

HEINONLINE

Citation: 60 Vand. L. Rev. 905 2007



Content downloaded/printed from
HeinOnline (<http://heinonline.org>)
Sat Nov 14 21:11:54 2015

- Your use of this HeinOnline PDF indicates your acceptance of HeinOnline's Terms and Conditions of the license agreement available at <http://heinonline.org/HOL/License>
- The search text of this PDF is generated from uncorrected OCR text.
- To obtain permission to use this article beyond the scope of your HeinOnline license, please use:

[https://www.copyright.com/ccc/basicSearch.do?
&operation=go&searchType=0
&lastSearch=simple&all=on&titleOrStdNo=0042-2533](https://www.copyright.com/ccc/basicSearch.do?&operation=go&searchType=0&lastSearch=simple&all=on&titleOrStdNo=0042-2533)

NOTES

Containing Online Copyright Infringement: Use of the Digital Millennium Copyright Act's Foreign Site Provision to Block U.S. Access to Infringing Foreign Websites

I.	INTRODUCTION	906
II.	TITLE II OF THE DIGITAL MILLENNIUM COPYRIGHT ACT.....	909
III.	INTERPRETATION OF § 512(J)(1)(B)(II)	911
	A. <i>Textual Analysis of § 512(j)(1)(B)(ii)</i>	913
	1. What Constitutes an Internet Service Provider?	913
	2. Whose Internet Access Is to Be Restrained?	914
	3. What Constitutes Reasonable Steps to Block Access?	916
	4. How Do Courts Determine that the Online Location Is Outside of the United States?	916
	B. <i>Examination of the Considerations of § 512(j)(2)</i>	917
	1. Significance of the Burden of the ISP	917
	2. Magnitude of the Harm Likely to Be Suffered by the Copyright Owner	919
	3. Technical Feasibility and Effectiveness.....	921
	a. <i>IP Filtering</i>	923
	b. <i>URL Filtering</i>	924
	c. <i>DNS Filtering</i>	924
	4. Availability of Less Burdensome and Comparably Effective Means	925
IV.	MISGUIDED ARGUMENTS AGAINST THE USE OF THE PROVISION	927

A.	<i>Use of the Provision Does Not Violate the First Amendment</i>	927
B.	<i>Use of This Provision Will Not Have a "Chilling Effect" on Technology</i>	929
V.	APPLICATION OF § 512(J)(1)(B)(II)	930
A.	<i>How Copyright Holders Should Use § 512(j)(1)(B)(ii)</i>	931
B.	<i>Which Sites Copyright Holders May Block with § 512(j)(1)(B)(ii)</i>	933
VI.	CONCLUSION	936

I. INTRODUCTION

On June 27, 2005, the Supreme Court decided *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.* and dealt another blow to online copyright infringement.¹ From the early days of electronic bulletin boards to today's world of decentralized peer-to-peer services, the Internet has been used to infringe copyrights.² As infringement has increased, copyright holders have successfully fought to protect their works through the courts, seeking judgments against not only the primary infringers (the individuals who have illegally downloaded these works), but also the service providers who make these works available. Judgments extending secondary liability to these Internet services have protected copyrights and forced services to adapt to a changing legal landscape either by changing their technology or, more recently, by moving overseas and out of the reach of U.S. courts.

The original model for a copyright infringing service was Napster. Through Napster, users were able to search for the files of other users through a directory located on Napster's servers.³ If a match was found, Napster supplied the requesting user with the address of the computer containing the file, from which the requesting user was then able to download the file.⁴ As such, Napster had a central server, containing the names of the files available on its system. The plaintiffs in *A & M Records, Inc. v. Napster, Inc.* used

1. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005).

2. *See id.* at 922 (discussing decentralized peer-to-peer service offering many forms of copyrighted works); *Religious Tech. Ctr. v. Netcom On-Line Comm'n Servs., Inc.*, 923 F. Supp. 1231, 1250 (N.D. Cal. 1995); *Sega Enters., Ltd. v. MAPHIA*, 857 F. Supp. 679, 686 (N.D. Cal. 1994) (discussing a bulletin board posting of video games); *Playboy Enters., Inc. v. Frena*, 839 F. Supp. 1552, 1556 (M.D. Fla. 1993) (discussing a bulletin board posting of photographs).

3. *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1012 (9th Cir. 2001).

