UIC John Marshall Journal of Information Technology & Privacy Law

Volume 18
Issue 3 *Journal of Computer & Information Law - Spring 2000*

Article 1

Spring 2000

Service Provider Liability for Acts Committed by Users: What You Don't Know Can Hurt You, 18 J. Marshall J. Computer & Info. L. 591 (2000)

Mitchell P. Goldstein

ARTICLES

SERVICE PROVIDER LIABILITY FOR ACTS COMMITTED BY USERS: WHAT YOU DON'T KNOW CAN HURT YOU

by MITCHELL P. GOLDSTEIN†

† Mitchell Goldstein is the Director of Virginia's Joint Commission on Technology and Science. He received his J.D., *cum laude*, from The T.C. Williams School of Law at the University of Richmond in 1996 and his B.A., *cum laude*, from Boston University in 1993. Mr. Goldstein has experience in intellectual property and Y2K law.

PREFACE

By 1996, the courts were grappling with the application of current law and principles to the new medium known as the Internet. The decisions appeared to be inconsistent and left little certainty for service providers about what their liability would be for actions committed by subscribers. Congress had just passed the Communications Decency Act, but its implementation was delayed until the courts could decide its constitutionality. Part of that law would eventually be held unconstitutional.

At that time, service provider liability for acts committed by users had implications only for commercial entities who were "in the business of" providing Internet access. These entities include online service providers—those who provide content through proprietary networks in addition to Internet access, which is provided through the same networks—and Internet service providers—those who provide direct access to the Internet and usually have content provided in a central location, often a Web site, that anyone can access.

However, after reviewing the issues and new laws, it is clear that service provider liability can cover much more, including actions by companies that provide space on their networks for consumers to comment about products, people who use commercial programs to access a remote computer, companies that provide bulletin boards or other services to employees on an intranet and so much more. Because the implications of global access are so widespread, it is necessary to begin with the scope of the Internet and the extent of entities that fall into these categories.

I. INTRODUCTION

The Internet was started by the military in the 1960s to decentralize computer networks. The goal was to create a system that could survive a nuclear attack. Today the Internet is composed of not only the military network but also educational, governmental and commercial networks.

While the government (both civilian and military) has the defense of sovereign immunity to protect itself from lawsuits, other service providers are not so fortunate. These Internet and online service providers[1] can expect liability not only for acts that they have committed but also for acts that their subscribers have committed. Because the standard of

1. Internet service providers (ISPs) offer modem access to the Internet through their computers or computer network. Online service providers (OSPs) also provide access to the Internet through computer networks, but they also allow access to proprietary content that is available only to their subscribers. Bulletin board systems (BBSs) offer home computer owners a method for obtaining information from the provider's central data source by use of a modem.

liability in this area is uncertain, Internet and online service providers have no assurances that they will be protected.

An established standard of the liability of service providers for the acts committed by their subscribers is vital to the future of this technology. Many companies entering this field will want to make a profit. To do that, they must charge enough money to cover their expenses and liabilities. They will not be able to cover liabilities that they cannot predict. An unknown or vague standard of liability will frustrate this end.

For the hobbyist, a known standard of liability allows informed risk-taking and enables risk limitation. Because many systems are operated by hobbyists with limited time and money, an exceedingly high or uncertain standard of liability will discourage many from continuing to operate.

An analysis of the extent of the Internet illustrates the gravity of the problem. The Internet provides millions of people all over the world with access to countless databases, e-mail and vital research. It also allows users to transfer files, share research, work with people from remote sites, bank, shop and perform countless other day-to-day functions.

While it is impossible to determine the exact number of people who access the Internet, current estimates range from 130 million[2] to 304 million[3] worldwide, with an estimated 46.5 million[4] in the United States. This figure is expected to reach 90 million in the next four years.[5] Users communicate over the Internet using both commercial and noncommercial networks. By the middle of 1997, the Internet was comprised of 56.2 million host computers and almost 9.6 million Web sites in over 171 countries.[6] These numbers are growing exponentially every year.

The interests of subscribers and providers do not always coincide; when they conflict, problems can occur. Subscribers want to be able to join a service quickly and have complete freedom across the Internet. Providers need to ensure that new subscribers understand the rules of the road and the obligations that they have with respect to uploading material and communicating over the system.

ISPs and OSPs are engaged in the transmission and storage of billions of bits of information and, like those who are responsible for the operations of the Internet, may have no practical ability to control, on a

2. *See Nielsen/ /NetRatings* (visited May 25, 2000) <http://209.249.142.29/nnpm/owa/Nrpublicreports.usagemonthly>.

3. *See Nua Internet Surveys* (visited May 25, 2000) <http://www.nua.ie/surveys/how_many_online/index.html>.

4. *See The Strategis Group* (visited May 25, 2000) <http://www.strategisgroup.com/press/pubs/intdbl.html>.

5. *See id.*

6. *See Hobbes' Internet Timeline* (visited May 25, 2000) <http://info.isoc.org/guest/zakon/Internet/History/HIT.html>.

real-time basis, the content of the information traveling over or residing on their systems. Trillions of bits of data travel around the world each day. Providers cannot and do not monitor or review all this information to determine whether the messages infringe copyright, defame an individual or otherwise violate the law.[7]

OSPs merely provide the means by which individuals can exchange information or communicate. The courts have tried to create a regime that forces providers to spend time, money and resources protecting themselves. They have created an incentive for persons who have been wronged to ignore the real wrongdoers, if they can be identified, and go after the "deep pockets."

Providers have taken many actions on their own to ensure the integrity of the Internet. They have entered into agreements that make users aware of their obligations under copyright law and place responsibility for compliance upon the users. In addition, providers have taken measures to ensure that infringing messages are not posted or are removed when they are made aware of the infringing post. Providers reserve a contractual right to remove any content uploaded by any party for any reason. They can even use technology that allows them to screen for objectionable material. As a last resort, they may terminate a subscriber's access.

These actions may be admirable, but they may also be dangerous. Providers' attempts to regulate their systems may bring other types of liability. A service provider that monitors its servers too closely can be charged with knowledge of the existence of unlawful postings even though that provider had no actual knowledge of their existence. A provider that does not monitor its server at all may be guilty of negligence.

The interactive nature of the Internet raises significant liability concerns. Parties whose intellectual property is being infringed want service providers to be liable because it is difficult and sometimes impossible to identify, locate and prosecute the people who are really responsible. Service providers argue that this strict liability standard will stifle the growth of the Internet.

The most common sources of liability on the Internet are copyright infringement, pornography and defamation. What follows is an analysis of the cases and laws that shape the liability of service providers in this medium.

---

7. Providers may be able to monitor the information using screening programs and people to review it. However, this would be cost-prohibitive and impractical, because ISPs and OSPs may be subject to liability for the illegal postings that they do not catch if they choose to implement this type of surveillance.

II. COPYRIGHT INFRINGEMENT

The Copyright Act (the Act) protects original works of authorship fixed in any tangible medium or expression, whether existing or still to be developed, that can be "perceived, reproduced, or otherwise communicated."[8] Works of authorship include literary works, musical works, motion pictures, sound recordings and many other types.[9] The Act gives the author five exclusive rights: the rights to reproduce, prepare derivative works, distribute copies, perform the work publicly, and display the work publicly.[10] Anyone who violates any of these exclusive rights infringes the copyright.[11]

A. DIRECT INFRINGEMENT

In *Playboy Enterprises v. Frena*,[12] a federal district court had to determine a BBS operator's liability for the acts of users who had uploaded and downloaded the plaintiff's copyrighted photographs. The operator of the BBS was found liable as a direct infringer for violating the plaintiff's right to publicly distribute and display copies of its work.[13] The court granted partial summary judgment to the plaintiff on the issue of copyright infringement.

George Frena operated a subscription BBS that distributed unauthorized copies of Playboy's copyrighted photographs.[14] For a fee, customers could log onto the BBS, look at the pictures and download them onto their computers.

Frena stated that he never uploaded any of Playboy's photographs onto the BBS and that subscribers uploaded the photographs.[15] He also stated that he removed the photographs from the BBS when he received the complaint and had since that time monitored the BBS to prevent additional photographs from Playboy from being uploaded.[16] Frena's operation was clearly commercial. The BBS was provided to those paying twenty-five dollars per month or to those who purchased products from Frena.[17]

The court stated that there was "irrefutable evidence of direct copyright infringement . . . It [did] not matter that [ ] Frena may have been

8. *See* 17 U.S.C. § 102(a).
9. *See id.*
10. *See* § 106.
11. *See* § 501(a).
12. Playboy Enterprises v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993).
13. *See id.* at 1556-57.
14. *Id.* at 1554.
15. *See id.*
16. *See id.*
17. *See Playboy*, 839 F. Supp. at 1557.

unaware of the copyright infringement."[18] In fact, Frena claimed that he innocently and without malice allowed subscribers to upload whatever they wanted onto the BBS. However, intent or knowledge is not an element of infringement, and thus even an innocent is liable for infringement."[19]

The court asked several questions. The first was whether the plaintiff held valid copyrights in the works. Second, the court looked at whether the defendant copied the copyrighted work. Finally, the court asked whether the copying violated one of the rights guaranteed under the Act.[20]

There was no dispute that Playboy owned valid copyrights to the pictures. To prove copying, the plaintiff had to show a similarity between the works available on Frena's BBS and its copyrighted works and that the defendant had access to the copyrighted works.[21] The pictures on the BBS were identical to photos that had appeared in Playboy and even included the Playboy logo. The court inferred access because Playboy sells millions of copies every month across the United States. Finally, the court held that Frena supplied a product containing unauthorized copies of a copyrighted work. This act violated Playboy's right of public distribution of a copyrighted work regardless of whether Frena made the copies himself.

Providing Playboy's photograph's to the BBS's subscribers not only violated Playboy's right to distribute copies of its copyrighted work but also its right to display that work publicly. In the context of copyright, display means any showing of a copy of the work, either directly or through a film, slide, television image or any other device or process.[22] In order for there to be copyright infringement, the display must be public.[23] "A 'public display' is a display 'at a place open to the public or . . . where a substantial number of persons outside of a normal circle of family and its social acquaintances is gathered.'"[24] A place is open to the public even if only paying customers may access it.[25] The court held that Frena's acts clearly fit these definitions.

As a result of this decision, every BBS can be held liable for violating the right of public display. As long as the work is copyrighted and the operator "displays" it on a BBS, the operator may be held liable for direct

18. *Id.* at 1558.

19. *See id.*

20. 17 U.S.C. §§ 101–22.

21. *See id.*

22. *See Playboy*, 839 F. Supp. at 1556 (quoting 17 U.S.C. § 101).

23. *See id.*

24. *See id* at 1557 (quoting 2 MELVILLE B. NIMMER, NIMMER ON COPYRIGHT § 8.14(c), at 8-169 (1993)).

25. *See id.*

copyright infringement. However, not all courts apply the test as strictly, and some do not apply this test for liability at all.

In another case that addressed this issue, *Religious Technology Center (RTC) v. Netcom*,[26] the district court applied the test to the benefit of the online service provider. The court decided that to establish a claim of copyright infringement, a plaintiff must demonstrate ownership of a valid copyright and show that the defendant copied protectable expression.[27]

RTC and Bridge Publications, Inc., holders of copyrights of the Scientology religion, filed suit against Netcom On-Line Communications (Netcom), Thomas Klemesrud (BBS operator), and Dennis Erlich (former minister of Scientology), claiming that Internet postings by Erlich infringed on their protected works. Netcom failed to take action against Erlich even after it was notified of Erlich's infringements. Netcom allowed Erlich's infringing messages to remain on its systems and to be distributed to Usenet servers worldwide. Netcom's failure to cancel the infringing message and stop it from being copied worldwide constituted substantial participation in Erlich's public distribution of the message.

Netcom escaped liability for direct copyright infringement, however, for several reasons. It did not create or control the content of the information available to its subscribers. It did not monitor messages as they were posted.[28] Netcom took no action after RTC informed it that Erlich had posted messages through Netcom's system that violated plaintiffs' copyrights, instead claiming that it could not shut out Erlich without shutting out all of the users of Klemesrud's BBS.[29]

The court believed that "Netcom's act of designing or implementing a system that automatically and uniformly creates temporary copies of all data sent through it is not unlike that of the owner of the copying machine who lets the public make copies with it."[30] This is not direct infringement, but it may be contributory infringement. Although the Act is a strict liability statute, there should still be some element of volition or causation, which is lacking where a defendant's system is merely used by a third party to create a copy.[31] Storing infringing copies on a defendant's system and retransmitting them to other servers is not a direct infringement of the exclusive right to reproduce the work when such copies are uploaded by an infringing user, not by the BBS operator.[32]

---

26. *See* Religious Technology Center v. Netcom, 907 F. Supp. 1361 (N.D. Cal. 1995).
27. *See id.* at 1366 (quoting Baxter v. MCA, 812 F.2d 421 (9th Cir. 1987)).
28. *See id.* at 1368.
29. *See id.*
30. *See id.* at 1369.
31. *See id.*
32. *See Religious Technology Center*, 907 F. Supp. at 1371.

