consumers.

D. What Can Content Providers Do To Prevent Infringement?

The White Paper and its supporters also identify a second incentive that would be supplied by the imposition of strict liability on service providers—they argue that strict liability is required to provide ISPs with incentives to develop technological solutions to stop infringement. Unlike editorial control measures, the benefits from technological solutions would not be offset with significant associated negative impacts upon speech, access, and privacy.

Although supporters of strict liability fail to specifically identify any technical solutions that service providers can implement, they nonetheless routinely assert that ISPs should be strictly liable because they are better equipped to prevent online infringement, typically supporting this claim with little more than the bare assertion itself.[247] The White

Ken Wasch Interview, *supra* note 9. Since the SPA is well known for making examples out of small service providers and sysops that refuse to comply, it would make no business sense for an ISP to knowingly fail to comply with these minimal requirements. *See infra* note 278.

[246] The Communications Decency Act, for example, immunizes providers from liability for indecent content if they take reasonable measures to prevent minors from viewing such material. Pub. L. 104-104, Stat. 56 (amending 47 U.S.C. § 223). Section 223(e)(5) establishes as a defense "good faith, reasonable measures to prevent minors from gaining access to prohibited communications." Section 223(f)(1) immunizes providers from common law actions resulting from "attempting in good faith to restrict or prevent access to, or the transmission of, prohibited communications." *See also* Pamela Mendels, *Government Defines 'Safe Harbor' Under Communications Decency Act*, NEW YORK TIMES CYBERTIMES (last modified May 8, 1996) <http://www.nytimes.com/library/cyber/week/0508decency.html>.

[247] *See, e.g.*, *Hearings on H.R. 2441*, *supra* note 160, at 290 (statement of William J. Cook, Attorney, Willian, Brink, Hofer, Gilson & Lione) (offering the statement that "ISPs can utilize and implement technology, including software, that is capable of automatically screening material posted on the network," yet providing no further

Paper, for example, even after conceding that policing efforts and inadequate indemnification from infringing subscribers "may add to their cost of doing business," concluded that ISPs "are still in a better position to prevent or stop copyright infringement than the copyright owner. Between these two relatively innocent parties, the best policy is to hold the service provider liable."[248]

This conclusory language is simply not supported by the facts. It is not even supported by the White Paper itself—other than subscriber identification and account termination, the entire 238-page report did not identify a single technologically feasible method by which ISPs could "prevent or stop" infringement.[249] In fact, the White Paper conceded that "it is still virtually impossible for operators of large systems to contemporaneously review every message transmitted or file uploaded."[250] Yet the White Paper devoted a separate section, nearly twice as long as its entire consideration of service provider liability, to technological solutions that copyright owners can employ to protect their works.[251] In sharp contrast with the "virtual impossibility" of an ISP's efforts, the White Paper introduced this section with:

> Technological solutions are playing and will continue to play a significant role in meeting [the need for secure online commerce]. A wide variety of new tools to facilitate access and use of Internet-based information products and services are being rapidly developed and deployed. Concurrently, copyright owners are developing and implementing technical solutions to facilitate the delivery of protected works in an easy, consumer-friendly yet reliable and secure way. These solutions enable copyright owners not only to protect their works against unauthorized access, reproduction, manipulation, distribution, performance or display, but also serve to assure the integrity of these works and to address copyright management and licensing concerns.
>
> . . . .
>
> Technological solutions exist today and improved means are being developed to better protect digital works through varying combinations of hardware and software. Protection schemes can be implemented at the level of the copyrighted work or at more comprehensive levels such as the operating system, the network or both. For example, technological solutions can be used to prevent or restrict access to a work; limit or control access to the source of a work; limit reproduction, adaptation, distribution, performance or display of the

elaboration beyond a footnote to court cases that, in turn, provide no elaboration).

[248] IITF WHITE PAPER, *supra* note 173, at 117.

[249] "[T]he Working Group expects the access provider to be held accountable for a subscriber's infringing activity, yet does not provide any means to the proposed end goal." Wendy M. Melone, Note, *Contributory Liability for Access Providers: Solving the Conundrum Digitalization Has Placed on Copyright Laws*, 49 FED. COM. L.J. 491, 506 (1997).

[250] IITF WHITE PAPER, *supra* note 173, at 116.

[251] *Id.* at 177-200.

> work; identify attribution and ownership of a work; and manage or facilitate copyright licensing.[252]

1. *Technological Solutions for Digital Media*

Although many other solutions are still under development or refinement, there are many solutions that content owners can, and in fact do, use today. Some of the technological solutions discussed in the White Paper include digital fingerprinting, digital copy protection, and encryption. In addition, there are many other promising techniques that the White Paper either did not identify or sufficiently elaborate upon.[253]

One technological solution to copyright infringement identified by the White Paper involves the use of "digital signatures," or "digital fingerprints," unique identification codes that are embedded within the data structure of a digitally-rendered work.[254] Although digital signatures may be inserted into any computer file, they are currently used most commonly with images, where they are called "digital watermarks."[255] An author uses digital watermarking to embed copyright information within the work. The embedded information can

[252] *Id.* at 177-78.

[253] In fairness to the White Paper, it did note that: "In April 1995, the Working Group was compelled to place the Report in concrete form, and, thus, to stop adjusting the text with respect to just-received news. As a result, the Working Group has elected to . . . not discuss every possible technological development of which it recently became aware." IITF WHITE PAPER, *supra* note 173, at 6 n.15. Likewise, there will undoubtedly be additional solutions developed after this Comment goes to press.

[254] *See* IITF WHITE PAPER, *supra* note 173, at 189-90.

[255] The most common system is a proprietary technology called Digimarc. *See Welcome to Digimarc* (visited Apr. 4, 1998) <http://www.digimarc.com>. Digimarc is emerging as the de facto standard and is currently included in over 90% of all image editing applications. *See About Digital Watermarking* (visited Apr. 4, 1998) <http://www.digimarc.com/about_wm.html>. One very promising extension of this technology is a new system invented by Digimarc that will allow the author to automatically search the Web for infringing copies:

> Digimarc's new innovative MarcSpider™, the first service to search the World Wide Web for digitally watermarked images, enables Playboy to track images that have been re-posted on the Web. The MarcSpider crawls the Web, looking at hundreds of millions of pieces of information, locating Digimarc watermarked images and reporting back where and when they were found.

Digimarc Technology to Help Playboy Crack Down on Image Piracy Over the Internet (visited Feb. 21, 1997) <http://www.digimarc.com/pr016.html>. *See also infra* note 387 (describing several other systems that automatically scan the Internet).

be made transparent to the end user, can survive most file alterations, and, unless the author desires otherwise, does not interfere in any way with the use or viewing of the work. Although digital watermarking does not provide true copy protection, many other digital fingerprinting systems are being developed that would also prevent the unauthorized use or copying of the work. As digital fingerprinting technology matures, it promises to provide a simple, unobtrusive, and effective technological solution to infringement.[256]

Another solution described in the White Paper is the use of digital copy management systems, a technique that typically uses a combination of software and hardware.[257] Using such systems, a digital work is encoded to require the use of a specific combination of software and hardware. One popular hybrid hardware/software copy protection solution involves the use of a "dongle," a device that must be attached to the computer in order for the software to be used.[258] Without the required hardware device, a copy of the work itself is useless.[259]

Another technological solution to copyright infringement identified by the White Paper is the use of encryption technology to prevent unauthorized use of copyrighted materials.[260] Encryption offers

[256] *See, e.g.*, infra note 387.

[257] *See* IITF WHITE PAPER, *supra* note 173, at 189-90.

[258] *See generally* McCandless, *supra* note 6, at 178-79.

While generally offering quite secure protection, dongles are occasionally defeated. The manufacturer of one recently released dongle boasted that it would take 44,000 years to crack the hardware code. While this may be mathematically true, an ingenious cracker defeated the system only days after a dongle-protected program's release. Rather than attempting to actually break the code, the cracker instead altered the program to bypass its communication with the device. *See id.* at 178-79.

[259] One significant limitation of hybrid solutions, however, is that they inherently prevent the online delivery of a fully functional product. This limitation is at least partially offset if the vendor wishes to distribute a function- or time-limited version of the product as a "try-before-you-buy" demonstration version.

Another, and perhaps ultimately more problematic, limitation of such hybrid software/hardware solutions is that the hardware device must be constantly attached to the computer, potentially interfering with the use of other hardware devices attached to the computer. Since the potential for compatibility problems increases in proportion to the number of dongles attached to any particular computer, if every program were to implement such a solution, the problems might quickly swallow the benefits.

[260] *See* IITF WHITE PAPER, *supra* note 173, at 185-87.

One such system that has been successfully employed is Adobe Systems' "Type on Call" program. Adobe is a leading publisher of fonts (computer typefaces). Using the Type on Call system, the end user purchases an encrypted Compact Disc that contains over 2,100 copyrighted fonts. In order to use any of these fonts, however, the user must call Adobe or connect with them over the Internet in order to purchase an unlocking code. The user can purchase the codes for as many of the fonts as he would like. *See Adobe Type on Call Overview* (visited Oct. 18, 1997) <http://www.adobe.com/prodindex/typeoncall/main.html>.

virtually foolproof data security—modern encryption methods render a work invulnerable to attack from even the most sophisticated hacker.[261] Encryption by itself, however, only prevents unauthorized access to the original work. Once an authorized user decodes the work, it may be copied and distributed as easily as any other work.[262]

One very promising technological solution overlooked by the White Paper is the use of "smart card" technology.[263] As opposed to the familiar "dumb" magnetic stripe system used with credit cards, smart cards have a tiny embedded microprocessor that can store data and sophisticated encryption keys. Using a smart card copyright protection system, the owner of a work would be required to insert an authorized

Encryption may also be used to protect conventional text-based works. *See Ambia Corporation - Signet Document Security* (visited Feb. 17, 1998) <http://www.ambia.com/signet.htm>.

For a detailed explanation of one proposed system using encryption technology to provide copyright protection, see Ralf C. Hauser, *Using the Internet to Reduce Software Piracy* (last modified Apr. 4, 1995) <http://www.zurich.ibm.com/pub/sti/www/g-kk/publications/1995/hauser95.html>.

[261] Although theoretically one can simply generate random keys until one works (a so-called "brute force" attack), the following excerpt describes the impossibility of a brute force attack against a file encrypted with a relatively small 128 bit key:

> Let's say that you had developed a special purpose chip that could try a billion keys per second. This is FAR beyond anything that could really be developed today. Let's also say that you could afford to throw a billion such chips at the problem at the same time. It would still require over 10,000,000,000,000 years to try all of the possible 128 bit keys. That is something like a thousand times the age of the known universe!

Peter Simons, *Frequently Asked Questions - alt.security.pgp* § 3.2 (last modified Dec. 17, 1997) <http://www.pgp.net/pgpnet/pgp-faq/>. Modern key sizes, however, can be as large as 2,048 bits.

The security of encryption is such that all but the most elementary encryption methods are actually classified by the United States as "munitions" and their exportation is therefore forbidden. *See* Arms Export Control Act, 22 U.S.C. § 2778 (1997); International Traffic in Arms Regulations, 22 C.F.R. §§ 120-30 (1994). These export controls have been the subject of sometimes bitter dispute between the Government and software companies. *See* Rory O'Conner, *Encryption 'Scrambling' Plan Meets Cool Reception* (last modified Nov. 19, 1996) <http://www2.sjmercury.com/business/compute/encrypt1118.htm>.

[262] *But see Softlock at a Glance* (visited Mar. 16, 1998) <http://www.softlock.com/glance.html> (encryption system that automatically re-locks all copies, allowing them to be run only in limited-functionality "demonstration" modes until the recipient of the new copy purchases an unlocking code).

[263] For a detailed exposition of smart card technology, see *ASE - Aladdin Smartcard Environment* (last modified Jan. 27, 1998) <http://www.hasp.com/ase/ase.htm>. The White Paper did briefly mention smart cards, but only in the context of European personal banking systems. *See* IITF WHITE PAPER, *supra* note 173, at 193-94.

card before the work could be used. Copies of the work are worthless to anyone without that user's card. Smart card systems are inexpensive, simple, and virtually foolproof. Additionally, since the code in the card's microprocessor can be updated, a single card could be used for all programs, with its code being updated at the point of sale or, in the case of online purchases, over a secure encrypted connection. Although the card reader itself would be inexpensive and small enough to be implemented even in laptop computers, successful deployment would require the adoption of an industry standard card reader.[264]

Finally, the changing nature of computing itself may provide a partial solution to online infringement. One increasingly popular technology is the concept of "rented" applications.[265] Under this method, the end user does not actually purchase the program, but instead connects to a remote server and runs the program on that server. This method is very promising and offers benefits to both the end user and the program author. First, the program owner benefits by retaining possession of his work, making unauthorized copying impossible. Second, end users, especially businesses, benefit by only paying for the time that they need. Finally, a rental system enables end users to gain the benefits of even sophisticated programs that otherwise might be unaffordable to the cost of the applications or special hardware needed to run them.[266]

Another closely related technology, which many visionaries and market leaders believe is the future of computing, is the so-called "network computing" or "thin-client" system, which is, in essence, the "rented" application method taken to its logical extreme.[267] Under this system, the end user has an inexpensive stripped-down terminal (a "thin client" or "information appliance") consisting of little more than a

[264] A single software vendor could not unilaterally employ the smart card system because the expense of the cost of the card reader would be borne by its purchasers alone. If, however, the industry were to arrive at a consensus on smart cards, the cost of the card reader would not be identified with any single vendor.

[265] *See, e.g.*, Tim Clark, *Hot Market for Rent-an-app* (last modified Jan. 23, 1998) <http://www.news.com/News/Item/0,4,18368,00.html>. One such system is being advanced by Lotus Development, a pioneer in Internet technologies and security. *See Lotus Ships Domino SPA Tools to Enable Web Developers to Create "Rentable" Applications Based on Lotus Domino* (last modified Jan. 23, 1997) <http://www.internet.ibm.com/news/243e.html>.

[266] *See* Mary E. Thyfault, *App Hosting Plan* (last modified Feb. 23, 1998) <http://techweb.cmp.com/iw/670/70iuhst.htm>. Additionally, the user is assured of having access to the most recent version of the application, thereby eliminating the all too frequent problem of upgrading local software.

[267] *See generally Are Thin Clients Fat Opportunities?* (visited Feb. 22, 1998) <http://marketspace.altavista.digital.com/WebPort/English/I-School.asp?showContent=yes&ArticleId=50> (providing overview of various business and consumer thin-client technologies).

display, keyboard, and network adapter. The application programs are run and the data is saved on a remote server, rather than on the local user's terminal. The thin client approach is quickly gaining widespread acceptance in both business[268] and consumer[269] markets. Network computing possesses the same positive attributes to content providers as rented applications—an author would either retain physical possession of his work, requiring end users to run the program from the author's server, or the author would license or sell the work to other server administrators, who would presumably be far less likely to allow infringement of the work.[270] Not only do content providers retain better control of their works, but also the devices on the client side (diskless "information appliances") are incapable of creating infringing copies.