4. *Id.*

evidence of this central server to show that Napster had actual knowledge of the infringing files on its system and the right and ability to supervise the infringing activity.⁵ After the plaintiffs had demonstrated a likelihood of success on the merits of both contributory and vicarious liability claims, the Ninth Circuit upheld a preliminary injunction against Napster.⁶ The ruling eventually resulted in Napster's closure and the emergence of new file-sharing services.⁷

The Ninth Circuit's holding in *Napster* indicated to other services that courts would not hesitate to apply secondary liability to file-sharing services. As a result, services adopted new technologies in an effort to avoid Napster's fate. What had hurt Napster so greatly was its centralized server. When the company owns and operates a server, it is difficult to argue that it does not know what occurs on that server or that it has no control over what occurs on it. New services therefore opted for decentralized systems. Most notable of this new crop of file-sharing services was Grokster.

Once a user downloaded and installed the Grokster software, he could request and download files directly from other users, thereby avoiding the need for a central server.⁸ As such, in subsequent lawsuits, Grokster argued against the imposition of vicarious liability because it had no control over its system.⁹ Further, Grokster argued that the Court's ruling in *Sony Corp. of America v. Universal City Studios, Inc.*,¹⁰ coupled with the available non-infringing uses of its system,¹¹ prevented the imposition of contributory liability. In deciding *Grokster*, the Supreme Court did not reach either the issue of contributory or vicarious liability, but instead focused on the inducement of copyright infringement.¹² The Court held "that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps

5. *Id.* at 1020-22.

6. *Id.* at 1022-24.

7. *Online Music: Calling the Tune*, *ECONOMIST*, Oct. 8, 2005, at 75.

8. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 921 (2005).

9. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp. 2d 1029, 1045 (C.D. Cal. 2003) ("[Grokster] argue[s] principally that [it] do[es] not have the ability to control the infringement Because they have no ability to supervise or control the file-sharing networks, or to restrict access to them, [Grokster] maintain[s] that [it] cannot police what is being traded as Napster could.").

10. *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984) ("[T]he sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses.").

11. Such uses included access to the works of Shakespeare and the briefs to the case. *Grokster*, 545 U.S. at 923.

12. *Id.* at 931 n.9.

taken to foster infringement, is liable for the resulting acts of infringement of third parties.”¹³

Following *Grokster*, file-sharing services may now be subject to contributory liability, vicarious liability, or liability for inducing infringement. As a result, it has become quite difficult to operate a copyright infringing file-sharing service in the United States without the risk of some form of liability. Rather than finding new ways to avoid liability in the United States, sites are springing up in foreign countries.¹⁴ Operating in foreign locales keeps services out of the reach of U.S. courts and subjects them to foreign laws and courts which may be more sympathetic to their activities.¹⁵

While direct action against a foreign site is not possible in U.S. courts, the Digital Millennium Copyright Act (“DMCA”) allows courts to order the blocking of infringing sites. Section 512(j)(1)(B)(ii) (the “Foreign Site Provision”) permits an order to restrain an Internet service provider (“ISP”) from providing access to a “specific, identified, online location outside the United States.” Therefore this provision, with some limitations, may be used to block U.S. access to infringing foreign sites. While the Foreign Site Provision does not shut down the site altogether, it effectively does so for those in the United States. Although it is unclear whether decentralized peer-to-peer services are subject to this provision, as they do not necessarily consist of a “specific, identified, online location outside the United States,” the sites on which the peer-to-peer software is offered for downloading could be blocked. Further, foreign services that illegally offer copyrighted music could be blocked.¹⁶ Although the Foreign Site

13. *Id.* at 918.

14. For instance, piracy sites are seen in Russia, China, Taiwan, and Korea, among other countries. *Governments Said to Lack Political Will to Address Piracy*, CONSUMER ELECTRONICS DAILY, June 24, 2005, at 15.

15. Sam Yagan, President of MetaMachine (developer and distributor of the peer-to-peer program eDonkey), testified before the Senate Committee on the Judiciary that “individuals, basic researchers, hobbyists, and hackers . . . will continue to explore [peer-to-peer] technological advances, although probably not publicly in the United States for fear of ruinous litigation prosecuted by the entertainment industry.” *Protecting Copyright and Innovation in a Post-Grokster World: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 33 (2005); see *Russian DA Clears AllOfMP3.com of Copyright Infringement Charges*, ONLINE REPORTER, Mar. 12, 2005, http://www.onlinereporter.com/article.php?article_id=1021 (indicating that foreign courts and copyright law may make it difficult to shut down foreign sites).