Netcom was not the first link in the chain of distribution. It did not maintain an archive of files for its users. It did not create or control the content of the information available to its subscribers; it merely provided access to the Internet. The court decided that

> [w]here the infringing subscriber is clearly directly liable for the same act, it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet.[33]

On the facts of this case, however, Netcom could still have been found guilty of contributory infringement.

In *Frena*, the defendant had no knowledge of the infringing activity, but the true infringer was unknown. By contrast, in *Netcom*, the defendant had knowledge of the infringing activity and there was a known infringer. The deciding factor for the *Netcom* court seemed to be that Frena profited directly from the acts of its infringing subscriber, whereas the defendants in Netcom did not.

In direct contrast to *Netcom,* the court in *MAI Systems Corp. v. Peak Computer, Inc.*[34] held that a temporary copy is a copy nonetheless. MAI Systems manufactured computers and designed software to run those computers. Peak Computers maintained computers, including MAI computers, for its client. When some businesses that used MAI to service their computers learned of the move of an employee from MAI to Peak, they too switched to Peak.

MAI filed suit against Peak and others alleging, *inter alia,* copyright infringement. The court granted partial summary judgment for MAI and entered a permanent injunction on the issue of copyright infringement. The permanent injunction enjoined the defendants as follows:

> Peak [and certain others were] permanently enjoined from copying . . . or otherwise infringing Mai's copyrighted works . . . The "copying" enjoined . . . include[d] the acts of loading, or causing to be loaded, directly or indirectly, any Mai software from any magnetic storage or read only memory device into electronic random access memory [RAM] of the central processing unit of a computer system.[35]

In its review, the Ninth Circuit affirmed the injunction.[36] To prevail on a claim of copyright infringement, MAI had to prove ownership of a copyright and a "'copying' of protectable expression" beyond the scope of

---

33. *See id.* at 1372.

34. *See* MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993).

35. *See id.* at 515.

36. *See id.* The Court of Appeals modified the injunction on other grounds that are beyond the scope of this paper. *Id.*

a license.[37] MAI software licenses did not allow the use or copying of MAI software by third parties such as Peak.[38] Therefore, any "copying" done by Peak was "beyond the scope" of the license."[39]

A "copying" for purposes of copyright law occurs when a computer program is transferred from a permanent storage device to a computer's RAM.[40] In the absence of ownership of the copyright or express permission by license, this act constitutes copyright infringement.[41]

Peak alleged, but did not offer evidence to prove, that the copy created in the RAM is not fixed. Furthermore, the court acknowledged that "it is a property of RAM that when the computer is turned off, the copy of the program in RAM is lost."[42] The court stated that it "found no case which specifically holds that the copying of software into RAM creates a 'copy' under the Copyright Act."[43] The court went on to note that "it is generally accepted that the loading of software into a computer constitutes the creation of a copy under the Copyright Act."[44] The court concluded by relying on its finding that "the copy created in the RAM can be 'perceived, reproduced, or otherwise communicated' and held that the loading of software into the RAM creates a copy under the Copyright Act."[45]

The court relied on the notion that the loading of software creates a copy under the Act. While the court recognized the distinction between loading software into the hard drive of a computer, which is permanent, and loading software into the computer's RAM, which is temporary, it paid no attention to this distinction. That aside, Peak loaded a copy of the software into its computer systems; Netcom only facilitated the distribution of software. Furthermore, in *Netcom*, the software could not be "perceived, reproduced, or otherwise communicated" until it reached its destination. Netcom escaped liability for direct infringement because it took no direct action to violate RTC's copyrights; Peak was held liable because it took a direct action and made a copy (according to the court) of MAI's copyrighted works. Unlike the system in *Netcom*, Peak's system did not automatically and uniformly create temporary copies of the data sent through it.[46]

---

37. *See id.* at 517 (quoting S.O.S., Inc. v. Payday, Inc., 886 F.2d 1081, 1085 (9th Cir. 1989)).

38. *See id.*

39. *See id.*

40. *See MAI*, 991 F.2d at 518.

41. *See id.*

42. *See id.* at 519.

43. *See id.*

44. *See id.*; *see, e.g.*, Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 260 (5th Cir. 1988).

45. *MAI*, 991 F.2d at 519; *see also* 17 U.S.C. § 101.

46. *See* Religious Technology Center v. Netcom, 907 F. Supp. 1361 (N.D. Cal. 1995).

The important distinction in this case is the court's holding that Peak was not an owner of the copies of the software for purposes of § 117 and thus did not enjoy the right to copy that is conferred on owners by that statute. Peak had merely licensed the software from MAI. The agreement between MAI and Peak imposed more severe restrictions on Peak's rights with respect to the software than would have been imposed if Peak owned copies of the software. They would be subject only to the limits of the copyright holder under the Act. Because Peak only had a license to use the software, its copying was a violation of the Act.[47] If Peak had owned the software, it would have the right to make a copy of the software for the purpose of using it or creating an archival copy.

In the most recent case to address this issue, *Playboy Enterprises, Inc. v. Hardenburgh*,[48] Playboy brought a copyright and trademark infringement action against Rusty-N-Edie's, Inc. (RNE), a BBS, and Russ Hardenburgh, its president. RNE and Hardenburgh operated Rusty-N-Edie's BBS. For a fee, subscribers could access certain files, which were off-limits to the general public, and download a set number of megabytes every week.

To increase its stockpile of available information and thereby its attractiveness to new customers, Rusty-N-Edie's BBS provided an incentive to encourage subscribers to upload information onto the BBS. For every megabyte that subscribers uploaded onto the BBS, they were permitted to download 1.5 extra megabytes of information in addition to the amount available under the terms of the subscription. Information uploaded onto the BBS went directly to an "upload file" where a BBS employee briefly checked the new files to ascertain whether they were "acceptable," meaning not pornographic and not clearly protected by copyright.

Playboy filed suit against RNE and Hardenburgh, alleging that they infringed its copyrights and trademarks. The magistrate in charge of the case recommended that the court grant Playboy's motion for summary judgment regarding the defendants' liability for direct copyright infringement but deny the motion regarding the trademark infringement. The magistrate reasoned that Playboy owned copyrights to the files that appeared on the BBS and that it was immaterial that BBS subscribers uploaded the information, not the BBS operators. As for the allegation of trademark infringement, the magistrate reasoned that Playboy would have to prove that the defendants themselves, and not their subscribers,

47. *See also* Advanced Computer Services of Michigan v. MAI Systems Corp., 845 F. Supp. 356 (E.D. Va. 1994) (holding that MAI customers were not owners of the copyrighted software; they possessed only the limited rights set forth in their licensing agreements).

48. *See* Playboy Enterprises, Inc., v. Hardenburgh, 982 F. Supp. 503 (N.D. Ohio 1997).

engaged in the infringing conduct. Both sides filed objections to this report.

In the district court opinion, Judge Sam Bell relied on *Netcom*, finding that direct infringement must involve some act on the part of the operator. In his words,

> [t]o impose direct infringement liability on a BBS where the operator did nothing more than provide space where information is exchanged, would result in liability for every single . . . server in the worldwide link of computers transmitting [the] subscriber's message to every other computer.[49]

Judge Bell also stated that

> the statute is cast in terms of activities which are reserved to copyright owners. It follows that an infringer must actually engage in one of those activities in order to directly violate the statute. There would be no reason to bifurcate copyright liability into the separate categories of direct and contributory if any remote causal connection to copyright infringement could be analyzed under theories of direct infringement [citation omitted].[50]

In analyzing the facts, the judge distinguished *Frena*, *Sega*,[51] and *Netcom*. He found that the defendants distributed and displayed copies of photographs in derogation of Playboy's copyrights.[52] He focused on two key facts: the defendants encouraged subscribers to upload files, and they used a screening procedure to view all uploaded files and move all approved files to an area for subscribers to view them. These two facts "transform[ed] Defendants from passive providers of a space in which infringing activities happened to occur to active participants in the process of copyright infringement."[53] He believed that:

> [i]t [was] inconsistent to argue that one may actively encourage and control the uploading and dissemination of adult files, but cannot held [sic] liable for copyright violations because it is too difficult to determine which files infringe upon someone else's copyrights.[54]

The defendants violated two of Playboy's exclusive rights: the rights of distribution and public display. The judge focused on the defendants' involvement in the uploading process to hold that they violated Playboy's right of distribution. They "disseminated unlawful copies of [Playboy's] photographs to the public by adopting a policy in which BBS employees moved those copies to the generally available files instead of discarding them."[55] In violating Playboy's right of public display, the defendants

49. *See id.*, at 512 (quoting *Religious Technology Center*, 907 F. Supp. at 1369).
50. *Id.* at 512–13.
51. For a discussion of the *Sega* decision, *see* discussion *infra* Part II.B.
52. *See Playboy*, 982 F. Supp. at 513.
53. *Id.*
54. *Id.*
55. *Id.*

displayed copies of Playboy's photographs "to the public by adopting a policy which allowed their employees to place those photographs in files available to subscribers."[56]

The defendants tried to argue that they could not possibly monitor each and every file to determine whether it violated someone's copyright. This argument failed because they actively engaged in the conduct that led to the infringement.

Judge Bell held that Hardenburgh, as president of the BBS, also was liable for direct copyright infringement because he could not "use the corporate veil as a defense to this action."[57] The judge relied on *Southern Bell Tel. & Tel. v. Associated Tel. Directory Publishers*[58] in holding that Hardenburgh was liable for direct copyright infringement based on the BBS's policies of active participation in the infringing activities. In that case, the Eleventh Circuit stated that an individual, including a corporate officer, who has the ability to supervise infringing activity, or who personally participates in that activity, is personally liable for the infringement.[59]

B. Contributory Infringement

Even if a service provider can escape liability for the direct copyright infringement of its subscribers, it may still face contributory infringement. Courts have included a knowledge requirement before liability can be imposed. The court in *Playboy*, for example, also found the defendants guilty of contributory infringement. The Second Circuit in *Gershwin Publishing Corp. v. Columbia Artists*[60] held that a party shall be liable for contributory infringement where it, "with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another."[61] In *Playboy*, Judge Bell reasoned that the defendants had constructive knowledge that infringing activity was likely to be occurring on their BBS. He stated that "it seem[ed] disingenuous for Defendants to assert that they were unaware that copies of photographs from Playboy Magazine were likely to find their way onto the BBS."[62] However, merely foreseeing the possibility of infringing acts should not be enough for liability, because we can all foresee that anything we create might be used for unlawful purposes.

---

56. *Id.*

57. *Id.*

58. *See* Southern Bell Tel. & Tel. v. Associated Tel. Directory Publishers, 756 F.2d 801, 811 (11th Cir. 1985).

59. *See id.*

60. *See* Gershwin Publishing Corp. v. Columbia Artists, 443 F.2d 1159 (2d Cir. 1971).

61. *See id.* at 1162.

62. Playboy Enterprises, Inc., v. Hardenburgh, 982 F. Supp. 503, 514 (N.D. Ohio 1997).

From the facts presented in *Playboy*, it could be inferred that RNE and Hardenburgh knew of the infringing activity because BBS employees removed copyright information from the photographs when they moved the files. The court believed that that the defendants induced their subscribers to violate Playboy's copyrights because they induced their subscribers to upload files. The court ignored the fact that many of these files were perfectly legal; only 20 of over 100,000 files were proven to infringe Playboy's copyrights.[63]

The *Gershwin* court added that participation must be substantial to prove contributory infringement.[64] Substantial participation was shown through proof that the defendant was in a position to monitor the activity of the direct infringers and therefore should have acted to prevent the infringement."[65]

In *Gershwin*, the American Society of Composers, Authors, and Publishers (ASCAP) brought a copyright infringement action against Columbia Artists Management, Inc. (CAMI), to determine whether CAMI was liable for and could be compelled to pay license fees when musical compositions in the ASCAP repertory were performed at concerts sponsored by local community concert associations promoted by CAMI.[66] The court granted summary judgment for the plaintiff, finding that CAMI had caused the copyright infringement by "organizing, supervising and controlling" the local organization and by "knowingly participating in its infringement."[67]

CAMI's level of participation included numerous acts. For example, it organized concerts and helped to create audiences for artists in communities too small to support a commercial promoter. It was compensated by community artists for its work in the formation and direction of local associations. In addition, artists managed by CAMI paid a management fee. CAMI obtained the titles of the musical compositions that the artists were going to perform and put them in a program with CAMI's name prominently displayed on the cover. CAMI deliberately made no effort to obtain copyright clearance for musical compositions included in the programs and performed at the concerts.[68]

A copyright holder has the exclusive right to perform the copyrighted work publicly for profit.[69] Also, one who, with knowledge of the infringing activity, induces, causes or materially contributes to the in-

63. *See Gershwin*, 443 F.2d at 1162.

64. *Id.* (quoting Apple Computer, Inc., v. Microsoft Corp., 821 F. Supp. 616, 625 (N.D. Cal. 1993)).

65. *Id.* at 1163.

66. *See id.* at 1160.

67. *Id.*

68. *See id.* at 1161.