[268] "Intranets," secure internal company information networks based on Internet technology and software, are growing even faster than the Internet. *See generally Intranet - PC Webopaedia and Links* (visited Feb. 22, 1998) <http://www.pcwebopedia.com/intranet.htm>; *The Intranet FAQ* (last modified Feb. 10, 1998) <http://www.innergy.com/ifaq.html>. The thin client approach is ideally suited to the Intranet environment and several influential computer software and hardware producers have already begun shipping low-cost network computing terminals and server-side software. *See* Mitch Wagner, *Wyse Drops Thin-Client Pricing to $349*, TECH WEB NEWS (last modified Feb. 12, 1998) <http://www.techweb.com/wire/story/TWB19980212S0010>.

[269] Several consumer electronics companies have already experienced brisk sales of low-cost, diskless TV set-top "Internet terminals." *See, e.g.*, Christine MacDonald, *Prime Time for Net TVs* (last modified Jan. 8, 1997) <http://www.news.com/News/Item/0,4,6842,00.html>.

[270] Database publishers, for instance, are reluctant to make their data electronically available on the Internet, preferring the more secure environment of a direct subscriber relationship (*e.g.*, Westlaw and LEXIS):

> While the bulk of information products and services are still offered and used in hard copy formats, there is a steadily increasing demand for access to high quality and reliable data online over the Internet. Thus far, most IIA members producing content have limited their online distribution to secure, dedicated systems supported by a subscriber base. Access on these networks is generally controlled by the provider, and a relationship exists between producer and user. Such control is much less evident in many of the networks that constitute the Internet. Information providers are justifiably concerned that once their materials are placed on such open networks, unscrupulous or uninformed users will begin copying and redistributing the material without the same regard for property rights that has been established for copyrighted works offered in more traditional formats.

Prepared Testimony of Ronald G. Dunn, Pres., Info. Indus. Ass'n, Before the House Judiciary Comm., Courts and Intellectual Property Subcomm., Federal News Service, Sept. 16, 1997, *available in* LEXIS, Legis Library, Fednew File.

2. *Technological Solutions Available for Conventional Media*

Although some conventional media like prerecorded videotapes and Compact Discs employ copy-protection systems,[271] other conventional media like print documents and photographs remain vulnerable. Although there are several promising methods under development, few viable technological solutions have yet been proposed to protect works not originally generated in electronic form.[272]

Even though print media may remain vulnerable, the changing nature of content delivery will likely reduce losses due to online infringement. Over time, more traditional print media will migrate to electronic delivery, thus offering at least limited protection against online infringement since, assuming that there will be weak cross-elasticity of demand between print media and online media,[273] there will be a reduction in lost sales as print media migrate to online publishing. The fact that no single solution can currently protect all media should not, however, hinder the implementation of those systems that can provide substantial protection.[274]

[271] *See, e.g., Prepared Statement by Mark S. Belinsky, on Behalf of Macrovision Corp., on H.R. 2281, WIPO Copyright Treaties Implementation Act* (last modified Sept. 17, 1997) <http://www.house.gov/judiciary/4021.htm> (describing Macrovision's videocassette copy protection system used in the vast majority of prerecorded videotapes worldwide, as well as satellite television, cable television, pay-per-view, and Digital Video Disc copy protection systems); IITF WHITE PAPER, *supra* note 173, at 190 (describing "digital subcode channel" contained in digital sound recordings and broadcasts, used to prevent serial copying using digital audio recorders); Carol Levin, *It's a Fake! New Digital Fingerprints to Foil Software Pirates* (last modified Mar. 3, 1997) <http://www.zdnet.com/pcmag/news/trends/t970320a.html> (describing "DiscGard," a system that prevents CD and DVD duplication by "etching a digital fingerprint into the pits and lands of optical disks"; playback devices encoded with the system do not allow duplication and will thus "stop pirates in their tracks").

[272] Some progress has been made on systems that would print a very small digital fingerprint within a print article or image. If the work is then digitized, the fingerprint would be imported into the digital copy. *See, e.g.*, Andrew R. Sorkin, *Playboy Plans to Use Digital 'Watermarks,'* N.Y. TIMES CYBERTIMES (last modified June 30, 1997) <http://www.nytimes.com/library/cyber/week/063097playboy.html> (describing Playboy magazine's experiments with the digital fingerprinting of print images).

[273] At least one large print publisher seemed to indicate that this is the case: "Playboy is cracking down on suspected piracy of copyrighted property because it is launching a new subscription-based service in the next few weeks, which is in beta now." Macavinta, *supra* note 53.

[274] Some users will always be able to bypass any protection methods. "Copy-protection schemes are just speed bumps." McCandless, *supra* note 6, at 181 (quoting software executive). "There will never be a foolproof solution to what is at bottom an ethical problem." Levin, *supra* note 271 (quoting software industry representative). This is a reality of cyberspace that must be recognized and accepted.

3. *Summary*

The assertion that ISPs are in a better position than copyright owners to develop solutions to prevent infringement is simply not in accord with the facts. Proponents of strict liability have failed to identify any technological solutions that service providers can unilaterally implement, instead offering only vague speculation about what might be possible. In contrast, content providers have at their disposal many effective and time-tested technological solutions, as well as many other new technologies capable of immediate implementation.

Many content providers, most notably software suppliers, have successfully used technological solutions for many years.[275] Many software producers, however, have abandoned the once routine practice of copy-protecting their products. Although still widely used to protect recreational software, copy protection on business applications has been largely discontinued due to market pressures, predominantly from large businesses, to provide easier to use products.[276] This is not to suggest

[275] "To control unauthorized access, software publishers have long used passwords, serial codes and other similar systems, which must be correctly applied to a particular copy of a computer program before it can used." *Prepared Testimony of Robert W. Holleyman II, Pres., Bus. Software Alliance, Before the House Judiciary Committee, Courts and Intellectual Property Subcommittee, "Implementation of the World Intellectual Property Organization Copyright Treaty and the Balance of Responsibilities on the Internet,"* Federal News Service, Sept. 16, 1997, *available in* LEXIS, Legis Library, Fednew File [hereinafter *Holleyman Testimony on H.R. 2180 & H.R. 2281*].

[276] "Not all that long ago . . . most software programs came with copy protection embedded in code, but now very few have it because consumers rebelled against the notion that publishers would make it more difficult for them to use the software legitimately." Levin, *supra* note 271. *See also* Barbara Cohen, Note, *A Proposed Regime for Copyright Protection on the Internet*, 22 BROOK. J. INT'L L. 401, 411 (1996).

> In the mid-1980s, many software creators began to use copy protection devices in their programs. Although these methods were generally effective at thwarting unauthorized users, users nonetheless complained of the time and complexity involved in dealing with these devices, and they felt that the devices interfered with legitimate use of the software. The industry responded, for the most part, by leaving these devices off their products.

Id. (footnotes omitted). Similarly, in response to criticism that the SPA concentrates too much on legal solutions rather than technological solutions like cryptography or hardware dongles, Ken Wasch of the Software Publishers Association responded:

> Ten years ago there was a huge battle between the industry and users over copy protection. The last company to give up copy protection on a widespread basis was Lotus in 1987 when they sought a large order from the Defense Department. The users won.

that somehow software suppliers deserve to have their products stolen, but only to show that software producers, unlike service providers, have made a conscious economic decision that the benefits of vulnerability to piracy outweigh its costs. In contrast, the "affirmative policy decisions" to remain vulnerable to piracy supposedly made by ISPs may not be "decisions" at all, but merely the manifestation of their inability to effectively respond to the problem. Software producers that seek to impose liability on ISPs are, in effect, seeking to gain the benefits of copy protection without accepting the corresponding costs, instead shifting them to innocent parties far less capable of preventing the harm.

Most importantly, however, these technological solutions are capable of dramatically reducing the two sources of the greatest losses to the software industry – *corporate* software piracy and illegal commercial duplication plants in areas like the Far East. Unlike Internet piracy, whose participants frequently use and exchange pirated software "for the sheer thrill of it,"[277] corporate piracy and counterfeit copies represent *actual lost sales* to software producers. Despite the Software Publishers Association's history of strong rhetoric about the massive losses that Internet piracy inflicts upon software producers and its well-publicized lawsuits against small ISPs,[278] Ken Wasch, the SPA's President, recently admitted:

> . . . .
>
> Users did not want to be encumbered . . . by technical forms of protection . . . You can interview . . . any major company and they do not want copy protection of any sort because it restricts their freedom of deinstalling and reinstalling . . . every copy protection system known that has come forward somehow encumbers IS [information systems] managers from doing their job.

Ken Wasch interview, supra note 9. *But see Statement by Ken Wasch, President of Software Publishers Association, on Congressional Hearings to Address Software Piracy, supra* note 190 ("[O]ur only weapons against piracy have been litigation and moral suasion.").

[277] *See* Shapley, *supra* note 13. *See also* McCandless, *supra* note 6, at 134-35 (describing Internet software piracy as "a game," "a hobby," and "like stamp collecting").

[278] The Software Publishers Association (on behalf of its large software company members) has filed numerous suits against very small service providers. *See, e.g.*, Lance Rose, *SPA Copyright Bullies Shake Down the Web* (visited Nov. 11, 1997) <http://www.cyberlaw.com/spabull.html> (extremely critical article by prominent Internet attorney and author); Jonathan Wallace, *An Open Letter to the SPA* (last modified Dec. 1996) <http://www.spectacle.org/1296/spa.html> (another critical article written by an Internet lawyer); Mike Godwin, *Foul Play* (last modified Feb. 1997) <http://www.internetworld.com/print/monthly/1997/02/law.html>; Will Rodger, *SPA Withdraws Piracy Lawsuits* (last modified Nov. 25, 1996) <http://www5.zdnet.com/zdnn/content/inwk/0327/inwk0031.html>. The SPA Web site contains a page with hyperlinks to press releases detailing its current lawsuits against ISPs, of which virtually all are small local providers. *Anti-piracy Press Releases* (visited Mar. 16, 1998) <http://www.spa.org/piracy/pirnews.htm>.

> We don't think that the [Internet software pirates] really affect our industry that significantly. The biggest losses to the industry are in businesses where companies don't put management procedures in place to protect against software piracy. That's where the loss is . . . where they buy five copies of Lotus 1-2-3 and run it on twenty machines . . . It's mostly corporate users [who are abusing the copying privileges] . . . The other big loss to our industry is [foreign] CD pressing plants.[279]

The statistics support Mr. Wasch's observation. Approximately three-quarters of all software applications sold are business applications (non-recreational software such as word processors), yet sales to consumers only account for less than four percent of business software sales.[280] Therefore, even assuming arguendo that individual users illegally obtained one out of every two business applications currently in use, and Internet piracy accounted for every one of these illegal copies, completely stopping software piracy on the Internet would only increase revenues to business software producers less than four percent. Although providers of recreational software and other works may well be suffering proportionately greater losses,[281] and, as previously noted, a cultural shift towards disrespect of intellectual property rights in general would have disastrous effects on our economy, we must be cautious about

[279] *Ken Wasch interview, supra* note 9.

[280] *See Building an Information Economy: Software Industry Positions U.S. for New Digital Era*, at 18 n.12 (last modified July 1997) <http://www.bsa.org/info/econstudy.htm>.

[281] It is likely that recreational software producers suffer proportionately greater losses from online piracy, since it is doubtful how many users would actually purchase some of the expensive business applications that are commonly pirated on the Internet. This increased likelihood of lost sales, however, must be weighed against the fact that business applications are much more expensive on a per-copy basis, so, other things being equal, more recreational applications would need to be pirated in order to produce the same dollar losses to their producers. Perhaps the most disproportionately impacted group of all, however, are producers of smaller applications, both business and recreational, since their products are easier to exchange over the Internet, yet they are typically smaller companies that can least afford to have lost sales. "[P]iracy affects the small [software] companies most. . . there are a lot of small companies that need every user to have actually purchased the product." *Ken Wasch interview, supra* note 9. *See also Prepared Statement of the Honorable Howard Coble, Chairman, Before the House Judiciary Comm., Subcomm. on Courts and Intellectual Property, Regarding Electronic Copyright Piracy and the "No Electronic Theft (NET) Act,"* Federal News Service, Sept. 11, 1997, *available in* LEXIS, Legis Library, Fednew File ("It is self-evident that this transgression—the unauthorized access to a company's products—has even greater potential to ruin small, start-up companies. Let us not forget that small businesses still comprise that sector of our national economy which provides the most employment opportunities for American citizens.").

enacting policies that may have a significant negative impact upon all information consumers in order to provide benefits to relatively discrete segments of our economy. Additionally, there are signs that the increasing threat of Internet piracy is forcing content providers to rethink their cost-benefit analysis of technological solutions, a choice that is not available to Internet service providers.[282]

E. Strict Liability and Incentive Shifting

Proponents of strict liability for service providers have supported their arguments by pointing out that the economic incentives provided by strict liability tend to automatically force producers to arrive at the most economically efficient balance of cost and safety:

> [W]e need a behavioral control that will bring about the optimal result by forcing the relevant parties to determine the best precautions themselves. . . . In fact, one of the principal differences between negligence liability and strict liability is that strict liability removes the cost-benefit calculation from the court and imposes it on defendants. Here that means that strict liability will force [service providers] to determine the most advantageous mix of preventative measures . . . .[283]

This argument is grounded in the fundamental axiom of law and economics that incentives to prevent harm should lie with the party best able to prevent the harm. When applied to products liability, where the victim cannot casily prevent the harm, this principle mandates that the "optimum result" is obtained when manufacturers are forced to assume absolute responsibility for the safety of their products. When applied to the question of service provider liability, however, this principle may dictate a different result since *both* "relevant parties" have the ability "to determine the best precautions." As has been shown, however, while service providers have few effective tools to combat infringement, content providers have available a wide variety of effective "preventative measures" to guard against unauthorized uses of their products.

1. The Rationale for Strict Liability Turned on its Head

When, as with content providers, the victim is in possession of the most efficient means of preventing the harm, the rationale for strict

[282] "Today, software developers authors and publishers *are increasingly relying* on encryption, scrambling, passwords, and other similar means to control access to copies of works. These systems render the software unusable until the correct password or process is used to render it operative." *Holleyman Testimony on H.R. 2180 & H.R. 2281*, *supra* note 275 (emphasis added).

[283] Morril & Eaton, *supra* note 173, at 5.

liability for service providers is turned on its head. As observed by Judge Posner:

> [P]otential injurers subject to a rule of strict liability will automatically take into account possible changes in activity level, as well as possible changes in expenditures on care, in deciding whether to prevent accidents. . . .
>
> . . . .
>
> The problem with using this analysis to support a general rule of strict liability is that changes in activity level by *victims* are also a method of accident avoidance, and one that is encouraged by negligence liability but discouraged by strict liability. . . . Thus, strict liability encourages activity-level changes by potential injurers but discourages them by potential victims, while negligence liability encourages activity-level changes by potential victims but discourages them by potential injurers.
>
> If a class of activities can be identified in which activity-level changes by potential injurers appear to be the most efficient method of accident prevention, there is a strong argument for imposing strict liability on the people engaged in those activities. And, conversely, if there is a class of activities in which *activity-level changes by potential victims* are the most efficient method of accident prevention, there is a strong argument for no liability. . . .[284]

It would be an economically unsound policy to impose strict liability on service providers. Only through distorting the distribution of incentives calculus by ignoring the vastly superior position of service providers to prevent the harm can one reach the conclusion that the economic incentives to prevent infringement are best borne by service providers.