16. For instance, AllOfMP3.com is a Russian site where users can purchase music that the service does not have a right to distribute. *Ensuring Protection of Intellectual Property Rights of American Goods and Services in China: Before the Subcomm. on Fed. Financial Mgmt, Gov’t Info. and Int’l Sec. of the S. Comm. on Homeland Sec. and Gov’t Affairs*, 109th Cong. 4-5 (2005) (statement of Gary Burr, Songwriter, on behalf of himself and the Recording Industry Association of America). It is not a peer-to-peer site and thus has a “specific, identified, online location outside the United States,” and would be subject to 17 U.S.C. § 512(j)(1)(B)(ii) (2005).

Provision will not stop foreign infringing sites and foreign peer-to-peer services, it will make it more difficult to access these services, thereby making them less profitable and less enticing to both would-be creators and would-be users. A judgment against just a handful of ISP subscribers could be used to block access for the millions of other people using these service providers.

As infringing sites continue to emerge in foreign countries, the Foreign Site Provision will become more important for copyright holders. For this reason, this Note will take an in-depth look at the Foreign Site Provision. As the Foreign Site Provision was written as part of Title II of the Digital Millennium Copyright Act, Part II will explain why the Title was created and its content. Through textual analysis of the Foreign Site Provision and examination of the application of § 512(j)(2), Part III will indicate how courts should interpret the Foreign Site Provision. Arguments that the provision conflicts with the First Amendment and with technological innovation will be rebutted in Part IV. Part V will explain how a copyright holder should best use the Foreign Site Provision to protect his works.

II. TITLE II OF THE DIGITAL MILLENNIUM COPYRIGHT ACT

By 1998, Congress recognized that the uncertainty of liability on the Internet would damage content providers and service providers, stating in a Senate Report, “Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy.”¹⁷ The Senate Report also stated,

At the same time, without clarification of their liability, service providers may hesitate to . . . [invest] in the expansion of the speed and capacity of the Internet. In the ordinary course of their operations service providers must engage in all kinds of acts that expose them to potential copyright infringement liability.¹⁸

To define liability on the Internet, Congress passed Title II of the Digital Millennium Copyright Act of 1998, which limited “copyright infringement liability of on-line and Internet service providers under certain circumstances.”¹⁹ Its goal was to “preserve[] strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place [on the Internet and] . . . provide[] greater certainty to service

17. S. REP. NO. 105-190, at 8 (1998) (Conf. Rep.).

18. *Id.*

19. *Id.*

providers concerning their legal exposure for infringements that may occur in the course of their activities.”²⁰ Most importantly, Title II provides safe harbors that shield qualifying service providers from copyright infringement liability.²¹

Except as provided in § 512(j), the safe harbor provisions of the DMCA protect service providers from liability for monetary, injunctive, or other equitable relief.²² Section 512(a) shields a service provider from liability for “transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider.” Section 512(b) protects a service provider from liability “by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider.” Section 512(c) prevents service provider liability where a user stores infringing material on the service provider’s system or network. Under § 512(d) a service provider is not liable for infringement by referring or linking users to an online location containing infringing material or infringing activity.

Simply performing a function listed in § 512(a)-(d) does not shield a service provider from liability. The DMCA’s safe harbor provisions apply only if a service provider “has adopted and reasonably implemented . . . a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider’s system or network who are repeat infringers.”²³ Additionally, each of the four safe harbors has specific requirements that must be met for the ISP to receive protection from liability.²⁴

20. H.R. REP. NO. 105-551, pt. 2, at 49-50 (1998) (Conf. Rep.).

21. 17 U.S.C. § 512(a)-(d).

22. *Id.* § 512(j) permits injunctions in some cases.

23. § 512(i)(1)(A). The provision further requires that the service provider inform its subscribers of this policy. *Id.*

24. Section 512(a) is the safe harbor provision that specifies who may initiate the transmission, how the transmitted material must be sent, and how copies of the material may be stored on the service provider’s system.

Section 512(b) limits protection according to how the stored material is made available online, how the material is transmitted to subsequent users, whether the service provider complies with industry standard communication protocols, and whether the service provider has removed or disabled access to infringing material.