69. 17 U.S.C. § 106(5).

fringing conduct of another may be held liable as a contributory infringer.[70] In this case, CAMI organized the concerts, knew that copyrighted music would be played at these concerts and profited directly from the success of these concerts.

In addition to holding CAMI liable as a contributory infringer, the court also held it vicariously liable. In reaching this decision, the court stated,

> [w]ith knowledge that its artists included copyrighted compositions in their performances, CAMI created the . . . audience as a market for those artists. CAMI's pervasive participation in the formation and direction of th[e] association and its programming of compositions presented amply supported the district court's finding that it 'caused this copyright infringement.'[71]

The court went on to note that

> [a]lthough CAMI had no formal power to control either the local association or the artists for whom it served as agent, it is clear that the local association depended upon CAMI for direction in matters such as this, that CAMI was in a position to police the infringing conduct of its artists, and that it derived substantial financial benefit from the action of the primary infringers. CAMI knew that copyrighted works were being performed . . . and that neither the local association nor the performing artists would secure a copyright license.[72]

As a result of this level of activity, CAMI was held liable through both contributory infringement and vicarious liability.

The Supreme Court has limited the application of contributory infringement, however. In the landmark case of *Sony Corp. v. Universal City Studios, Inc.*,[73] the Court held that the sale of copying equipment alone does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes.[74] The Court applied a theory of third-party liability to a manufacturer of videocassette recorders (VCRs) for the infringing activities of the products' users. Despite the fact that the VCR enhanced the ability of VCR users to infringe, the Court did not apply a theory of direct infringement to the manufacturers.[75]

Recently, a district court applied these principles to service providers. In *Sega Enterprises, Ltd. v. MAPHIA*,[76] the court had to decide whether a BBS operator was liable for copyright infringement when it solicited subscribers to upload files containing copyrighted materials to

---

70. *See Gershwin*, 443 F.2d at 1162.
71. *Id.* at 1162-63.
72. *See id.* at 1162.
73. *See* Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984).
74. *Id.* at 442.
75. *Id.* at 434.
76. *See* Sega Enterprises, Ltd., v. MAPHIA, 857 F. Supp. 679 (N.D. Cal. 1994).

the BBS, making them made available for others to download.[77] The defendant solicited the uploading and received consideration for the right to download. Users obtained access by paying a fee or by purchasing the defendant's hardware device, which allowed Sega video game cartridges to be copied. The court found that the defendant's knowledge of the infringing activities, encouragement, direction and provision of the facilities through his operation of the BBS constituted contributory infringement, even though the defendant did not know exactly when files were uploaded and downloaded.

There was evidence in the form of printouts and online data from the defendant's BBS (MAPHIA) that the defendant and the BBS knew about the unauthorized uploading and downloading of Sega's copyrighted video games. The defendant solicited the copies so that they could be downloaded. The defendant sometimes charged a direct fee for downloading privileges. Users could even obtain copies of prerelease versions that are not available to the public.[78]

The plaintiff was granted a preliminary injunction, and the defendant's computers were impounded and used as evidence against him.[79] Allowing a practice like this to continue on even one BBS would be devastating to the many industries that rely on copyrights. These practices take away profits from the authors and discourage creativity.

The *Frena* decision runs counter to the other copyright decisions. Similar to the VCRs in *Sony*, a BBS enhances the ability of users to infringe. However, the district court applied the direct infringement test to the same set of facts that the Supreme Court would not: the sale of copying equipment (in this case, the sale of a BBS service) where the product is widely used for legitimate, unobjectionable purposes (in this case, access to data over the Internet). Unlike the defendant in *Gersh-*

77. *See id.* This is one of the postings from the MAPHIA BBS:

> Thank you for purchasing a Console Back Up Unit [copier] from PARSEC TRADING. As a free bonus for ordering from Dark Age, you receive a COMPLEMENTARY Free Download Ratio on our Customer Supporter BBS. This is if you cannot get a hold of SuperNintendo or Sega Genesis games. You can download up to 10 megabytes, which is equal to approximately 20 normal-sized SuperNintendo or Sega Genesis games.

Id. at 683.

78. *See id.* at 684.

79. *See, e.g.*, Steve Jackson Games v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994). When a subscriber has committed a crime, the courts will not always seize the provider's computers. In the Secret Service seized the computers at Steve Jackson Games, a publisher of books, magazines, role-playing games, and related products. Information about Network Security Technology's (an affiliate Bell Company) emergency call system was duplicated and distributed on the BBS run by Steve Jackson Games as a hobby. *Id.* at 459. The information available was nothing more than that which was published and distributed by Bell itself. *Id.* The court held that the Secret Service violated the Privacy Protection Act. *Id.*

win, Frena had no knowledge of the infringing activity. He did not induce, cause or materially contribute to the infringing conduct; he merely provided access to the Internet. He neither assisted his subscribers in any way nor profited directly from their infringing acts. Even if Frena had the knowledge, the precedent of *Sony, Gershwin* and *Sega* should make his crime contributory infringement at most.

C. VICARIOUS LIABILITY

Conduct that falls short of contributory infringement may still be actionable under vicarious liability.[80] A defendant is liable for vicarious liability for the acts of a primary infringer when the defendant has the right and ability to control and supervise the activities of the infringing party[81] and has a direct and financial interest in the activities of the infringer.[82]

The lines of precedent deal

> on the one hand, with the landlord leasing his property at a fixed rental to a tenant who engages in copyright-infringing conduct on the leased premises and, on the other hand, the proprietor or manager of a dance hall or music hall leasing his premises to or hiring a dance band, which brings in customers and profits to the proprietor by performing copyrighted music but without complying with terms of the Copyright Act. If the landlord lets his premises without knowledge of the impending infringement by his tenant, exercises no supervision over him, charges a fixed rental and receives no other benefit from the infringement, and contributes in no way to it, it has been held that the landlord is not liable for his tenant's wrongdoing. But, the cases are legion which hold the dance hall proprietor liable for the infringement of copyright resulting from the performance of a musical composition by a band or orchestra whose activities provide the proprietor with a source of customers and enhanced income. He is liable whether the bandleader is considered, as a technical matter, an employee or an independent contractor, and whether or not the proprietor has actual knowledge of the compositions to be played or any control over their selection.[83]

In the case which applied these lines of precedent, *Shapiro, Bernstein & Co. v. H.L. Green Co., Inc.*,[84] the plaintiffs were the copyright proprietors of several musical compositions. The defendant Jalen Amusement Company, Inc., operated the phonograph department as concessionaire in several stores of defendant H.L. Green Co., Inc. Jalen

80. *See* BLACK'S LAW DICTIONARY 1566 (6th ed. 1990). Vicarious liability is defined as the imposition of liability on one person for the actionable conduct of another, based solely on a relationship between the two persons. *Id.*

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

82. *Id.* at 309.

83. *See id.* at 307.

84. *See id.* at 304.

was charged in the complaint with having infringed the copyrights of these songs by manufacturing records in violation of 17 U.S.C. § 101(e).[85] The complaint also alleged that defendant Green was liable for copyright infringement because it sold, or contributed to, and participated actively in the sale of the bootleg records that were manufactured by Jalen and sold by Jalen in the Green stores.[86]

Jalen was operating under license agreements from Green, which provided that Jalen and its employees were to "abide by, observe and obey all rules and regulations promulgated" by Green.[87] Green, in its "unreviewable discretion," had the authority to discharge any employee believed to be conducting himself improperly.[88] Also, the license agreements provided that Green was to receive a percentage of Jalen's gross receipts from the sale of records, as its full compensation as licensor.[89]

Green retained the ultimate right of supervision over the conduct of the record concession and its employees.[90] By reserving for itself a proportionate share of the gross receipts from Jalen's sales of phonograph records, Green had a most definite financial interest in the success of Jalen's concession.[91] The court held that Green's relationship to its infringing licensee, as well as its strong concern for the financial success of the phonograph record concession, rendered it liable for the unauthorized sales of the bootleg records.[92]

The court reasoned that the protection accorded to literary property would be of little value if insulation for payment of damages could be secured by merely refraining from making an inquiry.[93] It is the innocent infringer who must suffer, since he, unlike the copyright owner, either has an opportunity to guard against the infringement by making a diligent inquiry, or at least the ability to guard against the infringement through an indemnity agreement or insurance.[94] The court concluded that even if a fairly constant system of surveillance is thought too burdensome, Green was in the position to safeguard itself in a less arduous manner against liability resulting from the conduct of its concessionaires.[95]

---

85. *Id.* at 305.

86. *Id.* at 306.

87. *See Shapiro*, 316 F.2d at 306.

88. *See id.*

89. *See id.*

90. *See id.* at 308.

91. *Id.*

92. *Id.*

93. *See Shapiro*, 316 F.2d at 308 (quoting De Acosta v. Brown, 146 F.2d 408, 412 (2d Cir. 1944)).

94. *See id.*

95. *Id.* at 309.

ISPs and OSPs do not fit this test easily: They do not have the necessary level of control over users, and BBS operators cannot monitor the uploading and downloading of every file by every user. With thousands, perhaps even millions, of messages travelling through a BBS every minute, an operator can not monitor all of them in real-time. Requiring this level of control would be unrealistic and burdensome.

Most BBS operators do not have the same level of control over their subscribers that Green had in *Shapiro*. Their relationship is more like that of a landlord and a tenant. Both put certain restrictions on those who use their property and exercise no supervision. Also, both of them usually charge a set fee for a specific period of time.

A court did try to apply this test to a BBS. In *Universal City Studios, Inc., v. Nintendo Co.*,[96] a party established vicarious liability by showing that another party, "with knowledge of the infringing activity, induce[d], cause[d] or materially contribute[d] to the infringing conduct of another."[97] Knowledge of the infringing activity, however, is not always necessary. When a work is copied, even if the person making the copy does not know, or have reason to know, that the work is copyrighted, an infringement may still be found.[98] Even subconscious copying has been held to be an infringement.[99]

This does not mean that knowledge is not needed. The operator still must have knowledge of the infringing material. However, the operator need not know that the material violates the Act.

Of course, if a landlord has knowledge that illegal activity is occurring on his premises, he may have an obligation to do something or risk liability. The BBS operator may have the same responsibility. Providers should not be allowed to bury their heads in the sand while knowing or having reason to know that their premises are being used for illegal conduct. Perhaps this is the correct standard of liability to apply to *Frena*.

D. The Online Copyright Infringement Liability Limitation Act

On October 28, 1998, Congress and the President finally entered the fray with the signing of the Digital Millennium Copyright Act, Public Law 105-304 (DMCA). Title V of the DMCA, the Online Copyright Infringement Liability Limitation Act (OCILLA), contained a new § 512 of the Copyright Act—the most significant change to copyright law since

96. *See* Universal City Studios v. Nintendo Co., 615 F.Supp. 838 (S.D.N.Y. 1985).

97. *See id.* at 857. This is the same test that the Supreme Court applied for contributory infringement in Gershwin Publishing Co. v. Columbia Artists, 443 F.2d 1159 (2d Cir. 1971).

98. *See* Sony Corp. v. Universal City Studios, 464 U.S. 417 (1984).

99. *See* Bright Tunes Music Corp. v. Harrisongs Music, Ltd., 420 F. Supp. 177 (S.D.N.Y. 1976).

the enactment of the Copyright Act of 1976. This law was Congress's attempt to overturn the ruling in *Stratton Oakmont v. Prodigy*.

This law does not protect all ISPs and OSPs. They must first meet the definition of service provider set forth in the OCILLA. In the context of transmitting, routing or providing connections to a third party's information through its system, OCILLA defines a service provider as

> an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.[100]

For the remaining sections of OCILLA, the term service provider also includes "a provider of online services or network access," in addition to those included in the definition above.

Both definitions cover entities such as Netcom Communications and MCI WorldCom, which transport messages from one computer to another through the Internet. The second definition also includes traditional ISPs and OSPs like America Online, CompuServe, Prodigy, Yahoo! and BBSs, which, in addition to transporting messages across the Internet, provide proprietary content to their subscribers. These definitions can also include corporate intranets and media companies that host informational websites. All of these entities provide content through the Internet, online services, or both.

After fitting into one of the definitions, the service provider must meet other conditions. It must adopt and reasonably implement, and inform its subscribers and account holders of, "a policy that provides for the termination . . . of subscribers and account holders . . . who are repeat infringers."[101] In addition, it must "accommodate" and "not interfere with technical measures" that are used by copyright owners to identify or protect copyrighted works.[102]

A service provider is not required to monitor its service or take affirmative steps to seek out the facts surrounding infringing activity on its site or system, except to avoid interfering with standard technical measures.[103] The service provider is not even required to gain access to, remove or disable access to the infringing material if this conduct is prohibited by law.[104]

The first limitation on liability covers transmitting, routing or providing connections for infringing material through a service provider's services or by storing that material in the course of such transmitting,

100. 17 U.S.C. § 512(k)(1).
101. *See* § 512(i)(1)(A).
102. *See* §§ 512(i)(1)(B), (i)(2).
103. *See* § 512(m)(1).
104. *See* § 512(m)(2).

routing or providing connections.[105] This limitation protects the "invisible" systems that work behind the scenes to connect one computer to another. The Internet was designed to transmit information through a series of connections so that a computer in Richmond, Virginia, may send data through computers in New York, Los Angeles and even Paris before the information reaches its intended destination in Washington, D.C.