The costs of any product, including internalized losses, are ultimately borne by either the consumers or producers of that product. In the absence of strict liability for service providers, the costs of infringement are internalized by content providers. The availability of infringing copies of a work diverts demand away from the provider's distribution channels. Content providers must therefore either charge higher prices for their products, thus passing the costs on to their consumers, or, if the costs cannot be passed on, accept lower profits. These market forces create incentives for content providers to either implement better protection systems or suffer defeat at the hands of more capable new entrants into the market. The current liability system properly imposes incentives upon content providers since they have the capability to effectively respond to those incentives.

[284] RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 177-78 (4th ed. 1992).

If strict liability were imposed on ISPs, they would face similar market pressure as they internalize the increased costs of providing information access. ISPs would therefore face increased incentives to prevent infringement, yet, unlike content providers, would be unable to effectively respond. New market entrants would fare no better. Thus, the cost of information access would increase with little prospect of technology to bring costs back down.

Thus, while losses from infringement will always provide *some* level of incentive to the copyright holder, even a massive increase in economic incentives placed upon ISPs would not be sufficient to offset even a small reduction in incentives to copyright holders because of the gross disparity in their relative abilities to respond to those incentives.[285] Strict liability for service providers would therefore merely shift the costs of infringement from one group of consumers (content purchasers) to another (information access purchasers). Content providers, however, have a much greater opportunity to minimize the costs that their consumers must eventually bear.

2. *The Threat to Affordable Access to Information*

It must also be remembered who will bear the ultimate costs of the unwise incentive shifting that would result from imposition of strict liability on service providers – information consumers. Increased information costs would threaten the growth of an increasingly important segment of America's economy. It is difficult to overstate the importance to our future of the continued growth in America's information infrastructure. More than half of all America's workforce is employed in information-related industries.[286] Communications and information technology are the quickest-growing sectors in the American economy.[287] Businesses, including those outside the information sectors, are quickly beginning to see the potential for growth presented by participation in online commerce.[288] Affordable access to the Internet is of special importance to small businesses, as presence on the World Wide

[285] *See generally* Byron F. Marchant, *On-Line on the Internet: First Amendment and Intellectual Property Uncertainties in the On-Line World*, 39. HOW. L.J. 477, 500-03 (1996).

[286] IITF WHITE PAPER, *supra* note 173, at 10.

[287] *Id.*

[288] A February 1998 study reported that online purchases per user increased 250% from 1996 to 1997. *Latest Intelliquest Survey Reports 62 Million American Adults Access the Internet/Online Service*, *supra* note 2. Further, these purchases only represent a minority of the true economic impact of online shopping; while only 17% of users purchased goods online, nearly 60% used the Internet to gather information about product pricing, features, and retail locations. *Id.*

Web allows smaller businesses to compete on substantially equal footing to their larger competitors.[289]

In addition to providing economic benefits, affordable access to information provides immeasurable educational opportunities to all Americans. Even those without the financial means to afford formal education can have access to a wealth of knowledge and opinion. People with disabilities can access vast amounts of information without traveling to a library. Americans in rural communities can have access to educational materials that they would otherwise be unable to obtain. Impoverished children will no longer be at a disadvantage because their parents cannot afford to furnish them with the latest educational materials. In short, by removing economic and physical barriers, affordable access to information can help level the playing field for all Americans.[290]

Yet universities, libraries, and other free or low cost providers would suffer the greatest impact from the increased costs of strict liability. It is likely that many would simply eliminate free access in order to avoid liability for a service for which they are not receiving revenue.[291]

[289] The Internet allows even very small businesses to offer their goods and services to a worldwide audience:

> The biggest winners [from growth in Internet commerce], aside from consumers, are likely to be small and mid-size businesses. Simply put, network technologies enable all businesses to compete in national and international markets by dramatically reducing their barriers to entry. Until recently, only large companies could afford the costs involved in far-flung business operations. The Internet has already changed this scenario.

Wasch Testimony on H.R. 2180, supra note 28.

[290] Increased information access costs will only add to the widening gap between the rich and poor in America:

> Faced with significant financial liability, most online service providers would simply stop providing such services. Or, for those that did continue, the added costs of staying in business—setting up monitoring systems, hiring hoards of copyright attorneys, and paying the damages anytime a decision to remove a user or content from the internet was wrong—would transform the internet from a robust low-cost competitive commodity available to many to a high-cost luxury available to only a few. Even this best-case scenario widens the gulf between the information "haves" and "have nots" in a way that ultimately will harm the whole economy and undermine the public policy goal of universal access to information.

Copyright Liability for Online Access Service Providers (visited Mar. 3, 1997) <http://www.ahccoalition.org/cn/liability.htm>.

[291] In addition to concerns about its chilling effect on "scholarly communications," educational institutions have expressed concern that strict liability will interfere with

Further, providers of rural Internet access would be disproportionately affected, as they face much higher costs than metropolitan area providers.[292] Increasing costs would disproportionately affect those most in need of affordable information access.

a. The Magnitude of the Threat

While the potential impact of strict liability on affordable information access defies accurate measurement, most industry analysts agree that the cost of Internet access is virtually certain to significantly increase.[293] The White Paper and other commentators have extrapolated that, since other businesses historically subject to strict liability for copyright infringement have not been put out of business, the threat to Internet service providers has been overestimated.[294] As one commentator

their role as "the public's 'on-ramps' to the information superhighway":

> Without reasonable insulation from liability based solely on the activities of school and library network users over which our institutions have no control, educational and library institutions may be forced by the prospect of crippling liability to call a halt to building new, or to dismantle or disable existing, access points to the Internet.
>
> Copyright law should uphold the principle that liability for infringing activity in the network environment rests primarily with the infringing party rather than with third parties. Companies and non-profit institutions should accept responsibility for acts undertaken at their behest, but should not be held liable for the acts of individuals—whatever their association—who act independently. This principle is an essential underpinning of robust information commerce as well as academic freedom.

Prepared Testimony of Prof. Robert L. Oakley, Georgetown University Law Ctr., Before the House Judiciary Comm., Courts and Intellectual Property Subcomm., Regarding Service Provider Liability by Library, Educational, and Scholarly Associations, Federal News Service, Sept. 16, 1997, *available in* LEXIS, Legis Library, Fednew File [hereinafter *Oakley Testimony on H.R. 2180 & H.R. 2281*].

[292] The U.S. Telephone Association, an organization of 1,400 local telephone companies (of which virtually all are also ISPs), has expressed great alarm over the continued viability of rural Internet access:

> [T]he ISP service USTA [U.S. Telephone Association] members provide particularly in rural areas, is usually the only opportunity consumers living in these areas have to access the Internet. . . . [R]ural Internet service is not a major revenue producer. Unlike local telephone service, rural Internet access is not subsidized . . . Margins for Internet access to rural consumers are extremely small. So, while USTA members are committed to the Internet, the threat of copyright lawsuits is becoming an increasingly salient consideration in offering the service at all.

Neel Testimony on H.R. 2180, *supra* note 220.

[293] *See, e.g.*, Elizabeth Weise, *Access Providers Rethinking Flat-Rate Pricing for Internet*, N.Y. TIMES CYBERTIMES, (last modified Jan. 12, 1997) <http://www.nytimes.com/library/cyber/week/011297flatrate.html>; Murphy & Hofacker, *supra* note 231; Lewis, *supra* note 231.

[294] *See, e.g.*, IITF WHITE PAPER, *supra* note 173, at 116-17; Charles H. Kennedy, *Is the Internet a New Legal Frontier?*, 39 HOW. L.J. 581, 583-84 (1996).

noted: "The risk of liability under present law appears not to have put photo finishers, copy centers, and book stores out of business, and certainly has not prevented the explosive growth of the Internet."[295]

This argument is vulnerable to attack on several grounds. First, the yardstick employed is unreasonably crude. The question is not whether access to the Internet will perish, but rather whether access will remain affordable. Simply because providers have not been put out of business does not mean that the costs associated with liability are not significant. Second, content providers have also enjoyed "explosive growth" as a result of the Internet and do not appear to be in jeopardy of going out of business either.[296] In fact, it defies logic that, if Internet piracy were that great of a threat, content providers would not have already responded by implementing (or re-implementing) some of the many effective technological solutions at their disposal.

Further, the comparison of Internet providers with photo finishers, copy centers, and retailers leaves much to be desired. Photo finishers and retailers can more easily detect the presence of infringing materials since they have at least some opportunity to visually examine the products for which they are liable. In contrast, visual inspection of a digital data stream is not possible.[297] Even for content resident on an

[295] Kennedy, *supra* note 294, at 584. *See also* IITF WHITE PAPER, *supra* note 173, at 116-17; *Kenswil Testimony on H.R. 2180*, *supra* note 201.

> Printers make "reproductions" under the Copyright Act every minute as part of their ordinary business, and they cannot know whether all or some of the materials they are reproducing are infringing someone's rights. . . . Yet there is no printer exemption in the Copyright Act. Bookstores, too, are technically at risk that they are committing or contributing to copyright infringement by virtue of their ordinary, day-to-day business operations. They cannot know the content of every book they sell, and whether any of it is infringing. . . . Yet there is no bookstore exemption in the Copyright Act. And the same can be said for CD pressing plants, record retailers, book and magazine publishers, TV broadcasters, and scores of others. What makes Internet Access Providers any different?

Id.

[296] "If you find me a copyright holder that's been pushed to the brink of bankruptcy by the Internet, then we have something to talk about." Paul Heltzel, *Use a Floppy, Go to Jail* (last modified August 1, 1997) <http://www.pcworld.com/news/daily/data/0897/970801175655.html> (quoting Mike Godwin, staff counsel for the Electronic Frontier Foundation).

[297] As observed by one service provider:

> In a traditional copyright situation, for example, a publisher or a distributor of material has the ability to check and confirm whether the material is an authorized copy, and can choose not to distribute questionable material prior

ISP's servers, the comparison is not fair. The cover of a CD or book reveals far greater information than does the typical eight-character computer file name. Additionally, the potential liability for an ISP is an order of magnitude greater than that faced by a photo finisher, retailer, or copy center.[298] For example, assume that two infringers are simultaneously copying a copyrighted image. Infringer A is at the local copy center, furiously photocopying the image. Infringer B is at home, scanning the image into his computer. In just a few seconds, B can connect to the Internet and upload the scanned image. In the same period of time, infringer A has made only a few copies, but B may have created liability for thousands of copies. Thus, Internet providers can be subjected to much greater liability, yet they have far less ability to prevent the harm.

b. The Shortcomings of the Innocent Infringer Doctrine and Indemnity

Advocates of strict liability also contend that the threat of ISP liability is overstated because ISPs are protected from massive liability by the "innocent infringer" doctrine, which allows a court to reduce a damage award to as little as $200 for unintentional infringement.[299] This is a

> to triggering any copyright liability. Many entities involved in electronic communications do not have that luxury—millions of messages are transported daily and pre-screening for infringing communications is both technically infeasible and practically impossible. Service providers, like the telephone company or an express delivery service, are conduits for information generated and distributed by others, rather than electronic bookstores that select and present particular texts, while declining to market other texts.

Purcell Testimony on H.R. 2441, *supra* note 223.

[298] The White Paper recognized that the Internet could cause much greater *losses to authors* than conventional copying media:

> Authors are wary of entering [the online distribution market] because doing so exposes their works to a higher risk of piracy and other unauthorized uses than any of the traditional, current modes of dissemination. . . . Just one unauthorized uploading of a work onto a bulletin board, for instance—unlike, perhaps, most single reproductions and distributions in the analog or print environment—could have devastating effects on the market for the work.

IITF WHITE PAPER, *supra* note 173, at 178 (emphasis added). It seems disingenuous for the White Paper to later minimize the fact that the Internet could also cause much greater *liability to service providers*.

[299] *See, e.g.*, Morril & Eaton, *supra* note 173, at 3.

> [S]trict liability still permits consideration of relative culpability at the sanction stage: the sanction imposed on an "innocent [copyright] infringer" may be limited to a $200 fine. Therefore, . . . applying direct copyright infringement to on-line service providers in connection with the infringing activities of their subscribers should not seriously impede the growth of the Internet . . .

Id. See also IITF WHITE PAPER, *supra* note 173, at 119-20; Kennedy, *supra* note 294, at 583-84. The "innocent infringer" doctrine is defined in section 504 of the Copyright specious argument that ignores the realities of modern litigation; the threat of a nominal fine pales in comparison to the thousands of dollars required to defend even a meritless case. Successful plaintiffs are also usually awarded their costs and attorney fees.[300] Thus, even an "innocent" ISP will likely be saddled with paying the entire cost of the litigation. The innocent infringer defense offers no real protection from exposure to substantial liability, which is especially devastating for small providers.[301]

Proponents of strict liability for ISPs also frequently suggest that subscriber indemnity agreements would substantially reduce ISP losses.[302] This is also unrealistic, as subscribers will frequently be unable to make good on their promise. Even if the subscriber secures his account with a credit card, ISPs would often be unable to recover indemnity in excess of the credit line. Even assuming minimal litigation expenses and a minimal damage award, the costs to the ISP would routinely be greater than it could recover. Finally, since much of the

Act:

> In a case where the infringer sustains the burden of proving, and the court finds, that such infringer was not aware and had no reason to believe that his or her acts constituted an infringement of copyright, the court in its discretion may reduce the award of statutory damages to a sum of not less than $200.

17 U.S.C. § 504(c)(2) (1997).

[300] Attorney's fees awards "are the rule rather than the exception and should be awarded routinely." Playboy Enters., Inc. v. Webbworld, Inc., 968 F. Supp. 1171, 1177 (N.D. Tex. 1997). Attorney's fees, however, are only available to plaintiffs who registered the work prior to the infringement. *See* 17 U.S.C. § 412 (1997).

[301] *See, e.g., Purcell Testimony on H.R. 2441*, *supra* note 223.

> Without a clear, realistic standard, Internet access and service provision will become the sole purview of the telecommunications giants that can afford to absorb and settle large liability claims. The threat of legal fees alone could exclude entrepreneurial and niche providers from the market.
>
> . . . .
>
> As an entrepreneur in a competitive industry, I can assure you that defending a copyright lawsuit is an expense that could easily destroy a small business. Recently, an access-only provider in Northern Virginia was sued by a copyright owner under a theory of copyright infringement. Although the service provider settled before trial, just a few months of litigation preparation represented a large chunk of its annual revenue. This is a burden that most providers are unable to undertake, particularly if they can do nothing to minimize their liability.

Id. (presumably referring to *Religious Tech. Ctr. v. Lerma*, 908 F. Supp. 1362 (E.D. Va. 1995)).

[302] *See, e.g.*, IITF WHITE PAPER, *supra* note 173, at 178; Morril & Eaton, *supra* note 173, at 4.

content on an ISP's servers comes from outside its system, an ISP may not be able to locate, much less obtain indemnity from, the actual infringer.

Perhaps the most persuasive argument that the threat of increased costs may be overstated is that, so far, no truly "innocent" ISP has been held liable for copyright infringement in any reported decision.[303] This argument ignores the fact, however, that none of these decisions have any binding effect, as none have advanced to an appellate court. Further, these "inconsistent federal district court decisions hardly constitute a model for orderly relationships and business certainty."[304]

3. The Need for Alternatives to Liability-Based Incentive Distribution

Imposing strict liability upon Internet service providers would be an economically unwise policy choice. Most arguments in favor of strict

[303] *See, e.g., Prepared Statement of Michael K. Kirk, Exec. Dir., Am. Intellectual Property Law Association, Before the House Comm. on the Judiciary, Subcomm. on Courts and Intellectual Property*, Federal News Service, Sept. 17, 1997, *available in* LEXIS, Legis Library, Fednew File.