Section 512(c) requires that a service provider not have actual knowledge of infringement, nor receive a direct financial benefit from the infringing activity while having the right and ability to control that activity. § 512(c)(1)(A)(i), (c)(1)(B). If the service provider knows of infringement, he must quickly act to remove the infringing material. § 512(c)(1)(A)(iii), (c)(1)(C). Additionally, it requires that the service provider designate an agent to receive notification of claimed infringement and provide contact information for the agent. § 512(c)(2). Finally, § 512(c)(3) specifies what is required for effective notification of copyright infringement.

Section 512(d)’s safe harbor requires that the service provider either not have actual knowledge of the infringement or that it remove or disable access to the material upon

Thus, while the safe harbors exist, they do not completely immunize service providers from liability. Regardless of which safe harbor a service provider falls into, it may still be enjoined through the use of § 512(j).²⁵ Section 512(j)(1)(B)(i) (the “Individual User Provision”) permits a court to enjoin a service provider from “providing access to a subscriber . . . who is using the provider’s service to engage in infringing activity . . . by terminating the account[. . . .]” Although the Individual User Provision would keep a direct infringer from continuing his activities through his current service provider, this does little to stop the wide-spread infringement occurring on the Internet. While the Individual User Provision focuses on the Internet user who is directly infringing, the Foreign Site Provision focuses on the site that makes infringement possible. As a result, successful application of the Foreign Site Provision can greatly diminish copyright infringement and is one of the best options for copyright holders to protect their works from online piracy.

III. INTERPRETATION OF § 512(J)(1)(B)(II)

The DMCA allows the blocking of infringing foreign services through the Foreign Site Provision,²⁶ but before applying the many

notification. § 512(d)(1)(A), (d)(1)(C), (d)(3). If the service provider receives a direct financial benefit from the infringing activity, it must not have the right and ability to control the infringing activity. § 512(c)(2).

25. In fact, § 512(j)(1)(A) permits a court to grant an injunction “with respect to conduct other than that which qualifies for the limitation on remedies set forth in (17 U.S.C. § 512(a)).”

26. Injunctions under the DMCA are found in § 512(j), as reproduced below:

(j) Injunctions.—The following rules shall apply in the case of any application for an injunction under section 502 against a service provider that is not subject to monetary remedies under this section:

(1) Scope of relief.—

(A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms:

(i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider’s system or network.

(ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider’s system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.

elements specifically required by the provision, there must be a determination that infringement has occurred.²⁷ Under § 501, “[a]nyone who violates any of the exclusive rights of the copyright owner . . . is an infringer of the copyright or right of the author.”²⁸ In the Internet context, such infringement is most often seen through the unauthorized reproduction and/or distribution of a copyrighted work, which is typically music.²⁹

(B) If the service provider qualifies for the limitation on remedies described in subsection (a), the court may only grant injunctive relief in one or both of the following forms:

(i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.

(2) Considerations.—The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider—

(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;

(B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;

(C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and

(D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.

(3) Notice and ex parte orders.—Injunctive relief under this subsection shall be available only after

notice to the service provider and an opportunity for the service provider to appear are provided, except

for orders ensuring the preservation of evidence or other orders having no material adverse effect on the

operation of the service provider's communications network.

§ 512(j).

27. Section 512(j)(1)(B)(ii) is part of Chapter 5 of the Copyright Act and is entitled, “Copyright Infringement and Remedies.”

28. 17 U.S.C. § 501 (2005) (stating that the applicable exclusive rights are listed in §§ 106-22). With some limitations, a copyright owner has the exclusive right to reproduce his work, prepare derivative works, distribute copies, perform the work publicly, display the work publicly, and perform the work publicly by means of a digital audio transmission. 17 U.S.C. § 106 (2002).

29. Such acts violate § 106(1) and § 106(3) respectively. Online infringement has also been seen with other copyrighted works. *See* cases cited *supra* note 2.