These invisible systems are protected only if the following conditions are met:

> the transmission of the material was initiated by or at the direction of a person other than the service provider;
>
> the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;
>
> the service provider does not select the recipients of the material except as an automatic response to the request of another person;
>
> no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and
>
> the material is transmitted through the system or network without modification of its content.[106]

Another limitation applies to the practice known as caching. Caching is the practice of retaining, for a limited time, material that has been made available online by a person other than the service provider and then transmitted to a third party at his discretion.[107] By storing this material on its system, the service provider ensures faster access when a subscriber wishes to return to the material.

To qualify for this limitation, the service provider must meet the following conditions:

> The service provider's storage of the material must be carried out through an automatic technical process for the purpose of making the material available to those users who requested the information;
>
> the service provider must transmit the material without modification to its content;
>
> the service provider must comply with the rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online;

105. *See* § 512(a).
106. *See* 17 U.S.C. § 512(a)(1)-(5).
107. § 512(b)(1).

> the service provider must not interfere with the ability of technology associated with the cached material to return certain information to the person who made the information available online;
>
> if the person making the information available online has placed conditions on access to the cached material, such as the payment of a fee or the provision of a password, the service provider must permit access to that material only to those users that have met those conditions and only in accordance with those conditions; and
>
> upon notification of claimed infringement, the service provider responds expeditiously to remove, or disable access to, the infringing material.[108]

The final two limitations cover storing information on the service provider's system at a user's request[109] and referring or linking users to an online site containing infringing material using information location tools (e.g., directories, search engines, hypertext links).[110] A service provider's liability for these activities is limited if the following conditions are met:

> The service provider does not have actual knowledge that the material is infringing, is not aware of the facts or circumstances from which infringing activity is apparent or upon obtaining such knowledge, acts expeditiously to remove, or disable access to, the material;
>
> in a case in which the service provider has the right and ability to control such activity, it does not receive a financial benefit directly attributable to the infringing activity, and
>
> upon notification of claimed infringement, the service provider responds expeditiously to remove, or disable access to, the infringing material.[111]

Where a service provider is required, upon notification, to remove or disable access to infringing material, it must first designate an agent to receive those notifications and provide this information both to the Register of Copyrights and to the public through its Web site.[112]

To be effective, this notification must be in writing and include the signature of a person authorized to act of behalf of the owner of the copyright that has been infringed; identification of the copyrighted work claimed to have been infringed; identification of the material that is claimed to be infringing and information reasonably sufficient to permit the service provider to locate the infringing material; information reasonably sufficient to permit the service provider to contact the complaining party; a statement that the complaining party has a good faith belief that use of the material in the manner complained of is not author-

108. *See* § 512(b)(2).
109. *See* § 512(c).
110. § 512(d).
111. *See* § 512(c)(1)(A)-(C).
112. *See* 17 U.S.C. §§ 512(b)(2)(E), (c)(1)(C), (c)(2), (d)(3).

ized by the copyright owner, its agent or the law; and a statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.[113] Any person who knowingly materially misrepresents that material is infringing in the notification shall be liable for any damages incurred by the alleged infringer, by any copyright owner or its authorized agent, or by a service provider who is injured by that misrepresentation.[114]

If the material later turns out not to be infringing, the service provider has some protection if it acted in good faith.[115] If the service provider removed the material or disabled access to it based on the notification, the service provider must take reasonable steps to notify the subscriber that it has taken this action and allow the alleged infringer to respond.[116]

OCILLA provides procedures for a copyright owner or its authorized agent to request the clerk of any U.S. district court to issue a subpoena to the service provider for identification of the alleged infringer.[117]

If the service provider's conduct does not qualify for limitation, the service provider can still argue that its conduct was not infringing and use other defenses to protect against a claim of copyright infringement.[118] If the service provider is held to have infringed a copyright under the Act, it can be subject to monetary damages and injunctive relief with certain limitations.

This amendment to the Act does not require service providers to police their systems in search of infringing activity. This task is still the responsibility of the copyright owner. Service providers are not even required to gain access to, remove or disable access to material in cases in which those acts are prohibited by law.[119]

E. Court Decisions Revisited

With the amendment of the Copyright Act, the liability of service providers has changed. A service provider will no longer be held liable for the infringement of its subscribers unless it has knowledge of the infringing activity. While there is no doubt that OCILLA covers the defendants in the above-mentioned cases, not all of the decisions would change under the new law.

---

113. *See* § 512(c)(3).
114. *See* § 512(f).
115. *See* § 512(g)(1).
116. *See* § 512(g)(2).
117. *See* § 512(h).
118. *See* 17 U.S.C. § 512(l).
119. *See* § 512(m).

Peak Computer would still be liable for copyright infringement because in that case, it had only licensed the software. Because it was not an owner of the software, Peak was bound by the restrictions set out in its license. One of those restrictions was that Peak could not copy the software for any reason.

Hardenburgh and his BBS would also retain their liability. The transmission of the material in that case was not carried out through an automatic technical process as required by 17 U.S.C. § 512(a)(2). In addition, employees of the BBS selected the material to be published through the screening process. Even if the BBS did not have knowledge of the infringing material, its affirmative acts would place it outside the protections and limitations of OCILLA.

Netcom still would not be liable and Frena and MAPHIA would escape liability. Neither service provider violated the conditions set forth under 17 U.S.C. § 512(a). Therefore, they would not liable for the infringement of their subscribers as long as they complied with the removal provisions.

III. PORNOGRAPHY

The Supreme Court developed a test for obscene pornography in *Miller v. California.*[120] The obscenity determination is to be based on community standards and not on national standards. Material is obscene if the average person, applying contemporary community standards, would find that the work, taken as a whole, appeals to the prurient interest; the materials depict or describe, in a patently offensive way, sexual conduct specifically prohibited by applicable state law; and the work, taken as a whole, lacks serious literary, artistic, political or scientific value.[121] This last requirement does not vary from community to community.[122] The Supreme Court tried to avoid developing a national test. The Court believed that such a test would be unworkable.

Defendants may not claim as a defense that they did not know the material in question was obscene according to community standards under the *Miller* test.[123] They may still claim as a defense that they did not know that the obscene material was present, but they may not use their ignorance of the applicable community standard as a defense.

The Court mandated a scienter (knowledge) requirement in obscenity laws in *Smith v. California*[124] long before it developed the *Miller* test. In *Smith,* the proprietor of a bookstore was convicted for violating a mu-

120. *See* Miller v. California, 413 U.S. 15 (1973).
121. *See id.* at 24.
122. *See* Pope v. Illinois, 481 U.S. 497 (1987).
123. Hamling v. United States, 418 U.S. 87, 123-24 (1974).
124. *See generally* Smith v. California, 361 U.S. 147 (1959).

nicipal ordinance, which made it unlawful for any person to possess an obscene or indecent writing in any business where books are sold.[125] The imposition of a jail sentence depended solely on the bookstore's possession "of a certain book found upon judicial investigation to be obscene."[126]

The Court held that strict liability in these cases would seriously restrict the dissemination of books that are not obscene by penalizing booksellers even though they had no notice of the book's character.[127] Every bookseller would be placed under an obligation to be aware of the contents of every book in the store. It would be unreasonable to demand a level of knowledge so near omniscience.[128] Imposing this type of strict liability statute would also have a chilling effect. It would tend to impose a severe limitation on the public's access to constitutionally protected matter.

How this test will apply to a BBS is unknown. A BBS, like a library or bookstore, contains thousands, sometimes billions, of bits of information. There is no way that a systems operator can monitor all of this information. However, courts may be able to impute knowledge on the systems operator based on the amount of control the operator has over the BBS.

Once system operators are aware that offending messages have been posted on the board, they arguably have a duty to remove the message.[129] Proof of scienter might be shown by the totality of the circumstances surrounding the operation, such as limited access, extensive password protection or a pattern of abuse. For BBS operators who take extensive measures to limit the potential of illegal activity on their boards or who have experienced illegal activity on their boards many times before, it may be implied that they know that the obscene material is present on their boards.

Since the Court developed the community standards requirement, the question has become, "Whose community standards should be applied?" When obscene material is physically sent from one community to another, either community's standards could apply. However, when obscene material is sent through the Internet, it appears simultaneously everywhere and nowhere. While the obscene material remains on the operator's BBS, anyone can access it with little more than a computer and a modem.

---

125. *Id.* at 148.

126. *See id.*

127. *See id.* at 152.

128. *See id.* at 153-54.

129. *See* United States v. Mishkin, 317 F.2d 634, 637 (2d Cir. 1963).

A. UNITED STATES V. THOMAS

The first obscenity case in which BBS operators were charged in the place where the material was received, rather than where it originated, was *United States v. Thomas.*[130] The Thomases operated an adults-only sexually oriented BBS in Milpitas, California, called Amateur Action. Access was limited to members who were given a password after they paid a membership fee and submitted a signed application form that requested the applicant's age, address and phone number. Mr. Thomas would then call the number to verify the information.

People who called the BBS without a password could only view the introductory screens, which contained brief, sexually explicit descriptions of graphic interchange format (gif) files and adult videotapes that were offered for sale. Customers would order the tapes by sending Mr. Thomas an e-mail message, and he would typically deliver them via United Parcel Service (UPS).

A United States postal inspector received a complaint regarding the BBS from an individual residing in the Western District of Tennessee. Working closely with an assistant U.S. attorney in Memphis, he became a member of the Amateur Action BBS. He then downloaded sexually oriented images, ordered a videotape, which was delivered by UPS, and sent an unsolicited videotape containing child pornography to the Thomases. The Thomases were indicted on obscenity charges based on those downloads.[131]

A Memphis jury convicted the Thomases on all of the obscenity charges, but not on the child pornography charge. Mr. Thomas was sentenced to thirty-seven months and Mrs. Thomas to thirty months. The jury also convicted the Thomases of an additional charge of one count of forfeiture under 18 U.S.C. § 1467.[132] This meant that the computer sys-

130. U.S. v. Thomas, 74 F.3d 701 (6th Cir. 1996).

131. *Id.* at 705-06. A federal grand jury for the Western District of Tennessee returned a twelve-count indictment charging Robert and Carleen Thomas with the following criminal violations: one count under 18 U.S.C. § 371 for conspiracy to violate federal obscenity laws 18 U.S.C. §§ 1462, 1465, six counts under 18 U.S.C. §1465 for knowingly using and causing to be used a facility and means of interstate commerce—a combined computer/telephone system—for the purpose of transporting obscene, computer-generated materials (the gif files) in interstate commerce, three counts under 18 U.S.C. § 1462 for shipping obscene videotapes via UPS, one count of causing the transportation of materials depicting minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(1) as to Mr. Thomas only (count 11), and one count of forfeiture under 18 U.S.C. § 1467. *Id.*

132. *See* 18 U.S.C. § 1467. Criminal forfeiture

> (a) Property subject to criminal forfeiture. - A person who is convicted of an offense involving obscene material . . . shall forfeit to the United States such person's interest in
>
> (1) any obscene material produced, transported, mailed, shipped, or received in violation of this chapter;

tem was to be forfeited to the United States.

Pornography vendors in more liberal jurisdictions have been prosecuted if they have knowingly or intentionally distributed obscenity into conservative jurisdictions. This case calls into question the meaning of "community standards." After all, communities are no longer defined by geographic boundaries. The case begs the question "Should the community standards in Memphis, Tennessee apply to material on a computer in California?"

According to this case, the community standard becomes that of the most conservative jurisdiction with a phone line and a computer. This analysis runs contrary to the decision of the Supreme Court in *Miller*, in which it tried to avoid a national standard for obscenity law.

The Thomases tried to argue that venue was improper. However, to establish a violation under 18 U.S.C. § 1465, the government need only prove that a defendant knowingly used a facility or means of interstate commerce for the purpose of distributing obscene materials. Venue lies in any district in which the offense was committed.[133] There is no constitutional impediment to the government's power to prosecute pornography dealers who distribute unprotected material in any district into which the material is sent.[134] The statute established a continuing offense within the venue provisions of 18 U.S.C. § 3237(a) that occurs in every judicial district which the material touches.[135] Venue for federal obscenity prosecutions lies in any district from, through, or into which the allegedly obscene material moves.[136] This may result in people being prosecuted in a community to which they have sent materials that would be obscene under that community's standards though the community from which it was sent would tolerate the same material.[137]

While the Thomases were convicted of violating Memphis' community standards, this case is far from determinative of the liability of service providers for illegal pornography or obscene materials posted by subscribers. In this case, the defendants had knowledge and control over the jurisdictions where materials were distributed. They had methods to limit user access in jurisdictions where the risk of a finding of obscenity

---

(2) any property, real or personal, constituting or traceable to gross profits or other proceeds obtained from such offense; and
(3) any property, real or personal, used or intended to be used to commit or to promote the commission of such offense, if the court in its discretion so determines . . . .

Id.

133. *Thomas*, 74 F.3d at 709 (quoting United States v. Beddow, 957 F.2d 1330, 1335 (6th Cir. 1992)).