> Our threshold problem . . . is that it is difficult to identify jurisprudence which makes the issue of on-line liability a real problem as opposed to a perceived problem. . . . We are not aware that a single [online service or Internet access provider] has ever been found liable for copyright infringement on the Internet. . . . Do we have a solution in search of a problem?

Id. This sentiment was echoed by a representative from the music industry:

> IAPs claim they are at risk for being held liable for "massive damages" and "face the prospect" of being adjudged culpable for infringement. But these are hypothetical risks only, not borne out in practice. Nor are we aware of any onslaught of debilitating lawsuits that threaten the very foundation of the Internet. To date, we count only a dozen or so decisions dealing with copyright liability on the Internet—and only a couple of them have involved IAPs. And the one decision dealing directly with the issue of IAP liability came out on the side of the IAP.

Kenswil Testimony on H.R. 2180, supra note 201.

[304] *Hearings on H.R. 2441, supra* note 160, at 250 (statement of Stephen M. Heaton, Gen. Counsel and Sec., CompuServe, Inc.) *See also Prepared Statement of David Nimmer, Irell & Manella, LLP, Los Angeles, on Behalf of the U.S. Tel. Ass'n, Before the House Comm. on the Judiciary, Subcomm. on Courts and Intellectual Property, Concerning H.R. 2265*, Federal News Service, Sept. 11, 1997, *available in* LEXIS, Legis Library, Fednew File.

> The lesson from that trio of cases [*Frena, Sega v. MAPHIA*, and *Netcom*] is that standards are only beginning to emerge for the level of duty that an ISP bears with respect to copyright infringement that crosses its services. Moreover, the different standards articulated by the district courts have yet to reach appellate review.
>
> In such a climate of confusion, the danger facing an ISP is that it can have no certainty, for example, that the standard enunciated in [*Frena*] will be rejected by other courts.

Id.

liability for service providers are grounded in the mistaken assumption that ISPs can effectively control content on their systems. Once this premise is stripped away, these arguments fail. Since the costs of injury should be internalized by those parties who can best respond to the consequential economic incentives, economically sound policy dictates that losses from infringement should continue to be borne by content providers, who are in a far better position to respond to the incentives.

Additional economic and social policy considerations weigh in favor of limiting the potential liability of Internet service providers. Affordable access to information is vital to America's continued leadership in information technologies. Potentially massive liability for service providers could force nonprofit institutions and rural providers to terminate free or low cost access, harming those who need it most.

This potentially massive liability to ISPs is, of course, due to the potentially massive damages to copyright owners. Therefore, it may properly be said that providing Americans with continued affordable access to information should not come at the expense of copyright owners.[305] Although all who are injured deserve compensation, any policy that myopically focuses on compensation necessarily misses the mark when applied to the realm of copyright. The substantive goals of tort and copyright are fundamentally different. While the driving force behind strict liability is the removal of the economic consequences of accidents, compensation for injury is only a collateral aim of copyright.[306] The goal of copyright is to promote innovation and creativi-

[305] As noted by a major publisher:

> No one—least of all those of us in the business of providing information—wants our society to devolve into segmented classes of information "haves" and "have-nots." However, ensuring that those who cannot afford to pay for information nevertheless have access to it is a broader societal responsibility, not one that should be borne primarily—let alone exclusively—by copyright owners.

Hearings on H.R. 2441, *supra* note 160, at 75 (statement of Barbara Munder, Senior Vice Pres., The McGraw-Hill Cos., Inc.).

[306] The purpose of copyright is "To Promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." U.S. CONST. art. I, § 9.

> [C]opyright law . . . makes reward to the owner a secondary consideration. . . . "'The sole interest of the United States and the primary object in conferring the monopoly lie in the general benefits derived by the public from the labors of authors.' It is said that reward to the author or artist serves to induce release to the public of the products of his creative genius."

ty.[307] The Internet, however, promises to accelerate the growth of innovation and creativity faster than any force in the history of mankind. The result of a policy that goes too far in pursuit of compensating copyright holders, thereby unwisely shifting economic incentives and costs, may therefore result in a net loss of innovation and creativity, a result contrary to copyright's fundamental goal.

Framing the argument in this way, however, presents a false dilemma—content providers and service providers must *both* prosper in order for *either* to prosper:

> Copyright holders, content providers and Internet access providers have a mutually dependent relationship—quality online content increases demand for Internet access, while increased Internet access increases the demand for quality online content. Absent significant cooperation among content and access providers, the Internet can easily dissolve into a muddle of competing and parochial interests.[308]

Content providers and access providers, rather than viewing each other as adversaries in a zero-sum game, must be encouraged to work together to develop new and more secure methods to ensure the widespread availability of online content. Both sides are becoming aware that the key to success is the development of systems and procedures that will minimize losses to both service providers and copyright holders. Content providers are beginning to realize that the adversarial relationship that has in the past defined the debate is counterproductive to the development of such systems.

> On the Internet and other networks, software publishers and telecommunications service providers will be partners, and each should learn to value the contribution the other will make to success on the Internet. Therefore, [the Software Publishers Association] is deeply interested in any change in existing law that could make that fight more difficult or less effective, and would appreciate the opportunity to speak with interested Members of Congress and organizations about such efforts.[309]

Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417, 429 (1984) (citations omitted).

[307] It is important to remember that the monopoly granted by copyright is also accompanied by statutory provisions limiting that monopoly.

> Copyright is at root about promoting creativity. . . . creativity results not just from the financial incentive for authors and inventors codified in Title 17 of the U.S. Code, but also from many provisions in the statute which promote access to copyrighted information. The best measure of our copyright law's success is whether it fairly balances those equal priorities in the service of the Framer's commitment to the broad dissemination of knowledge and information in a democracy.

Oakley Testimony on H.R. 2180 & H.R. 2281, *supra* note 291.

[308] *ITAA Discussion Paper*, *supra* note 25, at "Executive Summary."

[309] *Hearings on H.R. 2441*, *supra* note 160, at 85 (statement of Garry L. McDaniels, Pres., Skills Bank Corp., on behalf of the Software Publishers Ass'n).

What is clearly needed is a liability regime that provides for the proper distribution of economic incentives upon both content providers and service providers. Strict liability for service providers fails to properly distribute these incentives, as too much incentive is placed upon the shoulders of those least able to effectively respond. Likewise, unqualified exemption from liability for service providers also fails to properly distribute these incentives, as too little incentive is provided for service providers to assist copyright owners.

Rather than distributing incentives based upon inappropriate analogies imported from products liability doctrine, we need a legal framework that distributes the incentives in the specific areas where each party possesses the required expertise to effectively respond to them. Service providers specialize in the storage and transmission of data, irrespective of its content.[310] As one Web site developer noted, "I would rather partner with those of my clients who have intellectual property to protect that property via TECHNOLOGY rather than be forced out of my core competency because the law requires that I invest in hiring more lawyers than programmers."[311]

This is not to say, however, that ISPs do not play an important role in controlling intellectual property theft on the Internet. On the contrary, ISPs are in a unique position to assist copyright owners both in the identification of infringing parties and in the implementation of *author-developed* protection schemes.[312] But content providers must take the

[310] As observed by one service provider:

> Even if the [online service] boldly sets out to resolve the thorny questions of an alleged infringement, it is thereby taking on a task it is not well suited to do (because it is in essence a distributor and network access provider, not a creator or editor of copyrighted works)—and it inevitably becomes a de facto arbiter of copyright disputes that are truly between others. . . .
>
> . . . .
>
> The intensive factual investigation and legal copyright analysis should not be required of online companies regarding the infringement of others. OLS companies are not particularly well equipped to do this analysis; in fact, the copyright owner is far better equipped; and it is a completely unacceptable shifting of the burdens of ownership of private property away from the proprietor—who retains all the benefits of ownership.

Hearings on H.R. 2441, *supra* note 160, at 254-56 (statement of Stephen M. Heaton, Gen. Counsel and Sec., CompuServe Inc.).

[311] *Patel Testimony on H.R. 2180 & H.R. 2281*, *supra* note 215.

[312] As noted by a music industry executive:

initiative to develop technological solutions to infringement, as only they possess the expertise to identify whether a work is infringing.

> [O]nly the content owner or his agent can ever know for sure what is an authorized use. And even if a telco or ISP had a strong suspicion that a work is infringing based on the title of a site, the content owner is in a better position to make that judgement. Technology is currently available for content owners to search for infringements, *since they actually know what they are looking for.*[313]

As correctly observed by one entertainment industry executive: "[ISPs] and other telecommunications companies have a key role to play . . . [and] must shoulder their fair share of this burden. Of course copyright owners must take the lead. Our vigilance is essential. Internet piracy demands that we become the watchmen on the tower."[314]

It should be apparent that the current legal environment presents a poor forum for the development of any such solutions. A system of distributing incentives based on the threat of liability is antithetical to the cooperation of the litigants, yet this cooperation is essential to the development of the Internet as a secure and robust environment for commerce. The answers to the current questions raised by the ISP liability question cannot be found in existing case law or tort doctrine. A fresh and comprehensive approach to this new and challenging problem is needed.

V. RECOMMENDATIONS

ISP regulation is not a matter that should be left to the courts. There are too many questions, many quite technical in nature, that demand a definitive legislation solution. Each claim brought in these relatively uncharted legal waters therefore requires the trier of fact to attempt to understand intensely technical issues, to render what amounts to

> Just as technology has created this new threat of piracy on the Internet, so too can it solve the problem it has wrought. Precisely how, or when, remains unclear. But one conclusion appears inescapable: We will not be able to protect our music entirely on our own; encryption and other unilaterally-applied technology measures will not prevent any Internet user from taking any of the 4.7 billion CDs already out in the marketplace and uploading the music on them to the Internet, where it will become available to millions of downloaders worldwide. Virtually any technology used to protect our music will be *bilateral*, requiring hardware or software on the Internet or in computers to look for and act upon the technological protection measures encoded in our recordings. We need the cooperation of the online and Internet service providers . . . to help us protect our works. We cannot do it alone.

Kenswil Testimony on H.R. 2180, *supra* note 201 (emphasis added).

[313] *Neel Testimony on H.R. 2180*, *supra* note 220 (emphasis added).

[314] *Valenti Testimony on H.R. 2180 & H.R. 2281*, *supra* note 8.

scientific findings,[315] and to then apply those findings to laws that do not clearly define the rights and responsibilities of the litigants. Is it realistic to expect judges and juries to be able to consistently decide these complex issues?

> Determining which types of ISPs should be liable in which situations for copyright infringement requires a degree of technological sophistication that even the federal courts do not have. To date, the courts still have not differentiated between ISPs, BBS operators, and Web page operators. However, Congress, with almost unlimited access to technology experts and the time to extensively study the issues, is well-equipped to craft a technologically sophisticated solution for the online world.[316]

Even after the courts have waded through the thick technical issues and identified the legally relevant facts, they are then confronted with the daunting task of applying those facts to statutes that do not adequately guide them. As noted in the White Paper:

> It is difficult for intellectual property laws to keep pace with technology. When technological advances cause ambiguity in the law, courts look to the law's underlying purposes to resolve that ambiguity. However, when technology gets too far ahead of the law, and it becomes difficult and awkward to adapt the specific statutory provisions to comport with the law's principles, it is time for reevaluation and change. "Even though the 1976 Copyright Act was carefully drafted to be flexible enough to be applied to future innovations, technology has a habit of outstripping even the most flexible statutes."[317]

Finally, and perhaps most importantly, since the application of copyright to cyberspace has profound policy implications, yet is wholly statutory,

[315] *See supra* note 18 (describing the lengthy technological discussions in recent Internet-related court opinions).

[316] *Hearings on H.R. 2441, supra* note 160, at [page] (statement of William J. Cook, Attorney, Willian, Brink, Hofer, Gilson & Lione). "Reasonabilility" is particularly difficult to determine in unfamiliar factual settings.

> [A] broader issue related to the "cyberspace community" standards question is what the "reasonable" person would do in a given circumstance. The concept of reasonableness is pervasive in Anglo-American law, especially tort law. There is no inherent reason why the concept cannot apply in cyberspace. The problem is that in many situations, juries—and even cyberspace users themselves—may not know and may have no basis for knowing what is reasonable in cyberspace.

Hardy, *supra* note 206, at 1013.

[317] IITF WHITE PAPER, *supra* note 173, at 211 (quoting H.R. REP. NO. 101-735, 101st Cong., 2d Sess. 7 (1990), *reprinted in* 1990 U.S.C.C.A.N. 6935, 6938 (report accompanying legislation granting copyright owners of computer software an exclusive right to control rentals)). Despite this observation, the White Paper called for only relatively minor modifications to the Copyright Act. *Id.* at 211-38.

it presents the courts with a topic that our Constitution properly has assigned to Congress. As noted by the Supreme Court in *Sony v. Universal City Studios*:

> As the text of the Constitution makes plain, it is Congress that has been assigned the task of defining the scope of the limited monopoly that should be granted to authors or to inventors in order to give the public appropriate access to their work product. Because this task involves a difficult balance between the interests of authors and inventors in the control and exploitation of their writings and discoveries on the one hand, and society's competing interest in the free flow of ideas, information, and commerce on the other hand, our patent and copyright statutes have been amended repeatedly.
>
> . . . .
>
> The judiciary's reluctance to expand the protections afforded by the copyright without explicit legislative guidance is a recurring theme. Sound policy, as well as history, supports our consistent deference to Congress when major technological innovations alter the market for copyrighted materials. Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology.
>
> In a case . . . in which Congress has not plainly marked our course, we must be circumspect in construing the scope of rights created by a legislative enactment which never contemplated such a calculus of interests.[318]

The troubling legal questions presented by the rapid expansion of the Internet should be settled legislatively. Congress is the only body capable of answering the specific technical questions and reconciling the often competing policy interests associated with the question of liability for online copyright infringement. Congress is uniquely qualified not only to perform the required "calculus of interests," but also to perform the required assessment of what ISPs can and cannot realistically do and the costs associated with those actions.

> The rate at which technological developments are growing coupled with the complexity of technology is beyond many laypersons' ken. *A uniform system of managing information technology* and computer networks is needed to cope

[318] Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 429-31 (1984). Courts considering other issues related to cyberspace have also called for Congressional action to bring statutes in line with current technology. *See, e.g.*, It's in the Cards, Inc. v. Fuschetto, 535 N.W.2d 11, 14 (Wis. Ct. App. 1995) ("Applying the present libel laws to cyberspace or a computer network entails rewriting statutes that were designed to manage physical, printed objects, not computer networks or services. Consequently, it is for the legislature to address the increasingly common phenomenon of defamation on the information superhighway."); Religious Tech. Ctr. v. Netcom Online Communication Servs., Inc., 907 F. Supp. 1361, 1370 n.12 (N.D. Cal. 1995) (noting the similarity of ISPs to common carriers, but declining to summarily exempt them from liability on this basis; reasoning that such a determination "is to be resolved by Congress, not the courts"); United States v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994) (reluctantly dismissing criminal charges against an admitted infringer due to the inadequacy of the former criminal liability provisions of the Copyright Act).