Having determined that infringement has occurred, one may apply the Foreign Site Provision, which permits “[a]n order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.”³⁰ For a copyright holder to use the Foreign Site Provision to protect his works from infringement, several elements must be satisfied. There must be: (1) direct infringement, (2) a service provider, (3) who may block access, (4) through reasonable steps, and (5) the site or service in question must be located outside of the United States.³¹

Additionally, § 512(j)(2) requires that the court make several considerations. The court must consider the significance of the burden an injunction would impose on the service provider³² and the magnitude of harm to the copyright owner if the service provider is not enjoined.³³ Furthermore, the court must contemplate whether an “injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations.”³⁴ The availability of less burdensome and comparably effective means of preventing access to the material must also be evaluated.³⁵ As a result, an understanding of the applicability of the Foreign Site Provision requires textual analysis of the provision itself, as well as examination of § 512(j)(2).

A. Textual Analysis of § 512(j)(1)(B)(ii)

1. What Constitutes an Internet Service Provider?

The DMCA 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.”³⁶ Courts have defined this broadly to encompass newsgroups,³⁷ search engines,³⁸ online auction sites,³⁹ peer-

30. 17 U.S.C. § 502(j)(1)(B)(ii) (2005).

31. *Id.*

32. *Id.* § 502(j)(2)(A).

33. *Id.* § 502(j)(2)(B).

34. *Id.* § 502(j)(2)(C).

35. *Id.* § 502(j)(2)(D).

36. 17 U.S.C. § 512(k)(1)(A) (2005).

37. *ALS Scan, Inc. v. RemarQ Cmtys., Inc.*, 239 F.3d 619 (4th Cir. 2001).

38. *Parker v. Google, Inc.*, 422 F. Supp. 2d 492 (E.D. Pa. 2006).

39. *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Ca. 2001).

to-peer networks,⁴⁰ and the companies which provide Internet access.⁴¹ Thus, the definition allows the DMCA to reach a wide variety of services involved in foreign infringement.

While courts have construed “service provider” more narrowly, they have only done so in the context of the DMCA’s subpoena provision.⁴² The courts have held that “a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity.”⁴³ As such, what constitutes a “service provider” is only narrowed when the subpoena provision is at issue, which is not the case when dealing with the Foreign Site Provision. Although application of the Foreign Site Provision requires the disabling of access to some content, it does not require a subpoena, and thus does not require that a court follow the narrow “service provider” interpretation applied in § 512(h) cases.⁴⁴

2. Whose Internet Access Is to Be Restrained?

The plain meaning of the “restraining . . . from providing access” portion of the Foreign Site Provision requires a service provider to block access to an infringing site.⁴⁵ While straightforward in this regard, difficulties with interpreting this provision may arise in terms of scope. The text of the provision does not specify whose access is to be blocked; rather, the focus of the provision is on the infringing site or server.⁴⁶ Guidance in how to read the Foreign Site Provision may come from the previous provision, the Individual User Provision, which focuses on individuals. It states that the court may grant injunctive relief by providing:

An order restraining the service provider from providing access to a subscriber or account holder of the service provider’s system or network who is using the provider’s

40. *In re Aimster Copyright Litig.*, 334 F.3d 643 (7th Cir. 2003).

41. *Recording Indus. Ass’n of Am., Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1236 (D.C. Cir. 2003).

42. The subpoena provision specifically at issue is § 512(h) (describing (1) the request for identification of an alleged infringer, (2) the contents of the request, (3) the contents of the subpoena, (4) the basis for granting the subpoena, (5) the actions of a service provider receiving the subpoena, and (6) the rules applicable to the subpoena). See *Verizon*, 351 F.3d at 1236; *In re Charter Commc’ns, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 777 (8th Cir. 2005) (adopting the reasoning of *Verizon*).

43. *Verizon*, 351 F.3d at 1233.

44. See *id.* at 1236; *In re Charter Commc’ns, Inc.*, 393 F.3d at 777 (adopting the reasoning of *Verizon*).

45. 17 U.S.C. § 512(j)(1)(B)(ii) (2005).

46. *Id.*

service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.⁴⁷

The Supreme Court has held that “where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.”⁴⁸ Therefore, courts may read the Foreign Site Provision to apply to all subscribers of the ISP, once infringement has been established.⁴⁹

While the Foreign Site Provision may be read to block access to all subscribers of a particular service provider once an infringing site has been identified, the text of § 512 indicates that it should not apply to the subscribers of other service providers in the United States. Section 512 of the DMCA specifies the limitations on liability for online material and specifically speaks in terms of safe harbors for qualifying ISPs.⁵⁰ The safe harbor provisions apply only to “a system or network controlled or operated by or for the service provider”⁵¹ or “the provider referring or linking users.”⁵² The Act therefore applies to ISPs that are actually involved in some way with the infringement. If service providers without infringing customers are forced to block content because of the conduct of another service provider’s subscriber, it would improperly extend the reach of the Act.