134. *See id.* (quoting United States v. Bagnell, 679 F.2d 826, 830 (11th Cir. 1982)).

135. *See id.*

136. *See id.* (quoting United States v. Peraino, 645 F.2d 548, 551 (6th Cir. 1981).

137. *See id.* at 711.

was greater than that of California. Under the facts of this case, the Court found no need to redefine "community" for use in obscenity prosecutions involving BBSs.

Also, the defendants failed to raise the argument that "facility or means of interstate commerce" does not include "any method of communication between different states." They did not argue that the application of the statute in this case was an improper expansion of the meaning of the statute. While they did try to argue that the gif files were intangible and thus outside the scope of 18 U.S.C. § 1865, the court held that the manner in which the images moved did not affect their ability to be viewed on a computer screen in Tennessee or their ability to be printed out in hard copy in that distant location.[138] Given that the Thomases sent materials through the mail to Memphis that could be considered obscene, it was not a surprise that Memphis' standards were applied.

The question still remains whose community standards will be applied in a case where a subscriber places obscene material on a BBS. The material does not have a physical location. Also, the community may be difficult to define, and it will not be defined based on geographic boundaries.

Community is defined as a social group of any size whose members reside in a specific locality, share government, and often have a common cultural and historical heritage.[139] It is also a social, religious, occupational, or other group sharing common characteristics or interests and perceived or perceiving itself as distinct in some respect from the larger society within which it exists.[140] Internet users consider themselves distinct from the larger society and share many of the facets of a society that a geographic community shares. The Court has yet to alter its definition of community standards, but it is clear that this standard does not readily apply to the Internet.

B. THE COMMUNICATIONS DECENCY ACT

In February 1996, Congress passed Public Law 104-104: the Communications Decency Act of 1996 (CDA). Congress hoped "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material."[141] The CDA regulates materials sent directly to children. It also imposes felony penalties on anyone who

138. *See id.* at 707.

139. *See* RANDOM HOUSE UNABRIDGED DICTIONARY 414 (2d ed. 1993).

140. *See id.*

141. 47 U.S.C. § 230(b)(4).

> in interstate commerce or foreign communications by means of a telecommunications device knowingly makes, creates, or solicits, and initiates the transmission of, any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person.[142]

The law forbids the same conduct where the person knows that the recipient is under 18 years of age, "regardless of whether the maker of such communication placed the call or initiated the communication."[143]

Furthermore, § 230 of the law[144] provides that no interactive computer service provider[145] or user of such a system shall be treated as the publisher or speaker of any information provided by an information content provider.[146] It also provides that "no provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected;[147] or any action taken to enable or make available to information content providers or others the technical means to restrict access to said material.[148]

The CDA had its critics. Senator Patrick Leahy advocated its repeal even before it went into effect. In a statement before Congress, he stated that the legislation looks to the authority of the Federal Communications Commission to describe the precautions that can be taken to avoid criminal liability for posting indecent material.[149] It bans "patently offensive" and "indecent" communications. These are rather vague terms.

As a result of the law, America Online (AOL) deleted the profile of a women from Vermont who communicated with fellow breast cancer survivors online. According to AOL, she used the word breast, which AOL deemed vulgar. AOL later apologized and indicated it would permit the

---

142. *See* § 223(a)(1)(A).

143. *See* § 223(a)(1)(B).

144. *See* § 230(c)(1).

145. *See* § 230(e)(2). An interactive computer service is any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions. *Id.*

146. *See* § 230(e)(3). An information content provider is any provider or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service. *Id.*

147. *See* 47 U.S.C. § 230(c)(2)(A).

148. *See* § 230(c)(2)(B).

149. *See Statement of Senator Leahy on Repealing the Communications Decency Act*, Government Press Releases, Feb. 9, 1996, *available at* 1996 WL 8783190.

use of the word where appropriate without providing guidelines on what uses would be considered appropriate.

Senator Leahy was also concerned that advertisements that would be legal in print may subject providers to liability under this new law. Information about birth control, AIDS and even potty training could be affected.

The industry has also voiced its concern. On the same day that the bill was signed by President Clinton, twenty plaintiffs, including the American Civil Liberties Union, filed suit against U.S. Attorney General Janet Reno "seeking to enjoin the enforcement of the CDA on the ground that it violates the Constitution of the United States."[150] One week later, a federal district court in Pennsylvania enjoined enforcement of the provisions of the CDA regulating transmission of indecent materials, pending final resolution by a three-judge panel.[151] The judge believed that:

> plaintiffs have raised serious, substantial, difficult and doubtful questions . . . in their argument that the CDA is unconstitutionally vague in the use of the undefined term "indecent." § 223(a)(1)(B)(ii). This [struck him] as being serious because the undefined word "indecent," standing alone, would leave reasonable people perplexed in evaluating what is or is not prohibited by the statute.[152]

This word alone was the basis for a criminal felony prosecution.

The vagueness of the law not only added more uncertainty to the standard of liability but also could increase liability. This law could forbid using an indecent four-letter word, or discussing material deemed to be indecent, on BBSs or Internet chat areas and newsgroups accessible to children.

The CDA applies to any complaint instituted after its effective date, regardless of when the relevant conduct giving rise to the claims occurred.[153] It is Title V of the Telecommunications Act of 1996, which was designed to reduce regulation and encourage the rapid deployment of new telecommunications technologies.

The Supreme Court, in *ACLU v. Reno*,[154] held that the provisions of the CDA prohibiting transmission of obscene or indecent communications by means of telecommunications device to persons under age 18, or sending patently offensive communications through an interactive computer service to persons under 18, were content-based blanket restric-

150. *See* Richard Raysman & Peter Brown, *Liability of Internet Access Provider Under Decency Act*, 215 N.Y. L.J. 3 (Mar. 12, 1996).

151. *See* American Civil Liberties Union v. Reno, 1996 WL 65464 (E.D. Pa. 1996).

152. *See id.* at *2.

153. 47 U.S.C. § 230(d)(3). *Cf.* Zeran v. America Online, 129 F.3d 327 (4th Cir. 1997) and Doe v. America Online, 718 So.2d 385 (Fla. App. 1998).

154. *See* Reno v. ACLU, 521 U.S. 844 (1997).

tions on speech. The challenged provisions were facially overbroad in violation of the First Amendment. The constitutionality of the provision prohibiting the transmission of obscene or indecent communications by a telecommunications device to persons under age 18 would be saved from facial overbreadth challenge by severing the phrase "or indecent" from the statute.

Section 223(a) of the CDA criminalizes the knowing transmission of "obscene or indecent" messages to any recipient under 18. The district court enjoined the government from enforcing § 223(a)(1)(B) insofar as it relates to "indecent" communications. Section 223(d) prohibits the knowing sending or displaying to a person under 18 of any message that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs. In addition, the court enjoined the government from enforcing § 223(d) at all. The Supreme Court affirmed this decision.

These provisions are qualified by affirmative defenses. A service provider could escape liability if it took "good faith, reasonable, effective, and appropriate actions" to restrict or prevent access by minors. Another defense is available if the service provider restricted access by requiring a credit card, an adult access code, or adult personal identification number, measures designed to require proof of age.

Because this statute is a content-based regulation on speech, it must pass the strict scrutiny test established by the Supreme Court before it will be considered valid. Under this test, the statute must be narrowly tailored to meet a compelling state interest. In addition, the restriction must be the least restrictive means to achieve the compelling interest.

The Court expressed its concern that the terms "indecent" and "patently offensive" were not defined. The vagueness of this content-based regulation coupled with its increased deterrent as a criminal statute raise (sic) special First Amendment concerns because of its obvious chilling effect.[155] The CDA's vagueness undermined the likelihood that it was carefully tailored to the congressional goal of protecting minors from potentially harmful materials. The Court acknowledged that the government has an interest in protecting children from potentially harmful materials. However, the CDA was not narrowly tailored. "There [was] no textual support for the submission that material scientific, educational, or other redeeming social value [would] necessarily fall outside the CDA's prohibitions."[156]

The Court also addressed the defenses available to service providers, stating that it would prohibitively expensive for noncommercial and some commercial speakers who have Web sites to verify that their users

155. *Id.* at 845.
156. *See id.* at 847.

are adults.[157] The defenses provided by the CDA were not economically feasible for most noncommercial providers to adequately protect them from prosecution.

The Court stressed throughout its opinion that the user must take affirmative steps to access information on the Internet. Therefore, restrictions concerning the Internet will not be analyzed like other media, which are often more restricted. In addition, the Internet is not a scarce, expressive commodity that requires regulation in the way that television or radio frequencies are. This decision officially gave full constitutional protection to the Internet, unlike any other medium.

Almost all sexually explicit images available online are preceded by warnings as to the content. The district court stated that "odds are slim that a user would come across a sexually explicit sight by accident."[158]

The first prohibition (§ 223(a)) uses the term "indecent" while the second (§ 223(d)) uses the term "patently offensive." Given the absence of a definition of either term, this difference in language will provoke uncertainty among speakers about how the two standards relate to each other and just what they mean.[159] The vagueness of the CDA raises First Amendment concerns because, as a content-based regulation of speech, it has a chilling effect on arguably protected speech. Also, the "severity of criminal sanctions may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images.[160]

The Court established the *Miller* standard for obscenity to determine whether material is protected by the First Amendment. In the case of the CDA, the terms that set forth what material is prohibited are not defined. In addition, the CDA extends to include excretory activities as well as organs of both a sexual and excretory nature. Finally, the limitation that the work, taken as a whole, must lack serious literary, artistic, political, or scientific value is absent from the CDA. Language that is indecent or offensive, but not obscene, is protected by the First Amendment.[161]

---

157. *See id.* at 877.

158. *See id.* at 869. However, the accuracy of this statement is somewhat debatable. While researching a potential trademark for a client of my former firm, I entered an innocuous Web site address and was immediately transported to a site filled with pornography and "teasers." This information appeared on my computer by accident. While a warning preceded it, I had to scroll down to see the substance of the warning and ended up seeing more substance that I cared to see.

159. *See Reno*, 521 U.S. at 871.

160. *See id.* at 872.

161. *See* Sable Communications of California, Inc. v. FCC, 492 U.S. 115 (1989); FCC v. Pacifica Foundation, 438 U.S. 726 (1978); Carey v. Population Services Int'l, 431 U.S. 678 (1977).

In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the governmental purpose that the statute was enacted to serve.[162]

The breadth of the CDA was unprecedented. The undefined terms covered large amounts of nonobscene and nonpornographic material with educational or other value.[163] The Court noted that transmitting obscenity and child pornography is already illegal under federal law.[164]

The community standards criterion as applied to the Internet creates a national standard, which the Court refused to create in *Miller* and refused to create in this case. Doing so would lead all speech to be judged by the most conservative community in the country, if not the world.

Under the CDA, a mother allowing her 17-year-old to use the family computer to obtain information on the Internet that the mother, in her parental judgment, deems appropriate could face a lengthy prison term.[165] A father who sends his 17-year-old son at college information on birth control via e-mail could be incarcerated even though neither he, his child, nor anyone in their home community found the material "indecent" or "patently offensive," if the college town's community thought otherwise.

To draw a line between speech covered by this statute and speech not covered by this statute "involves a far more serious invasion of the legislative domain."[166] The Court refused to rewrite the law to conform to constitutional requirements.

Even after the Court limited the reach of the CDA in *Reno*, the statute still had an impact on the state of the law. The immunity that was established by § 230 remained intact.

The first state court case to apply this provision was *Doe v. America Online, Inc.*[167] In 1994, Richard Lee Russell committed sexual battery on John Doe, who was then eleven years old. Russell engaged Doe and other minor males to perform sexual activities on him and another while videotaping and photographing these sexual acts. Russell used AOL chat rooms to market the videotape and photographs.

Doe's mother filed suit, alleging several state law causes of action against AOL and Russell. She claimed that AOL reserved the right to

162. *See* Reno v. ACLU, 521 U.S. 844, 874 (1997).
163. *See id.* at 878.
164. *See* 18 U.S.C. §§ 1461–65, 2251.
165. *See* 47 U.S.C. § 223(a)(2).
166. *See Reno*, 521 U.S. at 884.
167. *See* Doe v. America Online, 718 So.2d 385 (Fla. App. 1998).

monitor the chat rooms to ensure that members adhered to its rules and to the law. She claimed that AOL had knowledge of the activities because others had complained about Russell's acts.

AOL moved to dismiss the case, arguing that Doe's claims are barred by § 230. The trial court dismissed the case against AOL, stating that "making AOL liable for Russell's chat room communications would treat AOL as the 'publisher or speaker' of those communications."[168] The court held that the CDA bars such claims.