> with the impact of the information age. It is the responsibility of the legislature to manage this technology and to change or amend the statutes as needed.[319]

Regulation of the Internet is inevitable. Congress should take this opportunity to extend America's leadership in information technologies by establishing a successful model of electronic commerce that other nations will emulate, rather than being forced to fit our laws within a framework established by other countries that were more willing to take the lead.[320] A new framework that maximizes the untapped potential of both access providers and content providers would increase copyright authors' willingness to make their products available through electronic commerce, thereby reducing transactions costs and providing for cost-effective global marketing of America's information products.[321] Likewise, a stable legal environment for service providers would also help reduce their costs, thereby ensuring that Americans continue to enjoy affordable access to information.

[319] *It's in the Cards*, 535 N.W.2d at 14-15 (emphasis added).

[320] As an intellectual property attorney urged Congress:

> I believe legislation on this issue is inevitable, if not here, then abroad. Use of the Internet is widespread and rapidly growing in many other nations. Some of these countries are now becoming part of the Internet and are taking actions and considering legislation that will have a direct impact on the way U.S. companies operate on the Internet. . . . It is just a short leap until . . . other countries consider legislation delineating the liability of ISPs, including American companies, for online copyright infringement. Some of this foreign legislation may have a distinct chilling effect on the Internet in the absence of guidance from Congress. Therefore, while Congress is now in a position to determine the future of intellectual property on the Internet . . . Congress may soon find itself following the lead of other countries.

Hearings on H.R. 2441, *supra* note 160, at 287-88 (statement of William J. Cook, Attorney, Willian, Brink, Hofer, Gilson & Lione).

[321] Without a secure online environment, content providers are reluctant to offer their most valuable works online. As noted by an executive with publisher McGraw-Hill:

> [T]he material that The McGraw-Hill Companies and its information industry counterparts make available directly over the Internet provides only catalogs or sample selections of works. We do not and cannot offer more because there is too great a risk to our valuable intellectual property in an environment where the culture and technology offer so little protection for the rights of content producers. As a result, many of our most popular and successful products... are not as readily available as either we or our customers would like.

Hearings on H.R. 2441, *supra* note 160, at 72 (statement of Barbara Munder, Senior Vice Pres., The McGraw-Hill Cos., Inc.).

A. *Congress Should Set Broad National Policy Goals and Delegate Rulemaking to the FCC*

This new statutory framework must be uniform in order to be effective. Any regulations that negatively impact an ISP's subscribers must be uniformly applied so that the marketplace does not punish disproportionately regulated providers.[322] Further, the most promising technological solutions to online copyright infringement can be effective only if they are standardized and uniformly applied.[323] Finally, many of the existing laws that impact ISPs, such as copyright, are exclusively federal and, either expressly or by implication, preemptive.[324]

[322] This provides further support for total federal preemption of the field. If one state were to impose more stringent requirements than another, users could easily switch to the out-of-state provider. Additionally, large providers may be disadvantaged more than small providers if regulations are not mandatory and uniform.

> [S]elf-regulation should be not be voluntary, but should be mandated through legislation. A voluntary duty would not provide sufficient protection to copyrights. While major ISPs would most likely shoulder a voluntary duty, the smaller ISPs would have a direct incentive to ignore a voluntary duty. These smaller ISPs can more effectively compete with the bigger ISPs by giving their subscribers access to content not available on the bigger systems . . .
>
> The likely compliance of only the major ISPs with a voluntary duty will not provide any protection to copyrights. If copyright infringing material is available anywhere online, it can be disseminated worldwide in a matter of minutes.

Hearings on H.R. 2441, *supra* note 160, at 293 (statement of William J. Cook, Attorney, Willian, Brink, Hofer, Gilson & Lione).

[323] Since competing standards require wasted research and development effort and leave producers open to the threat of obsolescence, both hardware and software-based protection systems, like most computer technologies, require standardization to be successful in the marketplace. *See, e.g.*, *supra* note 264 and accompanying text (describing the need for standardization for successful deployment of a smart card system). Additionally, development and standardization of easy-to-use software protection solutions would help to relieve the negative market pressures currently suffered by those manufacturers who choose to copy-protect their programs. *See supra* note 276 and accompanying text.

[324] The Copyright Act is expressly preemptive. *See* 17 U.S.C. § 301(a) (1997). *See also* Del Madera Properties v. Rhodes and Gardner, Inc., 820 F.2d 973, 977 (9th Cir. 1987) ("A state law is preempted by federal copyright law if (1) the work at issue comes within the subject matter of copyright; and (2) the state law rights are 'equivalent to rights within the general scope of copyright.'"); Ohio v. Perry, No. C-960297, 1997 Ohio App. LEXIS 453 (Ohio App. 1997) at *18-19 (overturning a pirate BBS operator's criminal conviction based on a state "unauthorized use of property" statute due to preemption of the Copyright Act).

See generally Trotter Hardy, *Contracts, Copyright, and Preemption in a Digital World*, 1 RICH. J.L. & TECH 2 (1995) <http://www.urich.edu/similarjolt/v1i1/hardy.html> (providing overview of copyright preemption and the Internet).

Other laws affecting ISPs are also preemptive. *See, e.g.*, Communications Decency Act of 1996, Pub. L. 104-104 § 502, 110 Stat. 56, (amending 47 U.S.C. § 223 (f)(2))

As a threshold matter, however, it must be recognized that the Internet is a global medium and that the United States obviously can only regulate what occurs within its territories. This does not, however, present quite the impediment that it might seem. First, seventy percent of all Internet traffic starts and stops within the United States.[325] Second, ninety eight percent of all Internet servers are located in North America, Western Europe, Japan, and Australia, countries historically friendly to the United States.[326] If our laws are successful in establishing a secure environment for online commerce, these other countries might be persuaded to emulate them or to join a US-lead coalition.[327] If enough nations were to unite, even historically recalcitrant nations like China might be persuaded to join.

In order to provide uniformity, Congress should wholly preempt state regulation of service providers and create uniform national regulations.[328] Congress should confine its statutes in this area to only broad statements of policy objectives, delegating to an administrative agency the task of giving effect to these broad goals with appropriate regulations.[329] Specific regulations would require more careful study than any House or Senate subcommittee could provide, even if its members

(expressly providing for federal preemption, although allowing for "complementary state regulation or oversight for intrastate communications").

[325] *Prepared Testimony of Allee Willis, Songwriter, on Behalf of Broadcast Music, Inc., Before the House Judiciary Comm., Courts and Intellectual Property Subcomm., Regarding H.R. 2180 ("On-Line Copyright Limitation Liability Act") and H.R. 2281 ("WIPO Copyright Treaties Implementation Act")*, Federal News Service, Sept. 16, 1997, *available in* LEXIS, Legis Library, Fednew File.

[326] Zgodzinski, *supra* note 4.

[327] Global laws would, of course, be ideal. The recent progress in the development of international treaties makes it more likely that other nations would be willing to employ similar systems in their countries. *See generally* IITF WHITE PAPER, *supra* note 173, at 135-39. In December 1996, at an international conference sponsored by the World Intellectual Property Organization, the WIPO Copyright Treaty was agreed upon. As of March 10, 1998, the WIPO Copyright Treaty had been signed by 50 nations and the European Community, but had been ratified only by Indonesia. The full text of the treaty, as well as a current list of signatories, is available at the WIPO Web site (visited Apr. 5, 1997) <http://www.wipo.org>.

[328] Given the inherently interstate nature of the national information infrastructure, any regulation of ISPs seems clearly within Congress' commerce power.

[329] "Congress has long recognized that copyright laws must be written broadly in order to maintain the necessary flexibility that information providers and their customers require to meet changing marketplace demands." *Hearings on H.R. 2441*, *supra* note 160, at 75 (statement of Barbara Munder, Senior Vice Pres., The McGraw-Hill Cos., Inc.).

worked on the issue to the exclusion of all other business. The intensely technical nature of Internet technology and the certainty that it will undergo constant evolution demands regulation and oversight of ISPs by a specialized agency.

Since Internet access is inherently related to communications technologies already under the regulation of the FCC, it would be the obvious choice for an administrative agency.[330] Additionally, the FCC already has much of the technical expertise and infrastructure required to enact the regulations, monitor compliance, and hear cases involving failure to comply. The FCC should be empowered to establish and maintain specific guidelines for ISP conduct in areas such as access control, implementation of technological solutions, investigation and resolution of infringement claims, and subscriber education. ISP conduct should be governed by these specific rules and procedures and ISP liability should be accessed solely in light of compliance with those procedures.

B. A Negotiated Rulemaking Approach Should be Used to Help Assure Balanced and Responsive Regulations

Content providers, access providers, the media, and free speech organizations have bitterly clashed on the issue of service provider liability. In order to assure that these and other stakeholders have a seat at the table, regulations should be adopted using the negotiated rulemaking process.[331] Contentious litigation can be replaced with enlightened discussion and cooperation.

Rather than Draconian legislation by uniformed legislators, a flexible negotiated rulemaking approach would also provide an ideal forum for the development of industry-driven, rather than government-driven, reform. The government-sponsored establishment of a dialog among information industry representatives promises to provide the most responsive and effective means of providing solutions to both the problems of today and the problems of tomorrow.[332] Agency coordi-

[330] Internet access inherently requires the use of some communications technology. Although Internet access is today primarily limited to telephone lines, emerging technologies for high-speed Internet access such as cable modems, satellite Internet access, and wireless access have already been employed and will undoubtedly become more popular. Since the FCC already regulates each of these technologies, it would be uniquely situated to keep pace with changes in the particular methods by which users will connect to the Internet in the future.

[331] *See* 5 U.S.C. §§ 561-580 (1997) (outlining the basic negotiated rulemaking approach).

[332] As observed in the White Paper:

nation of private research efforts would provide the greatest opportunity for the development of new technological solutions. Further, as these solutions are developed, the government would be able to provide essential standardization and uniform implementation. Congress, however, must ensure that the primary goal of any regulation in this area is to provide *useful* standardization, not merely standardization for its own sake. Since excessively rigid standardization hinders rather than promotes innovation and progress, Congress should regulate no more than is required.[333] Such an approach would be consistent with the history of the Internet, which was created through a flexible cooperative effort between government and private industry.[334]

Regulations that might have a negative impact upon affordable access to information must be prudently crafted. In order to avoid costly and ineffective regulations, all such regulations should be subject to careful cost/benefit analysis.[335] In addition to making sure that the costs of enforcement do not exceed its benefits to content providers, the needs of content providers must be balanced against America's need for affordable access to information. The negotiated rulemaking approach would ensure that all stakeholders would have an opportunity to present data on all relevant economic and social costs.

> Different service providers play different roles—and those roles are changing and being created virtually every day. At this time in the development and change in the players and roles, it is not feasible to identify *a priori* those circumstances or situations under which service providers should have reduced liability. However, it is reasonable to assume that such situations could and should be identified through discussion and negotiation among the service providers, the content owners and the government. We strongly encourage such actions in the interest of providing certainty and clarity in this emerging area of commerce.

IITF WHITE PAPER, *supra* note 173, at 123.

[333] *See, e.g., The Information Marketplace: Market Forces and Competition Will Build the Information Marketplace* (visited Mar. 16, 1998) <http://www.bsa.org/piracy/infomkt/forces.htm> (noting that "[r]egulated standards would be a major departure and a potential disastrous destabilizing force" in the software market and pointing to the technological superiority of computer monitors (which are not subject to government mandated regulated) to television sets (which are subject to decades-old government standardization) as a parallel example in hardware).

[334] *See supra* notes 32, 37 and accompanying text (describing, respectively, the governance and historical origin of the Internet).

[335] *See generally* Byron F. Marchant, *On-Line on the Internet: First Amendment and Intellectual Property Uncertainties in the On-Line World*, 39 HOW. L.J. 477 (1996) (arguing that the complex economic relationships presented by the national information infrastructure mandate a cost-sensitive approach; without such an approach, the benefits of monitoring may be outweighed by the costs).

By adopting the agency regulation approach, service providers would benefit by being subjected to specific, workable, and technologically realistic standards and by having their compliance with those standards judged by technologically savvy agency personnel. Likewise, content providers would benefit by having a secure uniform platform for online distribution of their works. Thus, by adopting a flexible negotiated rulemaking approach, both ISPs and content providers could be confident that each is being asked to do no more than is currently technologically and economically feasible.

C. *Regulations Can Reduce Losses Due To Infringement by Promoting Prevention and Deterrence*

The current debate over ISP liability has tended to divert attention from the area most needing additional consideration—*prevention.* The issue of ISP liability is inherently more retrospective than copyright's general goal of promoting innovation; it is focused on finding the proper defendant after the harm from infringement has already occurred. Unfortunately, this retrospective focus often obscures the more important underlying goal of prospectively preventing the harm from occurring in the first place.

The real harm to a copyright holder from online infringement occurs at the ends of the line, when infringing copies are created by downloaders. The initial act of infringement, the creation of copies on Internet servers, does not directly cause any economic damage to authors, as no sales have yet been lost. Once this initial act is complete, however, the work may be potentially downloaded *millions* of times, with each resultant copy potentially representing a lost sale.[336] Fur-

[336] Additionally, under the current infrastructure, once material is uploaded to the Internet, it may be difficult, if not impossible, to delete. *See, e.g., Purcell Testimony on H.R. 2441, supra* note 223.

> [I]t is difficult and may be quite time-consuming to eradicate an infringing posting after it has been identified.
>
> Although a service provider may be able to locate and remove or block a particular posting on its own server, the interconnections between servers means that no service provider could guarantee that a removed posting would not be accessible via another server or would not return to its server after the initial removal or blocking. Just a few minutes after a customer posts a message, it has likely already traveled to thousands of other servers.

Id. A message posted to Usenet, for instance, is immediately propagated to servers around the world. Messages can be deleted ("cancelled"), but currently this may only be done by either the posting parties themselves or by the administrator of the server that the message was posted from. There is no facility built in to the Usenet system for an individual server administrator to cancel any particular message from their server's storage. The system-wide Usenet administrators will only cancel messages if they are ther, even the quickest legal action will always be outpaced by the speed of the Internet.[337] Therefore, it is vitally important to prevent material from being made available on the Internet in the first place—in cyberspace, an ounce of prevention is worth *tons* of cure.

1. Standardized Subscriber Agreements Would Promote Subscriber Education and Accountability

Service providers should be required to provide standardized subscriber agreements.[338] The subscriber agreements should educate their subscribers about Internet abuse in general and online intellectual property theft in particular.[339] Not only would such notices help to prevent unintentional infringement borne out of ignorance,[340] but also

abusive of the system as a whole, not based upon the message's content. *See supra* note 73 and accompanying text.

[337] As noted by one intellectual property attorney:

> Considering the speed with which online infringement can utterly destroy the value of a copyright, courts are institutionally ill-equipped to prevent online copyright infringement with the required alacrity. Even the speediest court procedures, such as temporary restraining orders and preliminary injunctions, require the intervention of a middleman—the court—between the service provider and the copyright owner. Therefore, court procedures are not sufficiently immediate to prevent substantial damage from online copyright infringement.

Hearings on H.R. 2441, *supra* note 160, at 291 (statement of William J. Cook, Attorney, Willian, Brink, Hofer, Gilson & Lione).

[338] Virtually all service providers already require subscribers to manifest assent to detailed subscriber agreements. If the agreement is executed as part of an online signup process, the new subscriber is typically required to manifest assent to the terms by pressing a series of on-screen buttons. The penalties for willful infringement could easily be presented as a discrete item that must be specifically agreed to.