Although this interpretation of scope focuses on the language in the safe harbor provisions, it is also supported by one of the underlying purposes of the Act. The DMCA was enacted to protect ISPs from secondary liability for the direct infringement of their subscribers.⁵³ If none of the subscribers of the service provider at issue directly infringed, then the service provider would not be subject to secondary liability and thus would not be subject to the Foreign Site Provision of the DMCA.⁵⁴ Certainly, if the DMCA is to protect service

47. *Id.* § 512(j)(1)(B)(i) (emphasis added).

48. *KP Permanent Make-Up, Inc. v. Lasting Impression I, Inc.*, 543 U.S. 111, 118 (2004) (quoting *Russello v. United States*, 464 U.S. 16, 23 (1983) (quoting *United States v. Wong Kim Bo*, 472 F.2d 720, 722 (5th Cir. 1972) (alteration in original)) (internal punctuation and citations omitted)).

49. Such a broad reading of the scope of § 512(j)(1)(B)(ii) may come under fire due to its limitations on users who have not used a particular website for illegal ends. A simple reading of the text should dispel this argument because of its obvious focus on protecting copyrights—not users’ access to content.

50. § 512(a)-(d).

51. *Id.* § 512(a)-(c).

52. *Id.* § 512(d).

53. H.R. REP. NO. 105-551, pt. 2, at 21 (1998) (Conf. Rep.).

54. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 921, 930 (2005) (“One infringes contributorily by intentionally inducing or encouraging direct infringement . . . and

providers who have not been involved in the direct infringement of their own subscribers, it would seem obvious that it should also protect those whose subscribers have done nothing illegal at all.

While copyrights would best be protected if no U.S. service providers granted access to infringing sites, the text of the DMCA simply does not support such a proposition. Although this may lead to a constant shuffling of subscribers from one service to the next until all services have blocked particular sites, it will mean that only the services where such a problem exists will be required to implement the blocking technology. As such, textual analysis of the Foreign Site Provision requires its application only to the subscribers of a service provider through which direct infringement has occurred.

3. What Constitutes Reasonable Steps to Block Access?

The DMCA also requires that the ISP be able to block access to the "specific, identified, online location" through "reasonable steps."⁵⁵ The determination of what constitutes "reasonable steps" would need to be made on a case-by-case basis and analyzed in light of § 512(j)(2)(A).⁵⁶ That section indicates that courts should consider whether an injunction "would significantly burden either the provider or the operation of the provider's system or network."⁵⁷ Additionally, § 512(j)(2)(C) requires consideration of "whether implementation of such an injunction would be technically feasible and effective." Specifically, it requires that the court examine the ability of an ISP to block access to the infringing sites, rather than arbitrarily ordering an ISP to block access when doing so would either be technically or financially infeasible.⁵⁸

4. How Do Courts Determine that the Online Location Is Outside of the United States?

To block access to an infringing site, a court must determine that the online location is outside of the United States.⁵⁹ While a website can be viewed from many different computers in many different locations, the information is made available via the website's

infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it.").

55. § 512(j)(1)(B)(ii).

56. Analysis of § 512(j)(2) is seen *infra* Part III.B.1, "Significance of the Burden on the ISP."

57. § 512(j)(2)(A).

58. The technical feasibility and effectiveness of blocking measures are analyzed *infra* Part III.B.3, "Technical Feasibility and Effectiveness."

59. § 512(j)(1)(B)(ii).

server, a physical object from which the information is downloaded for viewing. The statute is concerned with the physical location of this server, not the many locations where the site can be viewed.

For a website to exist, it must be stored on a computer. For that website to be available to others across the Internet, that computer must be connected to the Internet. To be accessible by other computers, all servers have Internet Protocol ("IP") addresses.⁶⁰ While these addresses make it possible for users across the world to access a website, they also make it possible to determine the location of a particular website's server.⁶¹ The ability to trace a website's server to a particular country makes it possible to easily determine whether the Foreign Site Provision applies to an infringing website.