Doe appealed. The appellate court upheld the trial court's decision, basing its decision on *Zeran v. America Online*.[169] In addition, the court held that section 230 preempted the statutory and common laws of the state.[170]

Congress did not give up on its attempt to protect children from pornography. One and a half years after the Supreme Court struck down provisions of the CDA, Congress enacted the Child Online Protection Act (COPA).[171]

The government tried to remedy the problems with the CDA by enacting COPA, which was to go into effect on November 29, 1998, until Web site operators and content providers filed a lawsuit challenging its constitutionality in *ACLU v. Reno II*.[172] Unlike the CDA, COPA limited the prohibition to commercial purposes only but extended the content to all material that is harmful to minors. Material that is harmful to minors must, "taken as a whole, lack[ ] serious literary, artistic, political, or scientific value for minors."[173]

COPA retained the idea of affirmative defenses established in the CDA. These defenses apply if "in good faith, the defendant ha[d] restricted access by minors to material that is harmful to minors."[174] ISPs were specifically excluded.[175]

Like the CDA, violations of COPA may involve prison. Under COPA:

> Whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than $50,000, imprisoned not more than

168. *See id.* at 387.

169. *See* Zeran v. America Online, 129 F.3d 327 (4th Cir. 1997). For a more extensive discussion of *Zeran*, *see* discussion *infra* Part IV.C.

170. *See Doe*, 718 So.2d at 389.

171. *See* 47 U.S.C. § 231.

172. *See* American Civil Liberties Union v. Reno, 31 F.Supp.2d 473 (E.D. Pa. 1999).

173. *See* § 231(e)(6).

174. *See* § 231(c)

175. *See* § 231(b).

6 months, or both.[176]

Intentional violations lead to a fine of not more than $50,000 for each violation in addition to the previous penalties.[177] Civil penalties consisting of fines of not more than $50,000 also apply to violations of this Act.[178]

Like the CDA, COPA posed problems for the courts. Nothing in the text of COPA limits its applicability to commercial pornographers. COPA applies to communications that include, but are not necessarily wholly comprised of, material that is harmful to minors. Blocking or filtering technology may be at least as successful as COPA in restricting minors' access to harmful material online without imposing the burden on constitutionally protected speech that COPA imposes on adult users or Web site operators.

The same district court that enjoined the government from enforcing the CDA also preliminarily enjoined the government from enforcing § 231.

Obscenity is a concern because it is not protected by the First Amendment.[179] Service providers cannot use the First Amendment as a defense. A carrier of potentially obscene material must be wary of differences in the definitions of obscenity among the states[180] because it can be subject to jurisdiction in multiple states with diverse degrees of liability.

Systems operators can be held liable under any and all of these laws. The Supreme Court has even held that operators of adult bookstores could be prosecuted under a state racketeering influenced and corrupt organizations (RICO) statute for substantive obscenity violations.[181] BBSs are not very different from these bookstores. Both provide limited access to constitutionally protected material, as well as possibly unprotected material, and neither is able to monitor all of the information within its grasp. Perhaps BBS operators may one day be held liable under a RICO statute. BBS operators are protected to the extent that they cannot divulge data contained in an electronic communication service to an outside source except under limited circumstances; this includes pornographic messages.[182]

176. *See* § 231(a)(1).

177. *See* 47 U.S.C. § 231(a)(2).

178. *See* § 231(a)(3).

179. *See* Kois v. Wisconsin, 408 U.S. 229 (1972).

180. *See* Hamling v. United States, 418 U.S. 87 (1974).

181. *See* Fort Wayne Books, Inc. v. Indiana, 489 U.S. 46 (1989).

182. *See* 18 U.S.C. §§ 2701(a)(1), 2703–04 (1988).

IV. DEFAMATION

A. DEFAMATION LAW BEFORE THE CDA

In the landmark case of *New York Times v. Sullivan,*[183] the Supreme Court established the liability of publishers for defamation[184] of public officials. The Court stated that in order for a public official to recover damages in a defamation action, the plaintiff must show that the speaker acted with actual malice.[185] Actual malice is defined as knowingly false or reckless disregard for the truth.[186]

The Court expanded this doctrine in *Curtis Publishing Co. v. Butts,*[187] and *Associated Press v. Walker.*[188] *Curtis Publishing* involved the defamation of people who were not public officials but who were public figures. The Court held that some people, even though they are not part of the government, are nonetheless sufficiently influential to affect matters of important public concern.[189] Public figures are "those who, by reason of the notoriety of their achievements or the vigor and success with which they seek the public's attention, are properly classed as public figures."[190]

The Court further defined public figures in *Robert Welch, Inc., v. Gertz.*[191] In *Welch*, an attorney had represented a victim's family in a civil litigation against the police officer convicted of the killing. The defendant made false statements about the attorney in its publication *American Opinion.*

The Court ruled that the police officer was not a public figure, and, therefore, the publisher was not entitled to the protection under *Sullivan.* The attorney had not thrust himself into the vortex of this public issue, nor did he engage the public's attention in an attempt to influence the outcome.[192] The Court further determined that as long as liability is not imposed without some basis of fault, the states are free to write their own rules for private libels.[193]

---

183. *See* New York Times v. Sullivan, 376 U.S. 254 (1964).

184. *See* BLACK'S LAW DICTIONARY 417 (6th ed. 1990). Defamation is an intentional false communication, either published or publicly spoken, that injures another's reputation or good name. *Id.*

185. *See New York Times*, 376 U.S. at 273.

186. *See id.*

187. Curtis Publishing Co. v. Butts, 388 U.S. 130 (1967).

188. Associated Press v. Walker, 388 U.S. 130 (1967). This case was a companion case to *Curtis*, 388 U.S. at 130.

189. *See Curtis*, 388 U.S. at 164.

190. Robert Welch, Inc. v. Gertz, 418 U.S. 323, 342 (1974).

191. *See id.*

192. *See id.* at 345.

193. *See id.* at 347.

There are justifications for the heightened need of the state to protect a private person. Private persons are not on the same footing as a libeler.[194] In addition, public persons hold themselves out to public scrutiny and ridicule, while private persons do not.[195]

The Court limited its definition of a public figure and the ensuing limitation of liability. The Court decided that "[a]bsent clear evidence of general fame or notoriety in the community, and pervasive involvement in the affairs of society, an individual should not be deemed a public personality for all aspects of his life."[196] One must look "to the nature and extent of an individual's participation in the particular controversy giving rise to the defamation.[197]

The Court extended *Sullivan* further in *Dun & Bradstreet, Inc., v. Greenmoss Builders, Inc.*[198] Dun & Bradstreet, a private credit-reporting firm, published false information about Greenmoss Builders, suggesting that they had filed for bankruptcy, when in reality it was an employee who had filed. The Court held that the crucial distinction was whether the speech involved a public issue, public speech or an issue of public concern. While *Gertz* did not clearly draw the distinction, it was clear from the facts that such a limitation was implied.

On the Internet, the distinction between public and private persons is blurred. For example, a person can respond and attack; this is called "flaming" and is quite common. In addition, people continually hold themselves out for public scrutiny and ridicule. A person must complete several steps to sign up, read posts, and then enter the debate. By taking these voluntary steps to enter a debate and seek "public attention," knowing the potential for public scrutiny, even private people can thrust themselves into the public realm. While these people would not be public officials as defined by *Sullivan,* they could be public figures for the specific debate as defined by *Gertz.*

The question still exists about where commercial enterprises or private non-members fit into this mess. Must they seek public attention on the BBS? Or is it enough that they seek public attention elsewhere? Do they actually have the access to the channels of effective communication to counteract any false statements? These questions have yet to be answered. While these questions are important, they are beyond the scope of this paper.

---

194. *See id.* at 344.

195. *See* Welch, 418 U.S. at 345.

196. *See id.* at 352.

197. *See id.*

198. *See* Dun & Bradstreet, Inc., v. Greenmoss Builders, 472 U.S. 749 (1985).

B. A Split in the Courts: *Cubby* Versus *Stratton Oakmont*

OSPs confronted the issues surrounding online defamation for the first time in *Cubby, Inc., v. CompuServe, Inc.*[199] Cubby, Inc., and Robert Blanchard jointly developed "Skuttlebut," a database designed to carry news of the journalism industry to compete with another database, "Rumorville." Rumorville published items about Cubby that were carried nationwide on CompuServe. Cubby filed suit against CompuServe, claiming that these statements were false and defamatory.

Cameron Communications, Inc. (CCI), managed, reviewed, created, deleted, edited and controlled the content of the "Journalism Forum" in accordance with editorial and technical standards and conventions of style as established by CompuServe.[200] The Journalism Forum was one of over 150 special interest forums.[201] Rumorville was a daily newsletter that provided reports about broadcast journalism and journalists.[202]

Rumorville was published by Don Fitzpatrick Associates (DFA). DFA accepted total responsibility for the contents of Rumorville. CCI was required to limit access to Rumorville to those CompuServe Information Service subscribers who had made membership arrangements with DFA.[203]

CompuServe had no opportunity to review Rumorville's contents. CompuServe received no part of any fees that DFA charged for access to Rumorville, nor did CompuServe compensate DFA for providing Rumorville to the Journalism Forum.[204] CompuServe did not know of any complaints before suit being filed.

CompuServe claimed that it was a distributor and not a publisher of the material and could not know of the statements.[205] Generally, a party who repeats or republishes defamatory matter is liable as if he had originally published the statement.[206] However, news vendors, book stores, libraries, vendors and distributors of defamatory publications are not liable if they did not know or have reason to know of the defamation.[207]

Freedom of speech and of the press prevent the government from imposing strict liability on distributors for the content of materials they

199. *See* Cubby, Inc., v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).
200. *See id.* at 137.
201. *See id.*
202. *See id.*
203. *See id.*
204. *See id.*
205. *See* Cubby, 776 F. Supp. at 138.
206. *See id.* at 139 (quoting Cianci v. New York Times Publishing Co., 639 F.2d 54, 61 (2d Cir. 1980)).
207. *See id.* (quoting Lerman v. Chuckleberry Publishing, Inc., 521 F. Supp. 228 (S.D.N.Y. 1981)).

carry.[208] In addition, a state may not constitutionally enact a criminal statute that would be beyond the reach of its civil law of libel. The fear of damage awards can have significantly more potential to inhibit a party than the fear of prosecution under a criminal statute.[209]

The court summed up the liability as follows:

> Technology is rapidly transforming the information industry. A computerized database is the functional equivalent of a more traditional news vendor, and the inconsistent application of a lower standard of liability to an electronic news distributor such as CompuServe than that which is applied to a public library, book store, or newsstand would impose an undue burden on the free flow of information. Given the relevant First Amendment considerations, the appropriate standard of liability to be applied to CompuServe is whether it knew or had reason to know of the allegedly defamatory Rumorville statements.[210]

Plaintiffs put forward no evidence that CompuServe knew or had reason to know of the statements.

Defendants also alleged that DFA was CompuServe's agent. One essential characteristic of an agent–principal relationship is that the agent's acts are subject to the principal's direction and control.[211] By contrast, an independent contractor, in exercising an independent employment, contracts to perform a task according to the contractor's own methods, without being subject to the employer's control, except as to the product of the assigned task.[212]

An employer can be held vicariously liable for the tort of an independent contractor if the employer directed the act from which the injury resulted or took an affirmative, active part in its commission.[213] CompuServe's contractual right to remove text from its system if the text did not conform with its standards constituted control over, not direction of, CCI's work.[214] This right is insufficient to rise to the level of an agency relationship.

Despite CompuServe's contract contractual responsibilities to provide CCI with training and to indemnify CCI from claims resulting from information appearing in the Journalism Forum,[215] CompuServe did not have sufficient control over CCI and the management of forum to form

---

208. *See id.* (quoting Smith v. California, 361 U.S. 147, 152-53 (1959)).

209. *See* New York Times v. Sullivan, 376 U.S. 254, 277 (1964). While *Smith* involved criminal liability, its principles extend to civil liability. *Id.*

210. *See* Cubby, 776 F. Supp. at 140-41.

211. *See id.* at 142 (quoting In re Shulman Transport Enterprises, Inc., 744 F.2d 293, 295 (2d Cir. 1984)).

212. *See id.* at 142 (quoting Murray Hill Films, Inc., v. Martinair Holland, 1987 WL 14918 (S.D.N.Y. July 17, 1987)).

213. *See id.* at 143; *cf.* Ramos v. State, 34 A.D.2d 1056 (N.Y. App. Div. 1970).

214. *See id.*

215. *See* Cubby, 776 F. Supp. at 143.

an agency relationship. CompuServe had no direct contractual relationship with DFA. Their relationship was at most, that of an employer and an independent contractor.[216]

Cubby left some questions unresolved. The predominant question that OSPs need to know is "What was CompuServe's level of control and was it important?" CompuServe had no more editorial control over such a publication than does a public library, book store, or newsstand,[217] 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.[218]

As a result of *Cubby,* it appears that BBS operators and OSPs can choose their liability by choosing the amount of editorial control that they wish to exercise. However, as explained earlier, they may still be liable for copyright infringement and for violation of laws relating to pornography and obscenity.

The protection given to service providers in *Cubby* does not always attach. *Stratton Oakmont, Inc., v. Prodigy Servs. Co.*[219] illustrates one situation where a service provider was held liable for the acts of its subscribers. An unidentified BBS user made some defamatory remarks about Stratton Oakmont:

> Stratton Oakmont, a securities investment banking firm, and Daniel Porush, Stratton's president, committed criminal and fraudulent acts in connection with the initial public offering of stock of Solomon-Page Ltd.; the Solomon-Page offering was a "major criminal fraud" and "100% criminal fraud"; Porush was "soon to be proven criminal"; and Stratton was a "cult of brokers who either lie for a living or get fired."