[339] Other items to be addressed in such a standardized notice might include summaries of subscribers' potential liability for such offenses as online defamation, invasion of privacy, and indecent materials. Further, the notice might also inform parents as to the availability of tools designed to screen out sites inappropriate for their children. *See, e.g.*, *Project OPEN* (visited Apr. 5, 1997) <http://www.isa.net/project-open/index.html> (model notice from a cooperative effort between service providers and content providers, seeking to promote understanding about intellectual property issues, safe computing for children and other users, understanding about privacy rights, and consumer protection).

[340] An understanding of intellectual property rights is particularly important for the new generation of Internet users:

> [M]any cyberspace users are completely unfamiliar with any of the existing copyright laws and the implications that their Internet actions may have. Most are completely unaware that downloading material into the RAM of their computers, even if they never actually print the material or share it with anyone else, technically constitutes a reproduction under current U.S. copyright

they would put existing and would-be intentional infringers on notice as to the civil and criminal consequences of their actions. Additionally, providers should be required to supply subscribers with standardized software solutions that will allow them to voluntarily screen out unwanted content.[341] Since most providers require subscribers to secure their accounts with a credit card, a standardized agreement might also provide that ISPs are authorized to directly deduct court-awarded damages from the subscriber's credit card account, thus providing infringed authors with a convenient method of collecting judgments, as well as drawing further attention to the seriousness of infringement.[342]

2. *Restrictions on Unauthorized Access and File Transfer Logging Would Provide Subscriber Accountability*

The majority of the abuses occurring on the Internet are the result of one of its most valuable characteristics: *anonymity*. Internet users

> law and thus makes them infringers, albeit unintentionally. To aggravate the problem even further, although children currently account for only approximately two percent of total Internet users, their numbers are expected to dramatically increase in the next decade. Unless children can be taught the complexities of the current copyright statute early on, lessons that most of their adult counterparts have yet to learn, they too will join the ranks of copyright infringers.
>
> . . . .
>
> Anyone with a personal computer, a modem, and a telephone can now access vast amounts of copyrighted material at the touch of a button and become "infringers." Furthermore, there exists the apparent widespread belief that it is not a crime to "copy" the latest computer software or to give a downloaded program to a friend. As long as this type of attitude persists, infringement will be rampant on the Internet under the current regulation regime.

Cohen, *supra* note 276, at 412-14 (footnotes omitted).

[341] This would not present a hardship to service providers, as virtually all supply software packages to new subscribers. There is presently a wide array of software available to assist users in screening out unwanted content based on the IP address of sites known to contain objectionable material, key words in the content, or author-established content rating systems. *See generally* American Civil Liberties Union v. Reno, 929 F. Supp. 824, 838-46 (E.D. Penn. 1996) (describing many of the currently available content screening methods).

[342] The agreement should also clearly establish that the subscriber, even if institutional, is fully responsible for any civil damages caused by the use of that account, irrespective of whether the subscriber was the actual wrongdoer. If the subscriber fails to control access using his account, he should be primarily liable. The subscriber could then seek indemnity from the actual wrongdoer. The harsh effects of such a system could be mitigated by requiring the provider to make provisions for multiple user name/password combinations from a single account. The subscriber would, however, have to agree to remain primarily responsible for all damages caused by the use of his account, especially for the activities of his minor children.

In the common situation where all users of a business access the Internet through a single account, it would be the responsibility of the business to manage accountability on its network.

quickly learn that, under the present infrastructure, their activities often cannot easily be traced back to them. No matter what liability is imposed upon infringing users, enforcement of online copyright violations cannot be successful without an effective means of identifying them.

As a threshold matter, the often-overlooked distinction between *apparent* anonymity, or "pseudonymity," and *absolute,* or "true" anonymity, must be recognized.[343] Since Internet communications do not inherently identify their author, anyone wishing to voice an opinion on the Internet can do so with apparent anonymity by simply using a pseudonym (or no name at all).[344] Only by obtaining true anonymity, however, can the author be certain that his actions will be free from any *possibility* of reprisal. Pseudonymous communications usually leave an evidence trail that can be traced back, although often with great difficulty, to one or more Sysops or access providers who can identify the user.[345] As one author noted, "The single biggest myth about the Internet is that it's 'anonymous.'"[346] True anonymity must be specifically sought after using one of two methods: (1) by gaining access to the Internet using an account that cannot be traced back to the user, or (2) by using a server that either does not require that the user identify himself or removes the user's identification before his messages are transmitted to another server.[347] It is only true anonymity that presents

[343] *See generally* Lance Rose, *Anonymity Online: Its Value, and Its Social Costs* (last modified June 1995) <http://www.boardwatch.com/mag/95/jun/bwm45.htm>. *See also* Karina Rigby, *Anonymity on the Internet Must be Protected* (visited Feb. 13, 1998) <http://swissnet.ai.mit.edu/6095/student-papers/fall95-papers/rigby-anonymity.html> (describing the history and methodology of true anonymity on the Internet).

[344] A Web page, for instance, only displays the text or images selected by its author. Therefore, a Web page author may choose to use his real name, a pseudonym, or no name at all. A Usenet or IRC message is identified by the name supplied by its author and many, if not most, users choose to be identified by a pseudonym. An e-mail message, although it has a return address, only identifies its author's name if the author includes it in the text of the message.

[345] In the case of a Web page, the Web server Sysop will typically know the identity of its author. Similarly, e-mail and Usenet messages contain information that can be used to trace the message back to the originating server, whose Sysop will typically know the author's identity. Even IRC Sysops can identify a user's IP address.

[346] K.K. Campbell, *Anonymity: Internet's Great Myth* (last modified Dec. 5, 1996) <http://www.kkc.net/toronto-star/1996/ts1205.htm>.

[347] *See supra* notes 43-44 and accompanying text (describing anonymous remailers), *supra* note 233 and accompanying text (describing http proxy servers and anonymizers).

copyright enforcement problems, since pseudonymous communications can be traced back to their authors.

The unqualified removal of anonymity on the Internet, however, has obvious negative free speech implications and would undoubtedly be vigorously opposed, both by civil libertarians and users themselves.[348] That, however, is a larger issue that Congress need not resolve in the pursuit of copyright abuse prevention. The following recommendations would narrowly provide increased accountability for copyright violations, yet only have a minimal impact upon free speech.[349]

a. *Internet Access and Server Access Should Be Uniformly Controlled*

Regulations should establish a uniform system of Internet access control. Subject to certain exceptions described below, access providers should be required to restrict access to known users, to keep a log of the IP addresses assigned to each subscriber when he connects to the access server, and server Sysops should be required to restrict uploads to known users or known IP addresses.[350] Uniform access control measures are necessary in order to establish the identity, and therefore the accountability, of infringers.[351] Although nearly all Sysops and access providers do not allow anonymous use,[352] those that do are popular with Internet pirates.[353]

The impacts upon free speech from such access controls can easily be minimized. First, it must be remembered that access control measures would not interfere with pseudonymity; users would enjoy exactly the same level of apparent anonymity. Further, if access control regulations

[348] A recent survey of Internet users showed that they highly value anonymity and the ability to use pseudonyms. *See GVU's 5th WWW User Survey, supra* note 231.

[349] Further, the alternatives may be worse. *See, e.g., supra* notes 239-44 and accompanying text (describing the potential harms to free speech and privacy that may occur under a strict liability system where service providers were pressured to screen subscriber content).

[350] For those ISPs that control server access by allowing access only from the IP addresses that they own, the identity of an uploading subscriber can be determined by matching the server log with the its access server's IP address assignment log. *See supra* note 41 and accompanying text (describing dynamically assigned IP addresses).

[351] Many commentators have argued that service providers should be strictly liable because often the infringing user cannot be identified. Strict liability is not needed to address this problem; a rule that allowing unauthorized access or uploading (subject to the limitations described below) is per se contributory infringement will address this concern without making service providers liable in all other situations.

[352] *See* IITF WHITE PAPER, *supra* note 173, at 184.

[353] *See supra* note 82 and accompanying text (describing abuse of anonymous Web sites); *supra* notes 53-54 and accompanying text (describing abuse of anonymous FTP servers as pirate drop sites).

were accompanied by specific restrictions on both an ISP's ability and duty to disclose recorded information, Internet authors would actually enjoy *increased* apparent anonymity.[354] Only if the message were illegal would the ISP or Sysop be required or permitted to disclose the logged information.

Second, access control measures can easily be subject to exceptions that will avoid unnecessary impacts on free speech. For example, server Sysops could be permitted to allow the anonymous transfers of messages that do not exceed a specified maximum size. While this limitation would permit the anonymous exchange of even lengthy messages, it would present a substantial impediment to the anonymous transfer of work such as computer programs, sound recordings, and large images.[355]

Public Internet access points like libraries and universities could also provide similarly limited anonymous access. Alternatively, they could be exempted from access restrictions entirely, thus providing a safe haven for unrestricted anonymity. Although leaving these access points would also provide a safe haven for infringers, the added inconvenience of traveling would undoubtedly prevent them from being a significant loophole for infringers. A third alternative would be to hold public access points liable, but provide a "good faith" defense for those that can show that they have taken reasonable measures, considering the circumstances, to prevent infringement.[356]

Although these proposed access control measures would neither completely prevent anonymous infringement nor be completely free from

[354] *See infra* notes 359-61 and accompanying text.

[355] If such a system were adopted, there would also need to be a daily cumulative limit from any particular IP address. An individual message size limitation might be defeated by splitting a large work into several smaller anonymously posted messages. Imposing a maximum daily limit would help discourage this type of abuse. Given current technology, such a system could be defeated by a user who reaches the maximum, disconnects from the provider, and then reconnects (in all likelihood being assigned a different IP address) and resumes transfers. *See supra* note 41 and accompanying text (describing dynamically assigned addresses). A daily cumulative limit would prevent this.

Like any other copy prevention measure, pirates would find ways around the limitation, service providers would close these loopholes, pirates would find a way around the new system, and so on. A maximum daily limit, however, would at least present a sizeable "speed bump," deterring all but the most determined software pirates.

[356] This alternative could also be applied to server sysops as an alternative to a message size limitation.

negative free speech consequences, they would at least strike a fair balance between the two competing objectives.[357] Further, these recommendations are but one proposed solution; consideration by those most knowledgeable in technology and civil rights may well reveal superior alternatives.

b. File Transfers Should Be Uniformly Recorded

Although access control measures would be an important step, Internet server Sysops should also be required to record file transfers. Access control measures would only establish the identify of those who upload infringing content; server logs are required in order to identify where subsequently downloaded copies come to rest. Unlike complicated and unworkable content-based filtering systems, server activity logging is simple, passive, and effective. Servers would simply record the IP addresses of the computers that upload or download files from the server, a task which most servers are already configured to perform.[358]

Since Internet servers and ISP access servers together comprise "both ends" of a file transfer, combining server logs (which identify visitors only by IP address) with ISP address assignment logs (which match an IP address with the particular subscriber using that address at the time of the transfer) would result in a complete record of all file transfers. This combining would provide a simple but exceptionally powerful file tracing system that would assist both law enforcement and infringed authors in locating infringers and establishing the extent of their

[357] The Supreme Court has consistently upheld "time, place, and manner" restrictions on speech when they are content-neutral, narrowly tailored, and enacted to advance an important governmental interest. *See, e.g.*, Clark v. Community for Creative Non-Violence, 468 U.S. 288 (1984).

[358] The following excerpt taken from an actual Web server log illustrates how simple this collection process is:

```
198.53.172.27   1997-09-03 16:41:28   GET        /chat/chatcmd.ap
198.53.172.27   1997-09-03 16:41:28   AP_SERVE_FILE
c:\sdweb\home\chat\chatcmd.ap
24.1.130.243   1997-09-03 16:41:29    GET        /chat/dir.ap
24.1.130.243   1997-09-03 16:41:29    AP_SERVE_FILE
c:\sdweb\home\chat\dir.ap
24.1.130.243   1997-09-03 16:41:29    GET        /chat/dirtop.jpg
24.1.130.243   1997-09-03 16:41:29    SEND_FILE_BINAR
c:\sdweb\home\chat\dirtop.jpg
```

SmartDesk Personal Web Server Server Log List (visited Feb. 27, 1998) <http://www.internetsolutions.com/websuite/websrvsrc3.html>. This excerpt shows two different users (identified in the far left column by the IP addresses of their computers), the files that they requested, and the files that the server transferred to them. This data, from left to right, represents the IP address of the visitor, the date and time, the particular files sent ("get" is a request from the visitor's computer and "ap_serve_file" and "send_file_binar" indicate that a file was transmitted to the visitor's computer).

wrongdoing. Using this information, a procedure could be easily developed whereby nationwide activity involving an infringed work could be relayed back to its author or law enforcement officers.[359]

A file tracing system would not only assist authors in finding responsible parties, it would also prevent a great deal of further harm from occurring, as all infringing copies on Internet servers would be blocked or destroyed within a matter of hours. Such a system would allow the power of digital communications technology to be harnessed to fight the very ills that it facilitates; unlike the printing press, the photocopier, the audio recorder, or the VCR, the Internet can also provide the means to inhibit infringement.

c. *Regulations Should Protect Against Unauthorized Disclosure of Recorded Information*

A file tracing system raises a legitimate concern about the possibility that the recorded information would be misused either by private parties, the government ("Big Brother"), or even the ISPs themselves. Although IP address assignment and server logs by themselves do not convey much information and, as most Internet users are aware,[360] ISPs routinely collect this information anyway, the synthesis of this discrete information into a single system raises the specter of abuse. Appropriate

[359] As an example of how such a system might work: The author, using a standardized procedure, could file his claim with any convenient ISP. That ISP would then, using secure encrypted communication, send out an automated tracing request to the server or servers identified in the claim. The servers would remove or temporarily block the challenged work, check their logs to determine the IP address of any downloads of the work, and then forward the claim to the ISPs that own those addresses. Those ISPs would then check their IP address assignment logs to determine which of their subscribers downloaded the work. This information would then be returned to the requesting ISP, which would then assemble the information and return the completed report to the infringed author, who would then be in possession of a complete log of all potentially infringing activity related to his work.

[360] Most Internet users are aware that servers record their activities. *See GVU's 5th WWW User Survey*, *supra* note 231.

> Most users are aware the time of the request (85.1%) as well as the name of the requested page (82.7%) are loggable. Following in order of response rates, the name of the user's machine (71.0%), the name of the user's browser (59.0%), the user's email address (45.2%), the user's operating system name (37.9%), a site id the persists across sessions (a.k.a. cookies) (37.7%), and finally the user's physical location (31.7%). 14.7% reported not knowing what information is loggable.

Id.

safeguards, however, can minimize this risk. First, regulations should specifically define under what circumstances a claim may be brought and should provide for penalties against frivolous claims. Second, the claim process itself should have appropriate procedural safeguards to minimize the risk of fraudulent claims.[361] Finally, statutes could protect user privacy by providing that any unauthorized disclosure or other use of the collected information would subject the offending provider to civil and, in appropriate cases, criminal sanctions.[362] Since server usage data is routinely recorded, yet currently no restrictions are imposed upon its use, a file tracing system with these procedural safeguards would provide users with greater security and privacy than they currently enjoy.