A New York state court found that Prodigy could be sued for libel as if it were a newspaper or broadcaster because it exercised editorial control over one of its electronic bulletin boards. In various national newspaper articles written by Geoffrey Moore, Prodigy's Director of Market Programs and Communications, Prodigy held itself out as an online service that exercised editorial control over the content of messages posted on its computer bulletin boards,[220] thereby expressly likening itself to a

---

216. *See id.*

217. *See id.* Computerized database service is one of the modern, technologically interesting, alternative ways the public may obtain up-to-the-minute news and is entitled to the same protection as more established means of news distribution. *Id. See also* Daniel v. Dow Jones & Co., 137 Misc. 2d 94, 102 (N.Y.Civ.Ct. 1987).

218. *See id.* at 140.

219. *See* Stratton Oakmont, Inc., v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y.Misc. LEXIS 229 (N.Y. Sup. Ct. May 26, 1995).

220. *Id.* One such statement was

> We make no apology for pursuing a value system that reflects the culture of the millions of American families we aspire to serve. Certainly no responsible news-

newspaper.[221] Prodigy's hands-on approach to regulating the content of its users' communications opened the company up to liability even though it did not have knowledge of the communication at issue.

Prodigy had lengthy content guidelines. Users were requested to refrain from posting notes that were "insulting" and were advised that "notes that harass other members or are deemed to be in bad taste or grossly repugnant to community standards, or are deemed harmful to maintaining a harmonious online community, will be removed when brought to Prodigy's attention."[222] Prodigy used a software screening program that automatically prescreened bulletin board postings for offensive language.

Prodigy also used BBS leaders to supervise the boards. Board leaders could remove a note and send a previously prepared message giving reasons "ranging from solicitation, bad advice, insulting, wrong topic, off topic, bad taste, etc." Prodigy made decisions as to content, and these decisions constituted editorial control. The court noted that Prodigy's current system could have a chilling effect, but that was what Prodigy wanted; they just did not want the liability attached to it. The choice of material to go into a newspaper and the decisions made as to the content of the paper constitute the exercise of editorial control and judgment.[223] With this editorial control comes increased responsibility.[224]

The issue was whether Prodigy exercised sufficient editorial control over its BBSs to render it a publisher with the same responsibilities as a newspaper. Prodigy claimed that it had changed its policies, but they presented no evidence to support their claim. The court held that Prodigy was a publisher of statements concerning plaintiffs on its "Money Talk" computer bulletin board; and that Charles Epstein, the board leader, acted as Prodigy's agent for the purposes of the acts and omissions alleged.

The standard for determining Prodigy's liability was "one who repeats or otherwise republishes a libel is subject to liability as if he had originally published it."[225] The court acknowledged *Cubby* when it stated that in contrast, distributors such as bookstores and libraries may be liable for defamatory statements of others only if they knew or had reason to know of the defamatory statement at issue.[226] A distributor or

---

paper does less when it chooses the type of advertising it publishes, the letters it prints, the degree of nudity and unsupported gossip its editors tolerate.

Id.

221. *See id.*

222. *See id.*

223. *See* Miami Herald Publishing Co. v. Tornillo, 418 U.S. 241, 258 (1974).

224. *See* Cubby, Inc., v. CompuServe, Inc., 776 F. Supp. 135, 139 (S.D.N.Y. 1991).

225. *See id.* (quoting Cianci v. New Times Pub. Co., 693 F.2d 54, 61).

226. *See id.*

deliverer of defamatory material is considered a passive conduit and will not be found liable in the absence of fault.[227] However, Prodigy was not a passive conduit when it exercised the control equivalent to that of a newspaper editor.

The court noted that the issue addressed in this case "may ultimately be preempted by federal law if the Communications Decency Act of 1995 (now 1996) . . . is enacted." The CDA[228] overruled *Stratton Oakmont*. It protects those who take actions to limit this kind of abuse of the Internet.

Prodigy and Stratton Oakmont eventually settled their dispute. Stratton Oakmont did not to contest Prodigy's motion for reargument after Prodigy apologized for the incident.[229] The court denied Prodigy's request because Prodigy did not offer an acceptable excuse for its failure to include its new proof in the original papers.[230]

Prodigy tried to argue that the court "was given the false impression that Prodigy possesse[d] and exercise[d] significant editorial control and judgment over the content of its bulletin boards."[231] The question still remains how the court would have ruled had Prodigy put forth all of the information in its initial case.

CompuServe did little more than provide access to the Internet. However, Prodigy held itself out to the public as controlling the content of its bulletin boards. Prodigy implemented this control through its automatic software screening program and the guidelines that board leaders were required to enforce. It tried to have its cake and eat it too.

If a BBS adopts the message of one of its users, it can no doubt be held liable. If the BBS does not adopt the message, questions still remain about its liability. If the BBS does not even know about the message, it may still be held liable depending on its policies.

The result from *Stratton Oakmont* imposes a burden of constant surveillance on system operators. Systems operators cannot monitor every message or bit of information. In real time, with billions of bits of information travelling throughout the Internet every minute, this task is absolutely impossible. The cost of removing any illegal information, whether copyrighted, obscene or defamatory, is equally prohibitive.

---

227. *See id.* (quoting Misut v. Mooney, 124 Misc. 2d 95 (dismissing claims against the printer of a weekly newspaper containing allegedly libelous articles because of the absence of fault)).

228. *See supra* Part III.B.

229. *See Judge Refuses to Vacate Prodigy Libel Ruling*, NAT'L L.J., Jan. 1, 1996, at B2.

230. *See* Stratton Oakmont, Inc., v. Prodigy, 1995 WL 805178 (N.Y.Sup. Dec. 11, 1995).

231. *See id.* at *2.

C. THE CDA RIDES AGAIN

The ramifications of the CDA extend beyond illegal pornography. It has been applied to the area of defamation as well.

The CDA supposedly restored the incentive for OSPs to prevent the abuse of the Internet.[232] A private service can now choose to police its network without the liability that ensued in *Stratton Oakmont.* The statute was passed in part to overrule *Stratton Oakmont v. Prodigy.*[233] The conferees believed that such decisions create serious obstacles to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services.[234] The courts have been left with no alternative but to apply the CDA, even when they did not believe that the law was just in the situation.

In *Zeran v. America Online, Inc.*,[235] the Fourth Circuit held that section 230 of the CDA "plainly immunizes computer service providers like AOL from liability for information that originates with third parties."[236]

On April 25, 1995, an unidentified person posted a message on an AOL bulletin board advertising shirts featuring tasteless slogans related to the April 16, 1995, bombing the Alfred P. Murrah Federal Building in Oklahoma City. Those interested in purchasing the shirts were instructed to call "Ken" at Zeran's home phone number. Zeran received a high volume of angry and derogatory calls and death threats. Zeran ran his business out of his home and therefore could not change his phone number without harming his business. Zeran called AOL the same day and was assured by a representative that the posting would be removed. The employee also explained that as a matter of policy, AOL does not post retractions.

Over the next five days, the same thing happened with new, more offensive slogans and new products. When a local radio announcer received a copy of the posting, he related the message's contents on the air

---

232. *See* 47 U.S.C. § 230(b). Among the policies of the United States in enacting this law are:

> to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services,
>
> to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material, and
>
> to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

Id.

233. *See* H.R. CONF. REP. No. 104-158, at 194 (1996).

234. *See* Blumenthal v. Drudge, 992 F. Supp. 44, 52 n.13 (D.D.C. 1998).

235. *See* Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997).

236. *See id.* at 328.

and urged people to call Zeran. Zeran spoke to the police and to representatives of the radio station and AOL. Over two and a half weeks after the original posting, an Oklahoma City newspaper exposed the advertisements as a hoax and the radio announcer made an on-air apology.

Zeran filed suit against the radio station in January 1996 and against AOL in May 1996. In his suit against AOL, Zeran argued that AOL unreasonably delayed in removing defamatory messages posted by a third party, refused to post retractions of those messages and failed to screen for similar postings thereafter. The AOL case was transferred to the Eastern District of Virginia, where AOL successfully pled 47 U.S.C. § 230 as a defense. Zeran appealed.

The court looked to the plain language of the statute and Congress's stated intent in drafting it. Section 230[237] states:

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

The court stated that "[b]y its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service."[238] Furthermore, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content—are also barred.[239]

The court went on to note that "Congress recognized the Internet and interactive computer services as offering a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity."[240] Congress wanted to keep governmental regulation to a minimum and to preserve the free market that existed for the Internet and other interactive computer services.[241]

Imposing tort liability in an area with so much potential to enable speech would have an unacceptable chilling effect.[242] The *Stratton Oakmont* decision was just the type of the tort liability to which the court referred. Congress enacted § 230 to remove the disincentives to self-regulation created by that decision. Congress enacted § 230's broad immunity "to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material."[243]

---

237. *See* 47 U.S.C. § 230(c)(1).
238. *See Zeran*, 129 F.3d at 330.
239. *See id.*
240. *See id.* (quoting 47 U.S.C. § 230(a)(3)).
241. *See Zeran*, 129 F.3d at 330 (quoting 47 U.S.C. § 230(b)(2)).
242. *See id.* at 331.
243. *See* 47 U.S.C. § 230(b)(4).

Zeran tried to draw a distinction between publisher liability, which is barred by § 230, and distributor liability. However, the court did not agree, stating that "every one who takes part in the publication is charged with publication" for the purposes of defamation law.[244] There are different standards of liability that may be applied within the larger publisher category, depending on the specific type of publisher concerned.[245] In fact, once a service provider receives notice of a potentially defamatory posting, it is "thrust into the role of a traditional publisher" deciding then whether to publish, edit, or withdraw that posting.[246]

Zeran then argued that interpreting § 230 to impose liability on service providers with knowledge of defamatory content on their services is consistent with the statutory purposes outlined in Part IIA of the CDA. This argument is contrary to the plain language of the statute. The court decided that "[l]iability upon notice would defeat the dual purposes advanced by § 230 of the CDA. It would reinforce service providers' incentives to restrict speech and abstain from self-regulation.[247] Notice-based liability would also deter service providers from regulating the dissemination of offensive material over their own services.[248] Because the probable effects of distributor liability on the vigor of Internet speech and on service provider self-regulation were directly contrary to the purposes of § 230, the court decided not to assume that Congress intended to leave liability upon notice intact.[249]

It is important to note that this law only bars claims against the service provider. The original culpable party can still be held liable.

Although this law by its plain language protects service providers from liability for acts with which it had nothing to do, it also protects them from liability for acts that they facilitate. This is an unfortunate side effect of a law that was drafted more broadly than it needed to be to achieve its intended purpose.

Section 230 is clearly not needed to protect a service provider that has not violated any laws and has no knowledge of wrongdoing by its users. Some state courts have reached this conclusion without resorting to § 230, which proves that the purposes of the CDA can be achieved

244. *See Zeran*, 129 F.3d at 332 (quoting W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 113 (5th ed. 1984)).

245. *See Zeran*, 129 F.3d at 332. The court was explaining the differences in the outcomes of *Stratton Oakmont v. Prodigy* and *Cubby v. CompuServe*. *Id.* The Fourth Circuit stated that these cases merely illustrated the different standards of liability for publishers and distributors within the context of publisher liability. *Id.* These cases did not, according to the Court, create two different standards of liability based on the role—publisher or distributor. *Id. Cf.* KEETON ET AL., *supra* note 244, § 113.

246. *See Zeran*, 129 F.3d at 332.

247. *See id.* at 333.

248. *See id.*

249. *See id.*

without § 230 and that the section may be overbroad. In *Lunney v. Prodigy*,[250] an unknown impostor opened a number of accounts with Prodigy Services Company in the name of Lunney, a teenage Boy Scout. The impostor posted two vulgar messages in Lunney's name on a Prodigy bulletin board and sent a threatening, profane e-mail message to a local scoutmaster who in turn notified the police and Lunney's scoutmaster. After an investigation, the police and his scoutmaster readily accepted Lunney's innocence.

Prodigy notified Lunney that it was terminating one of the accounts in his name "due to the transmission of obscene, abusive, threatening, and sexually explicit material through the Prodigy service and providing inaccurate profile information." Lunney advised Prodigy about the impostor and Prodigy apologized. Prodigy later informed Lunney that it had uncovered and closed four more accounts in his name all within two days after they were opened.

Lunney sued Prodigy, claiming that as a result of Prodigy's dereliction in allowing these accounts to be opened in his name, he had been stigmatized and defamed. The trial court denied Prodigy's motion for summary judgment and the appellate division reversed, holding that the messages did not defame Lunney and that Prodigy was not the publisher. Lunney appealed to the state's highest court.