3. Changes to the Copyright Act and Increased Criminal Enforcement Efforts Would Provide Enhanced Deterrence

Although increasing user accountability for copyright infringement would be a significant step, it would not, by itself, be sufficient to provide effective deterrence to Internet copyright abusers. This is because users understand (either explicitly or implicitly) that virtually no one is being prosecuted, either civilly or criminally, for infringement. Since many infringers are, as a practical matter, judgment-proof, [363] the only real threat for these users must be provided by criminal penalties. It was precisely for this reason that in 1997 Congress passed the No Electronic Theft (NET) Act, amending the Copyright Act to remove the requirement that the defendant have realized or anticipated some financial gain.[364] Unfortunately, the NET Act provisions are ambigu-

[361] Such safeguards might include requirements that the claimant first procure a subpoena, post a bond, or sign the claim under penalty of perjury.

[362] For example, it is generally a violation of federal law to intercept or view private electronic communications. *See supra* note 48. Sysops that fail to follow specific procedures for the lawful disclosure of private electronic may be subject to fines or imprisonment, or both. *See* 18 U.S.C. §§ 2511(3)(a), 2511(3)(b), 2511(4) (1997).

[363] "Most operators of pirate sites have nothing we can collect." Will Rodger, *Bill Would Erase Copyright Loophole* (last modified Sept. 22, 1997) <http://www.zdnet.com/intweek/print/970922/inwk0065.htm> (quoting Sandra Sellers, Vice Pres. of Enforcement and Educ. for the Software Publishers Ass'n).

[364] Considering that the vast majority of online piracy is noncommercial, the pre-1997 "for purpose of commercial advantage or private financial gain" language of section 506(a) made it impossible to criminally prosecute most online pirates. One case, *United States v. LaMacchia*, 871 F. Supp. 535 (D. Mass. 1994), drew national attention to this problem. LaMacchia operated an FTP drop site on a university's computer. Over one million dollars worth of software was pirated through the site. LaMacchia was indicted on wire fraud, since his lack of "for-profit" motive precluded criminal prosecution under copyright law. The court reluctantly upheld the trial court's granting of LaMacchia's motion to dismiss, finding that although the Copyright Act controlled over the wire fraud statutes, it provided no penalty for LaMacchia's conduct. This

ous about when liability is triggered and fail to reach some of the most harmful and egregious acts of infringement. A comprehensive plan aimed at reducing losses for copyright holders should include further statutory clarifications and aggressive enforcement efforts.

a. A File Tracing System Would Enable More Effective Criminal Enforcement of Copyright Laws

In order to avoid criminal liability for "minor, isolated instances of willful infringement,"[365] the current provisions attach criminal liability for "the reproduction or distribution . . . during any 180-day period . . . of 1 or more copyrighted works, which have a total retail value of more than $1,000."[366] Unfortunately, unless file activity is recorded, most violations will go undetected. Since very few works have a retail value over $1,000, criminal liability for distribution will usually attach only if a user distributes multiple works collectively worth over $1,000. If these works are uploaded to a single site, the violation will be obvious. If, however, as is the more typical scenario, the user instead spreads out these uploads over multiple sessions or to multiple sites, his criminal

decision, responsible for the coining of the phrase "LaMacchia loophole," was understandably the subject of widespread commentary and criticism.

In response to this criticism, the NET Act, The No Electronic Theft (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678 (codified as amended in scattered sections of 17, 18, and 28 U.S.C.), amended section 506(a) of the Copyright Act to alternatively define criminal infringement as willful infringement "by the reproduction or distribution, *including by electronic means*, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000." 17 U.S.C. § 506(a)(2) (1997) (emphasis added). Other NET Act provisions combine with existing provisions to include fines and imprisonment up to one year for violations involving copies of one or more works with a total retail value of $1,000 or more, up to five years for violations involving copies of one or more works (ten or more works in the case of phonorecords) with a total retail value of $2,500 or more, and up to six years for subsequent violations. *See* 17 U.S.C. § 506; 18 U.S.C. §§ 2319, 3571.

The NET Act's removal of the for-profit requirement is consistent with many software pirates' view of pirated programs as being merely the currency of the hardcore Internet software piracy world. *See* McCandless, *supra* note 6, at 175.

[365] *Statement of Marybeth Peters, Register of Copyrights, Before the House Subcomm. on Courts and Intellectual Property, on H.R. 2265*, (last modified Sept. 11, 1997) <http://www.house.gov/judiciary/41109.htm> (suggesting clarifications to H.R. 2265 (the bill which was enacted as the NET Act) to prevent criminal liability for "minor, isolated instances of willful infringement"; these suggestions were incorporated into the bill as enacted).

[366] 17 U.S.C. § 506(b) (1997).

liability will likely go unnoticed. As an illustration of this problem, assume that a user uploads $999 worth of software to Usenet every two weeks. Since the vast majority of Usenet servers delete binary messages only a few days after they are received,[367] that user's violation of the $1,000/180-day minimum would not be recognizable at any given time. A similar situation would exist if the user instead uploaded $999 worth of software simultaneously to several different sites. These violations would go unnoticed and unpunished, even though the user would have greatly exceeded the threshold for criminal liability. Similarly, although the NET Act also attaches criminal liability for possession of works with a total retail value over $1,000, there is currently no way for investigators to identify even those users who have downloaded huge stockpiles of infringing works.

A file tracing system would not only enable prosecutors and infringed authors to recognize when an individual's infringement is cumulatively sufficient to trigger criminal liability, but would also provide an accurate measurement of the extent of his wrongdoing. Thus, a file tracing system would increase the likelihood that infringers would be caught and held fully accountable for their misconduct, thereby greatly enhancing the deterrent effect of the current criminal laws.

b. Additional Amendments Should Be Enacted to Close Gaps in the Copyright Act

The existing criminal liability provisions in the Copyright Act do not address many of the most common and harmful online copyright violations. The NET Act, while it removed the "for profit" loophole, failed to close other significant gaps in criminal and civil liability. In order to bring them in line with the realities of online piracy, the criminal liability provisions of the NET Act should be supplemented and clarified.

First, the NET Act failed to include criminal liability for the increasingly popular use of software copy protection cracks.[368] Since cracks and serial numbers have no "retail value," pirates that distribute them will escape criminal liability, even though their acts are willful and capable of causing tremendous losses to copyright holders. The Copyright Act should be further amended to specifically include criminal

[367] *See supra* note 238 (describing Usenet server retention time).

[368] *See Holleyman Testimony on H.R. 2180 & H.R. 2281*, *supra* note 275 (noting increasing use of software protection cracks); *Sellers Statement on H.R. 2265*, *supra* note 13 (calling for criminal penalties for persons who create and distribute utilities to circumvent software copy protection).

liability for the knowing possession or distribution of any device, program, or other data specifically intended to defeat software copy-protection schemes.[369] Additionally, the Copyright Act should be amended to attribute the retail value of a work to any device specifically intended to defeat its copy protection, thus effectively giving each crack the value of the work itself.

Second, the NET Act failed to explicitly include criminal liability for conspiracy to infringe. Organized software piracy groups supply much of the software that is distributed on the Internet.[370] Without their expertise, these programs could not be pirated.[371] Reducing the activities of these groups would have a dramatic influence on the supply of pirated computer software.

Finally, the Copyright Act should be amended to explicitly provide civil liability for the full extent of damages created when a user makes a protected work available for widespread copying. In order to ensure that courts assess damages that comport with the realities of online

[369] Several bills pending in Congress would prohibit such devices. One of the provisions of H.R. 2281, for example, would amend the Copyright Act to provide that:

> (2) No person shall manufacture, import, offer to the public, provide or otherwise traffic in any technology, product, service, device, component, or part thereof that —
>
> (A) is primarily designed or produced for the purpose of circumventing a technological protection measure that effectively controls access to a work protected under this title;
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological protection measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person for use in circumventing a technological protection measure that effectively controls access to a work protected under this title.

WIPO Copyright Treaties Implementation Act, H.R. 2281, 105th Cong. (1997). *See also* Digital Era Copyright Enhancement Act, H.R. 3048, 105th Cong. (1997) (prohibiting the intentional removal, deactivation, or circumvention of copy protection measures and the alteration or removal copy management information).

[370] *See supra* notes 68-69 and accompanying text.

[371] Many of the programs illegally distributed on the Internet require extensive cracking and other preparation for online distribution, procedures requiring effort or expertise greater than the causal infringer is able or willing to provide. *See, e.g.*, McCandless, *supra* note 6, at 180 (describing one program of which there were "only three or four crackers in the world" who could successfully break its copy protection scheme). *See also infra* notes 378-82 and accompanying text (describing the activities of one organized cracking group).

infringement,[372] the Copyright Act should be amended to specifically provide that those who willfully upload infringing material will be held liable for the value of the copies that are subsequently downloaded, with server logs considered to be presumptive proof of the number of copies downloaded.[373]

c. *Increased Criminal Enforcement Efforts Would Reduce Online Piracy*

No matter what criminal or civil liability is imposed upon Internet infringers, however, those provisions must be enforced if they are to have a significant deterrent effect. The NET Act, for instance, has yet to have any noticeable effect on the trafficking of copyrighted works on the Internet.[374] Although news of the NET Act was the subject of much discussion throughout the Internet, particularly in the software piracy newsgroups, the lack of any subsequent enforcement efforts has caused the infringing activities to continue unabated.

The power of high-profile enforcement efforts should not be underestimated. Although there have been few widely reported actions taken against online software pirates, and none since the passage of the NET Act, the few actions that have been taken have had a remarkable chilling effect upon the open trading of pirated software on the Internet. One example is "Operation Cyber Strike," a quick-strike campaign launched in January 1997 by the FBI's International Computer Crime Squad.[375] The FBI targeted organized piracy groups in seven states using private BBSs, FTP, and Internet Relay Chat. Although no arrests were made, the FBI seized the BBS operators' hardware.[376] Even these limited enforcement actions were sufficient to send shock waves throughout the

[372] It must be noted, however, that the value of the number of copies downloaded does not represent an accurate measure of losses to infringed authors. *See supra* notes 11-14, 277-82 and accompanying text. Despite this, courts should resolve doubts as to the extent of actual losses against the infringing party.

[373] Liability should be limited to all "first-generation" copies that ultimately come to rest in the hands of a human being. The fact that copies were automatically created by intermediate Internet servers should not relieve the defendant of liability. If, however, another user downloads the work and then later uploads it to another server, the second user's act should be seen as a superseding act, cutting off the chain of liability for the original uploader.

[374] Indeed, it is unlikely that the NET Act will have any effect at all on piracy of some works. Since the Act only attaches liability to acts of infringement over any 180-day period with a "total retail value" of $1,000 or more, image piracy, for example, will largely escape its reach, since it would take hundreds or thousands of images to aggregate to over $1,000, even if a "retail value" could be established for each discrete image. A similar problem exists for sound recordings and other lesser-valued works.

[375] *See* Macavinta, *supra* note 53.

[376] *See* McCandless, *supra* note 6, at 177.

Internet piracy groups.[377] Activity in the Usenet software piracy newsgroups slowed dramatically and most of the prominent Internet piracy organizations kept a very low profile. Since there were no subsequent enforcement efforts, however, the infringing activities resumed to their normal level within a few weeks.

Another example occurred two months after Operation Cyber Strike. On March 17, 1997, in what was labeled a "first," Microsoft Corporation filed suit against Christopher Fazendin, alleging that he authored a Web page containing a crack to defeat the 90-day limit on the trial version of its Office 97 product.[378] A Microsoft attorney was candid about the fact that Microsoft brought the action to make an example of Mr. Fazendin: "This particular crack was so widely distributed and so serious an infringement on Microsoft's copyright on Office 97 that we thought it was appropriate for litigation."[379] Microsoft subpoenaed the router and server logs from Fazendin's ISP in an attempt to determine the amount of Microsoft's losses and announced that it might also use the logs to take action against those who downloaded the infringing material.[380] As with Operation Cyber Strike, the Usenet software piracy groups were instantly flooded with discussion over the Microsoft suit and activity in the Usenet cracks groups dramatically slowed. Three days after the Microsoft announcement, the notorious piracy group that originally conceived and distributed the crack announced that it was disbanding.[381] Sixteen days later, "The Inner Circle," perhaps the most

[377] One pirate even hastily set up a Web page to spread the news of which software pirates had been "busted." *FBI Busts at Inept* (visited Feb. 3, 1997, now no longer in existence) <http://inept.pheared.com/index2.html>.

[378] *See* Renee Deger, *Microsoft Files First Lawsuit Against Security Code Cracker*, PC WEEK ONLINE (last modified Mar. 18, 1997) <http://www5.zdnet.com/zdnn/content/pcwo/0318/pcwo0011.html>. Since the crack was merely a replacement file from the fully functional version of the Office 97 product, Microsoft sued Mr. Fazendin for direct infringement. Interviews with Christopher Fazendin via e-mail messages (Mar. 1997).

[379] Deger, *supra* note 378. The crack had been floating around Usenet for weeks and had received a great deal of publicity. *See* Kristi Coale, *Microsoft Hardballs Office 97 Cracker*, WIRED NEWS (last modified Mar. 19, 1997) <http://www.wired.com/news/technology/story/2661.html>; Rebecca Sykes, *Microsoft Sues Over Office 97 'crack,'* (last modified Mar. 19, 1997) <http://www.computerworld.com/search/AT-html/online/9703/970319officecrack.html>.

[380] *See* Coale, *supra* note 379.

[381] The full text of the Usenet message read:

> This is an OFFICIAL Statement from Phrozen Group to announce that Phrozen Crew will not I repeat WILL NOT be posting cracks to any newsgroups anymore. Furthermore all public ftp sites and web sites have been closed

high profile and prolific Internet software piracy group ever, also announced that it was disbanding.[382] As with Operation Cyber Strike, however, the lack of subsequent enforcement efforts caused the infringing activities to resume their normal level within a few weeks.

Without high-profile enforcement efforts, open and widespread online piracy will continue. The FBI and content providers, now empowered by the NET Act to seek criminal charges against online infringers, have indicated that they intend to increase enforcement efforts.[383] While aggressive enforcement efforts will not stop online copyright infringement, it would certainly make many Internet infringers determine that the benefits from online piracy simply are not worth the risks. Further, those pirates that persist would be driven "underground," forced to use private sites and e-mail exchanges.[384] This would reduce the availabil-

> PERMANENTLY. Phrozen Crew would like to reinstate [sic] that they NEVER DID support alt.binaries.cracks.phrozen-crew and alt.phrozen.cracks [Usenet newsgroups]. No emails will be entertained. Phrozen Crew wishes to thank all those who have supported PC in anyway [sic]. U know who u are:)!

Usenet message posted by "Saltine," Phrozen Crew member (Mar. 20, 1997) (on file with *San Diego Law Review*). Subsequent Usenet messages from Phrozen Crew members confirmed that the threat of legal action from Microsoft was a key factor in the group's decision to disband.

[382] *See generally* McCandless, *supra* note 6 (providing an in-depth look at the Inner Circle and its members). "The Analog Guy," a long-time Inner Circle member, cited "personal reasons" as the basis for the group's decision to disband. Usenet message posted by "The Analog Guy," Inner Circle member (Apr. 2, 1997) (on file with *San Diego Law Review*). Later communications revealed that the recent media exposure from the Wired article and the increased perceived threat of prosecution were likely the true motivating factors. One of the Inner Circle members, "Irrelevant," disclosed in a subsequent message that it was fortunate "that none of us ended up in prison (yet) for our good intentions." Usenet message posted by "Irrelevant," Inner Circle member (Apr. 2, 1997) (on file with *San Diego Law Review*).