Although there was some debate over whether Lunney had been defamed, the court assumed that he had been and moved on to the issue of liability. The court stated that Prodigy's role in transmitting e-mail is akin to that of a telephone company, which one neither wants nor expects to superintend the content of its subscribers' conversations.[251] That is, a service provider is merely a conduit. Prodigy was not a publisher of the e-mail transmitted through its system by a third party.[252]

Prodigy argued that while it reserved the right to screen its bulletin board messages, it was not required to, did not normally do so and could not be a publisher of bulletin board messages posted on its system by third parties. Even if Prodigy exercised the power to exclude certain vulgarities from the text of certain bulletin board messages, this would not alter its passive character in the millions of other messages in whose transmission it did not participate,[253] nor would this compel it to guarantee the content of those myriad messages.[254]

The court did not believe that the facts warranted a finding of negligence. To do so, the court argued, would "open an ISP to liability for the

250. *See* Lunney v. Prodigy, 723 N.E.2d 539 (N.Y. 1999)

251. *See id.*

252. *See id.*

253. *See id.* (quoting Lunney v. Prodigy, 683 N.Y.S.2d 557, 562 (N.Y. App. Div. 1998).

254. *See id.*

wrongful acts of countless potential tortfeasors committed against countless potential victims.[255]

The court declined to apply or even rule on the applicability of § 230 of the CDA, believing that the case did not call for it. The court further believed that deciding on issues beyond those necessary to decide the case at hand is "an ambition of that sort would entail something very much like drafting advisory opinions. Misdirected or misapplied, they can create the very kind of uncertainty, or confusion, that purposeful decisional law seeks to eliminate."[256]

This case leaves open a number of questions on ISP liability. Prodigy made the same arguments that it did in *Stratton Oakmont*. This time, the court reached a more logical result. The main difference is that the court did not reach the illogical conclusion that Prodigy should be held to an impossible standard of care that no individual or company could possibly meet. The irony is that this court reached its conclusion without resorting to 47 U.S.C. § 230, the law that was designed to create this conclusion. Maybe all Congress really needed to do was wait for a court to overturn *Stratton Oakmont*.

While some courts reach an appropriate decision without resorting to § 230, others reach a poor decision because of it. In *Blumenthal v. Drudge*,[257] the United States District Court for the District of Columbia felt compelled the use § 230 to immunize a service provider from liability for an act in which it participated but did not originate.

Matt Drudge, a gossip columnist, created, edited, updated and managed the content of the "Drudge Report." AOL signed an agreement with Drudge to make the Drudge Report available to all of its members for one year in exchange for a monthly royalty of $3,000.[258] After he completed a new edition of the report, Drudge would e-mail it to AOL, who then posted it on its service. AOL reserved the right to "remove content that AOL reasonably determine[d] to violate AOL's then standard terms of service."[259]

One edition of the report accused Sidney Blumenthal (then assistant to the President) of wife beating. Blumenthal and his wife, Jacqueline Jordan Blumenthal, Director of the President's Commission on White House Fellowships, brought a defamation suit against Drudge and AOL.

After receiving a letter from Blumenthal's attorney, Drudge retracted the story. When Drudge e-mailed the retraction to AOL, AOL

255. *See id.*

256. *See* Lunney v. Prodigy, 723 N.E.2d 242 (N.Y. 1999)

257. *See* Blumenthal v. Drudge, 992 F. Supp. 44 (D.D.C. 1998).

258. *See id.* at 47.

259. *See id.*

removed the report from its electronic archive, thus disabling access to the story on its network.

The court held that AOL was nothing more than a provider of an interactive computer service on which the Drudge Report was carried. Because Congress said clearly that such a provider shall not be treated as a "publisher or speaker," AOL could not be held liable in tort.[260]

The district court was not pleased to reach this result. In fact, as Judge Paul Friedman wrote, "[i]f it were writing on a clean slate, this Court would agree with plaintiffs."[261] It believed that AOL had taken advantage of all of the benefits of the CDA without accepting any of the burdens that Congress intended (e.g., self-policing). Nevertheless, Congress had spoken, and the CDA barred liability. Congress decided to effectively immunize service providers from tort liability for material that they disseminated but that was created by others.[262] AOL promoted the Drudge Report and retained the right to require changes in content and to remove the content. It took no responsibility for any damages that Drudge may cause. The CDA immunity bars liability even under these circumstances. This result makes no sense.

The stated purposes of the protection provision of the CDA are as follows:

> to promote the continued development of the Internet and other interactive computer services and other interactive media;
>
> to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
>
> to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services;
>
> to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material; and
>
> to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.[263]

Congress could have achieved these purposes using other means. The Internet was already thriving and growing despite the liability that may exist for those who wished to connect others to it. Companies created software for blocking and filtering objectionable sites even with the liability that they might face. With the reality of the growth of the In-

260. *See id.* at 50 (quoting 47 U.S.C. § 230(c)(1)).
261. *See id.* at 51.
262. *See id.* at 49.
263. *See* 47 U.S.C. §§ 230(b)(1)-(5).

ternet in mind, there appeared to be no need for this blanket immunity from liability.

This statute was designed to overrule the decision in *Stratton Oakmont*. What Congress failed to understand is that the *Stratton Oakmont* decision was an aberration, a poor decision of one court that could not stand. In *Stratton Oakmont*, the court tried to hold a service provider liable for the defamation committed by a subscriber solely because it reserved a right that it could never realistically exercise, the right to review and edit every statement posted on its service. The court in that case failed to realize the impossibility of this right.

Instead, Congress passed a law that, by its own terms, immunizes a service provider from any liability for an act committed by its subscribers. According to the purposes, Congress was only trying to encourage service providers to take the initiative to protect children from pornography. It did much more; it undermined defamation law and enabled service providers to escape liability even when they solicit the illegal material and actively engage in distributing it.

Subscribers can distribute copyright infringing, obscene and defamatory material without the service provider's knowledge. In these cases, the service provider should be protected from liability. OCILLA protects service providers unless they receive notice of the infringing material and do nothing. The CDA provision protects service providers if they receive notice and do nothing and even if they actively solicit and distribute the material. The standard of liability before the CDA would hold service providers liable when they actively participated in the illegal acts. This result is the correct result, not that which the CDA requires.

V. INTERNATIONAL DIMENSIONS

Actions against service providers are not solely a product of the United States. In fact, because of the global nature of the Internet, service providers may face liability in other countries where they do business if the harm is felt in that country. Therefore, it is important to look at events taking place around the world.

Complaints by German prosecutors prompted an OSP to cut off subscriber access to over 200 newsgroups with the words "sex," "gay" or "erotica" in the name.[264] They censored such groups as "clarinet. news.gay," which is an online newspaper focused on gay issues, and "gaynet.coming-out", which is a support group for gay men and women dealing with going public with their sexual orientation. German prosecutors

264. *See Statement of Senator Leahy on Repealing the Communications Decency Act*, Government Press Releases, Feb. 9, 1996, *available at* 1996 WL 8783190.

have also tried to get AOL to stop providing access to neo-Nazi propaganda.[265]

A German court held AOL liable for failing to prevent distribution of pirated music on its Web site.[266] Hit Box Software sued AOL Germany after discovering that its digital music files were being swapped on some of AOL's music forums.[267] The court said that AOL Germany should have been aware of possible copyright problems because of its system of volunteers who monitor the service.[268] AOL will appeal. In the United States, this issue arose in the case of *Stratton Oakmont v. Prodigy*; it took an act of Congress to overturn that law. In Germany, many believe that the verdict will be overturned.

In a prior case, the former head of CompuServe Germany was convicted for failing to block child pornography on its sites.[269] This widely criticized case was overturned. In that, like the case currently before the German courts, the service provider had no knowledge of the material on its service, nor did it have reason to know.

The United Kingdom passed The Defamation Act of 1996, a bill to protect OSPs against defamatory messages sent by users. The law provides a defense for ISPs as long as they are not primarily responsible for a defamatory statement, have taken reasonable care and do not know or have reason to suspect that their acts contributed to the publication of the libel.[270]

This law only protects service providers that have no knowledge of the defamatory statements. In *Godfrey v. Demon Internet Ltd.*,[271] an unknown person posted an obscene message to a newsgroup and falsely attributed it to Laurence Godfrey. After accessing the message through Demon's server, Godfrey notified Demon of the forged message and requested that they remove it. When Demon did not do so, Godfrey filed a libel suit against them. The High Court ruled that Demon could be sued for posting the allegedly libelous content from a third party because they knew of the posting and chose not to remove it. Demon initially challenged the ruling but settled at the last minute prior to trial to avoid a

265. *See id.*

266. *See* John T. Aquino, *German Court Holds America Online Responsible for Music Piracy*, E-COMMERCE LAW WEEKLY (Apr. 24, 2000) <http://www.lawnewsnetwork.com>.

267. *See id.*

268. *See id.*

269. *See id.*

270. *See* Frances Gibb, *Menace of Internet Libel Prompts New Defamation Bill*, TIMES (London), July 3, 1995, *available at* 1995 WL 7679866.

271. *See* Godfrey v. Demon Internet Ltd., 4 All E.R. 342 (1999). *See also* John T. Aquino, *British Court Concludes ISPs Liable for Bulletin Board Postings*, E-COMMERCE LAW WEEKLY (Apr. 7, 2000) <http://www.lawnewsnetwork.com/stories/A20742-2000Apr6.html>.

final ruling by the Court.[272]

This settlement now creates a problem for all service providers who "do business in" the United Kingdom. If an individual claims to have been defamed, the service provider must make the legal determination of whether the claim is accurate. An incorrect decision can result in liability, a legal problem, or censorship, a potential business problem with loss of profit margin. Even if the courts or the legislature in the United States refuse to enforce the judgment from the U.K. courts, companies that have assets in Europe will still be affected if this decision stands.

In the wake of the *Godfrey* decision, Outcast, a magazine for the gay community, asked the European Court of Human Rights to rule that British laws violate the right of freedom of expression on the Internet.[273] Outcast's ISP, Netbenefit, closed the site after a British newspaper for the gay community, Pink Paper, threatened to sue Netbenefit over content that was scheduled to appear on Outcast's Web site.[274] The Internet Service Providers' Association has asked the British government for an urgent review of the law to protect ISPs. The position of the European Convention on Human Rights has been to recognize the right to freedom of expression with exceptions to safeguard morality and copyright.[275] With both entities reviewing this law, it is only a matter of time before Europe enacts the type of protection that exists in the United States. Hopefully, they will make service providers liable for defamation when they solicit and distribute the defamatory material, unlike the outcome in the *Drudge* case.

In Australia, it is still unclear who is liable.[276] To protect themselves, service providers can now buy insurance. The Internet Industry Association is offering the "CyberLiability Plus" policy, which offers coverage for domestic and international liability for infringement of intellectual property rights, negligent acts, unauthorized access, data tampering, defamation and other causes of action.[277] This type of insurance may eventually become available in the United States, but it may be unnecessary, given the blanket immunity from liability afforded by 47 U.S.C. § 230.

---

272. *See id.*

273. *See British ISPs Close Web Sites in Wake of Defamation Settlement*, E-COMMERCE LAW WEEKLY (Apr. 24, 2000) <http://www.lawnewsnetwork.com>.

274. *See id.*

275. *See id.*

276. *See Australian Business Community Questions Who's Liable on the Internet?* COMPUTER AUDIT UPDATE, Dec. 1, 1995, *available at* 1995 WL 8322602.

277. *See* Adam Creed, *Australian Internet Industry Offered Cyber Insurance*, NEWSBYTES (Nov. 10, 1999) <http://www.newsbytes.com>.

VI. CONCLUSION

The Internet affects our everyday lives in numerous ways. It controls the flow of information for our bank accounts, our bills, and our businesses. Private persons access a piece of the Internet for simple tasks such as using an automated teller machine, using e-mail, or accessing their medical records at a pharmacy.

Most of us are not fortunate (or wealthy) enough to have our own access to the Internet, so we must use commercial sources (CompuServe, Prodigy, America Online, and thousands of ISPs and BBSs) for access. While these companies understand that there are risks involved, as with any venture, they need to understand what those risks are.

The courts and the legislature (state and federal; U.S. and foreign) do not agree on what that liability should be. If service providers know the potential risks, they can charge accordingly. However, if they do not know the extent of the risks, they may charge too little and end up taking a disproportionate share of the risk. The result may be fewer sources of access to the Internet and less competition. Considering that many BBSs are run by private persons as a part-time hobby, we may be left with only large corporations charging prohibitively high prices. Fewer means of access and higher costs will cripple this medium and the free flow of information that it promotes.

Before the courts and the legislature spoke, the issue of liability was left to the speculation of scholars who frequently disagreed. Now that they have spoken, the issue of liability is still confused. Only time will tell what the liability of online service providers will be for acts committed by subscribers. Until then, systems operators will have to be cautious. Ironically, this caution may cause the same chilling effect that the courts and the legislature have been trying to prevent.

ISPs have an added layer of issues that other industries do not face. Geographical boundaries do not exist. While other industries can limit the jurisdictions in which they do business, ISPs cannot. Anyone can access information on the Internet from anywhere in the world. Potentially, ISPs must know and follow the laws of every jurisdiction in the world. Without uniformity, this requirement can be devastating. Which approach, if any, the nations of the world will follow is only a matter of speculation. Until then, service providers need all the information they can get.