[383] Although it outlined many practical difficulties with prosecuting computer crimes, the Department of Justice claims to have "made great strides toward addressing [those] difficulties" and has recently "stepped up" enforcement efforts towards software pirates with its 1996 formation of the Computer Crime and Intellectual Property Section within the FBI. *See DiGregory Testimony on H.R. 2265*, *supra* note 68. "We hope that by bringing criminal laws to bear on some of the worst offenders, we will deter others from engaging in these illegal activities." *Id.*

Similarly, content providers have become emboldened by the passage of the NET Act and have indicated that they will seek to hold pirates criminally liable.

> Armed with a new federal law, the No Electronic Theft Act, the [Recording Industry Association of America] is trying to track down the biggest MP3 piracy sites, even going after sites that aren't profiting from the piracy. The trade group employs three full-time staffers to chase pirates—and has shut down more than 250 in the last year.

Brown, *supra* note 8.

[384] As an example of this, the recent enforcement campaign by the music industry against pirate sites resulted in the pirates "moving even further underground, backing away from the Web in favor of IRC, ICQ, and secret mailing lists." *Id.*

ity of pirated works to casual offenders, which undoubtedly account for the vast majority of unauthorized copies. Consequently, much of the unique infringement threat posed by the Internet would be eliminated, as losses from these private trading sessions would more closely approximate the losses suffered in the physical world when neighbors trade copies of computer programs or tape each other's CDs and videotapes.

D. ISPs and Content Providers Should Jointly Develop Technological Solutions

The most significant weakness in any program designed to locate infringing works is that it inescapably places the burden on copyright holders to discover and identify infringement of their works, since, in all but the most obvious cases, only the copyright owner can accurately determine whether a copy is infringing. Some content providers have reacted to the increasing problem of Internet piracy by assigning employees to seek out infringing copies of their works[385] and others have recruited the assistance of specialized Internet infringement "detectives."[386] Some content providers have automated this process by tagging their works with digital fingerprints and employing software programs that automatically scan the Internet for infringing copies of their works.[387] Although in each of these cases the content providers

[385] *See* Shapley, *supra* note 13; Brown, *supra* note 8; McCandless, *supra* note 6.

[386] Industry groups have formed detective squads and there are several new companies specializing in seeking out infringing copies. *See, e.g.*, Shapley, *supra* note 13, (describing "Internet detectives," "private sleuths, hired by corporations to guard their wares—from corporate logos to comic strips, from music to software—from the pilfering that computer technology makes so easy"); *Markwatch Licensing Page* (visited Nov. 15, 1997) <http://www.markwatch.com/license/> (describing "Markwatch," a service that will monitor the Internet for trademark "infringement, dilution, and genericide situations").

[387] Automated scanning systems are already in place for print media and music, and systems have been developed that will allow for similar identification of video, multimedia works, and online print media. *See, e.g., BMI Introduces Musicbot to Monitor Music Use on the Internet* (last modified Oct. 15, 1997) http://bmi.com/reading/news/musicbot.html>.

> Performing rights organization BMI today announced the creation of "MusicBot," a new web robot designed to gather market information and music trends while monitoring the use of music in cyberspace. The "MusicBot" will comb the web, quantifying the use of music on different sites. The robot, working 24 hours a day, seven days a week, provides BMI with the equivalent of a full-time staff of nearly two dozen web surfers at a fraction of the cost.

have reported great success in their efforts,[388] a file tracing system would dramatically increase their effectiveness. Once a single copy is located, a file tracing system would automatically find all other copies by looking forward and backward in the chain of distribution.

As previously described, both content providers and service providers have speculated about the possibility of developing some sort of automated system that would constantly scan a service provider's computers for the presence of infringing works. If such a system could be developed and uniformly implemented by all service providers, it could provide a massive reduction in online piracy. While service providers cannot unilaterally implement systems to locate infringing content, they can, however, execute a standardized *author-developed* identification system. Without cooperative efforts between content providers and service providers, no such system is possible. A negotiated rulemaking approach would provide a forum whereby service providers and content providers could work together to develop a system that is effective, yet not unduly burdensome on service providers, content providers, or their customers.

> This groundbreaking technology is part of a series of initiatives introduced by BMI to address the concerns of the more than 200,000 copyright holders it represents. . . .

Id. *See also* Robert E. Calem, *'Digital Watermarking' Scheme Protects Photo Copyrights*, N.Y. TIMES CYBERTIMES (last modified May 21, 1997) <http://www.nytimes.com/library/cyber/week/052197watermark.html> (describing the release of "MarcSpider," a program that "will scour the Web looking for images bearing its own PictureMarc tags and report its findings to the copyright holders").

Not only can digital fingerprints identify the works, but, when used in combination with uniformly implemented end user software or hardware, can also prevent unauthorized use, copying, or alteration of the works. *See, e.g.*, Nick Wingfield, *A Tool to Stop Image Snatchers* (last modified Apr. 22, 1997) <http://www.news.com/News/Item/0,4,9946,00.html> (describing "ThingMaker," a program that "will allow designers to 'lock' ordinary graphics and sound [and multimedia] files so that they cannot be duplicated or modified"); Levin, *supra* note 271 (describing "DiscGard," a system that prevents CD and DVD duplication by "etching a digital fingerprint into the pits and lands of optical disks"; playback devices encoded with the system would not allow duplication and will thus "stop pirates in their tracks").

[388] *See* Brown, *supra* note 8 (music industry executive reporting that pirates are "not hard to find" and "[e]very pirate we've gone after, we've caught"; music trade association reporting that three employees have shut down more than 250 pirate sites in the last year); Shapley, *supra* note 13, (describing success of companies specializing in searching for infringing materials on the Internet); Larry Lange, *Copyright Fight Rocks the Net* (last modified Feb. 25, 1997) <http://techweb.cmp.com/eet/news/98/995news/copyright.html> (automated scanning systems are "already putting a huge dent into the copyright piracy phenomenon"). *But see* McCandless, *supra* note 6 (anti-piracy specialists employed by software producer Novell report success, but fear that Internet piracy is too widespread to control).

E. New Regulations Would Assist Copyright Owners in Obtaining Civil Relief

Realizing that no system can realistically provide perfect deterrence or detection, copyright owners will always suffer some losses from online infringement. Regulations establishing a file tracing system would, however, greatly assist copyright holders in obtaining more complete civil relief.

In addition to allowing an infringed author to identify those responsible for uploading infringing copies, something that may be difficult or impossible today, a file tracing system would also allow the author to reach a whole new class of civil defendants—*downloaders.* All reported civil actions for online copyright infringement actions have been brought against either the uploader or his service provider. Downloaders are equally guilty of infringement, yet since their activities are not uniformly logged, they currently cannot be easily found.[389] Similarly, an infringed author seeking injunctive relief against a pirate site presently has no reliable method of accurately determining the location of other sites that may have downloaded the work. Although in many cases, if not most, actions against downloaders would be impractical due to jurisdictional and economic realities, a file tracing system would at least offer this as an option to infringed authors.[390]

A file tracing system would also help infringed copyright holders to be more fully compensated for their losses. Where an uploading defendant earned no profits from the work, copyright holders currently face significant challenges in proving damages, since there is usually no reliable method of determining how many infringing copies were

[389] *See supra* note 380 and accompanying text (describing Microsoft's subpoena of the router and server logs from the defendant's ISP in order to locate downloaders of its infringed work).

[390] The previously suggested provision in a standardized subscriber agreement (providing that ISPs are authorized to deduct court-awarded damages from subscribers' accounts) might make some actions against downloaders feasible. At the minimum, some authors might wish to have at least the capability to send demand or "cease and desist" letters to downloaders. *See, e.g.,* Lange, supra note 388 (describing campaign by Viacom, owner of rights to old *Star Trek* television show, of sending "cease and desist" letters to Web site authors who were infringing trademarks and copyrights). *But see supra* note 337 and accompanying text (describing inadequacies of even speedy injunctive relief when works can be transmitted over the Internet so rapidly).

ultimately downloaded.[391] If a file tracing system were combined with the previously suggested amendment explicitly creating liability for all downloaded copies, an infringed plaintiff would be more likely to be awarded his full damages.[392]

F. ISPs That Fully Comply With Regulations Should Be Shielded From Liability

ISPs, like common carriers,[393] should be regulated by specific

[391] "Civil damages are often insufficient. . . . Pirates can be organized, they *can have financial backing*, be nomadic, and create a great deal of harm, all without keeping records of the damage they've caused." Heltzel, *supra* note 296 (quoting Mark Traphagen, Vice Pres. of Intellectual Property and Trade Policy, Software Publishers Ass'n) (emphasis added).

The Copyright Act allows civil plaintiffs to recover either statutory damages or the sum of actual damages plus the infringer's profits. *See* 17 U.S.C. § 504 (1997). A civil plaintiff seeking actual damages must therefore show either the extent of the defendant's gain or the extent of his losses with reasonable certainty. Where the defendant earned no profits, the plaintiff's losses are obviously the only relevant factor. Similarly, a plaintiff seeking substantial statutory damages (which are only available to owners of registered works (*see id.* § 412)) must present evidence to guide the court's decision as to a "just" amount. Among the factors a court may consider in setting statutory damage amounts are: the expenses saved and profits reaped by the infringer, the deterrent effect of the award on defendant and on third parties, and the infringer's state of mind in committing the infringement. *See, e.g.*, Nintendo of Am., Inc. v. Dragon Pac. Intern., 40 F.3d 1007, 1011 (9th Cir. 1994).

[392] The burden of proof could then be shifted to the distributing defendant to prove that any particular downloader did not actually use or keep the infringing material. If the downloader testifies that he immediately eliminated the infringing copy, the court might allow for a reduction or elimination of damages based on the innocent infringer doctrine. *See* 17 U.S.C. § 504(c)(2) (1997). This consideration would only come into play, however, if the value of the infringed work was less than $200, since that is the minimum allowable award, even for innocent infringers. *Id.* It would be up to the uploader to seek indemnity from the subsequent downloaders.

Note that imposing liability for downloads upon uploaders would also effectively eliminate jurisdictional issues, since the uploader would, in essence, be held indirectly liable as a contributory infringer. Similarly, a file tracing system would allow infringed copyright holders to effectively extend their reach beyond the shores of the United States, even to nations that refuse to cooperate with the enforcement of international copyright treaties; so long as the infringing *uploader* is located in the United States, he could be held accountable for damages resulting from all infringing copies made, even if those copies were made by downloaders located abroad.

[393] Under the Copyright Act, common carriers are exempted from secondary liability. *See* 17 U.S.C. § 111 (1997). Internet service providers, however, do not fit under the existing definitions. The Communications Act of 1934 defines a common carrier as one that is required to furnish service upon request. *See* 47 U.S.C. § 201 (1997). *See also supra* note 197 (describing the Netcom court's refusal to extend the statutory definition to encompass service providers).

In order to bring ISPs under this definition, either the definition would have to be changed or the ISPs would be required to furnish service upon demand. Even the largest networks on the Internet, the backbone providers, don't have to accept *all* traffic; they only accept traffic from those networks with which they have agreed to "peer" with or uniform national regulations and, so long as they comply with these regulations, should be immunized from liability for subscriber-supplied content.[394] "Good Samaritan" provisions should also be enacted to help provide an incentive for service providers to voluntarily undertake good-faith editorial measures in excess of the regulatory minimums.

Compliance should be determined not by the courts, but rather by an administrative agency with the expertise to hear such technical matters. The FCC should also be empowered to sanction ISPs who fail to comply with regulations. As a prerequisite to pursing a lawsuit for damages against an ISP, an author should be required to first obtain an administrative determination that the ISP failed to comply with one or more relevant regulations.[395]

If these standards of conduct are formulated by an informed and responsive regulatory agency, with input from both content providers and service providers, content providers would be assured that service providers are doing the best job technologically and economically feasible. Likewise, service providers would be assured that they are being asked to do no more than is currently feasible.

to sell bandwidth. *See supra* notes 32-34 and accompanying text. Further, unlike the physical monopolies enjoyed by local telephone companies, dial-up customers can, with the economic limits imposed by long distance calling, choose any service provider in the nation. It would therefore be most appropriate to either change the definition of common carrier, or, alternatively, create an entirely new exemption for Internet service providers.

[394] Immunity and regulation go hand in hand. As observed by one intellectual property attorney:

> Giving ISPs a common carrier exemption [without regulation] would be the equivalent of allowing them to have their cake and eat it too. Common carriers in other fields, such as phone companies, have exemptions from certain types of liability because they also are extremely tightly regulated and have a host of legal duties. . . .
>
> If ISPs want the benefits of a common carrier exemption, they must accept the tight regulation that accompanies it.

Hearings on H.R. 2441, *supra* note 160, at 295-96 (statement of William J. Cook, Attorney, Willian, Brink, Hofer, Gilson & Lione).

[395] Administrative agency adjudication would not entirely replace the courts, however, as infringed authors should have immediate access to the courts in order to obtain prompt injunctive relief. Further, the author would be able to seek judicial review of the agency decision, subject to the limitation that the agency's findings of fact would, of course, be given great deference.

VI. CONCLUSION

Information technology is an increasingly vital component of the American economy, making immeasurable economic and educational opportunities available to a wide spectrum of society. Abuse of the Internet, however, threatens to hamper the growth of information technology. Online theft of intellectual property reduces content suppliers' willingness to make their products and services available online. Additionally, uncertain liability for service providers threatens to increase information access costs by providing a disincentive for new business investment in the Internet. If the Internet is to realize its full potential, it must provide a secure legal environment for electronic commerce.

A framework based on litigation and liability is a poor choice. The threat of liability is far too crude of a tool and too inherently retrospective in nature to properly distribute economic incentives to prevent online copyright abuses. Further, leaving the question of service provider liability with the courts will continue to provide uncertainty, as even the best informed judges cannot be expected to render consistent decisions when they are presented with an intensely technical and constantly evolving factual setting, which they are then required to apply to a statutory framework that has been outpaced by technology. Additionally, copyright is wholly statutory in nature and the application of its fundamental purposes to new technologies requires a careful balancing of policy considerations that is within the exclusive purview of Congress. Most importantly, however, a liability-based regime is the worst choice possible for encouraging cooperation between service providers and content providers.

New problems demand new solutions. Congress should supplant the current environment characterized by hostility and litigation with a flexible regulatory framework that ensures all interested parties a seat at the rulemaking table. A negotiated rulemaking approach would help to replace counterproductive distributive thinking with a more prospective viewpoint, thereby encouraging the creative thinking that will be required to develop workable and socially sensitive technological solutions to the increasing problem of online copyright infringement. A regulatory approach would provide the best forum for development of solutions that harness the power of the Internet to correct and prevent the very abuses that it makes possible.

Content providers and access providers, rather than viewing each other as adversaries in a zero-sum game, must be encouraged to recognize that they are actually partners mutually dependent on the secure widespread availability of online content. Ultimately, as stated by the Information Technology Industry Association, a broad-based coalition of service providers and content providers:

> The "debate" as it were should not be "who is responsible," but rather, how to best work together to protect this valuable medium and the content which will be distributed on it. The Internet access and service providers and the copyright holders and content providers are allies, not enemies. As with any successful community, the citizens of this digital community must work together to efficiently, economically, profitably deliver to the legitimate end-user, enhanced and copyright protected valuable content.[396]

TIMOTHY L. SKELTON

[396] *ITAA Discussion Paper*, *supra* note 25, § 3 ("Introduction").

UNIVERSITY OF SAN DIEGO

· A·D·1949 ·