B. Examination of the Considerations of § 512(j)(2)

Section 512(j)(2) requires courts to consider four factors in determining whether to grant injunctive relief. Those four factors consider (1) the significance of the burden of an injunction on the ISP,⁶² (2) "the magnitude of harm likely to be suffered by the copyright owner . . . if steps are not taken to prevent or restrain the infringement,"⁶³ (3) the technical feasibility and effectiveness of an injunction, and (4) whether it would "interfere with access to noninfringing material at other online locations,"⁶⁴ and "whether other less burdensome and comparably effective means . . . are available."⁶⁵ While such considerations will lead to a case-by-case analysis, some generalizations can be made regarding the magnitude of harm, the current state of blocking technology, and other viable options to protect the copyright holder. Therefore, examination of each consideration will provide guidance in how a court may decide this issue in the near future.

1. Significance of the Burden of the ISP

Section 512(j)(2)(A) states that a court shall consider "whether such an injunction, either alone or in combination with other such

60. For more information about servers, IP addresses, and Internet technologies, see *infra* Part III.B.3, "Technical Feasibility and Effectiveness."

61. InternetFrog.com allows users to determine a website's server location directly through its IP address. If the IP address is unknown, a user may use the site's Domain Name System Lookup to find a website's IP address and then determine the server's location.

62. § 512(j)(2)(A).

63. *Id.* § 512(j)(2)(B).

64. *Id.* § 512(j)(2)(C).

65. *Id.* § 512(j)(2)(D).

injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network." While this consideration requires analysis of the burden of implementing the blocking mechanism, such analysis depends largely on how the Foreign Site Provision is applied.⁶⁶ If the provision were held to apply to all ISPs (unlikely though such an application may be), then the relative burden on one ISP would not be as significant as if it were the only one obligated to block an infringing site. All ISPs would incur the increased costs, and all would in turn have to adjust prices and/or profits.⁶⁷

However, as stated previously, the provision should be held to only apply to the particular ISP of a direct infringer.⁶⁸ Thus, the burden may be great. An enjoined service provider pays to implement filters and loses content that is attractive to some of its subscribers. Non-enjoined services will continue to operate as before, without increased costs or diminished content—in other words, providing more content at possibly lower prices. As a result, the non-enjoined services become more attractive to would-be-infringing subscribers and the enjoined service providers lose customers. These would-be-infringing subscribers will continue to move to the non-enjoined service providers until all service providers are enjoined. While the burden will be great on the first enjoined service providers, it may be of equal magnitude for the last enjoined service providers if their attractiveness stems solely from the fact that they could still be used to access foreign infringing content.

The preceding analysis is based on two assumptions, which may not be applicable in every situation. First, it is based on the assumption that a commercially significant number of customers will switch services so that they may continue infringing. While a great number of infringers exist, many might just find it easier to find a different site which is not blocked or quit such activity altogether. Second, the analysis assumes that there will be other services available for these customers. While larger cities may have several options, many people in the United States do not have multiple services that will provide them with the high-speed access needed to

66. For more information about blocking mechanisms, see *infra* Part III.B.3, "Technical Feasibility and Effectiveness."

67. It should be noted that this might therefore favor larger market participants who could more easily spread costs over a wider customer base.

68. See *supra* Part III.A.2, "Whose Internet Access Is to Be Restrained?"

take full advantage of these infringing websites.⁶⁹ Therefore, the magnitude of the burden may be greatly diminished depending on the customers and competition of a given service.

2. Magnitude of the Harm Likely to Be Suffered by the Copyright Owner

Section 512(j)(2)(B) requires that the court consider “the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement.” While weighing the harm to the copyright owner makes sense in light of the previous provision’s consideration of the harm to the ISP, it places a copyright holder in a difficult position. Although the text of § 512(j)(2)(B) speaks in terms of harm “likely to be suffered,” it would seem that such a determination would no doubt be largely based on evidence of present harm. Surely it would be difficult to prove to a court that a copyright will be *greatly* infringed if not protected. Therefore, if a copyright holder acts too quickly (i.e., before his works have been substantially infringed) then he risks a finding that the magnitude of harm is not great enough to merit the injunction. If the copyright holder waits until the magnitude of harm is great, he must allow infringement for some time before seeking legal action. The consideration of the magnitude of harm to the copyright owner forces courts to forecast music trends or the future traffic on the website at issue. Both possibilities create a task that a court is ill-equipped to handle.

A determination of the magnitude of harm would most likely focus on the type of work infringed. Such an interpretation would apply a proportionality test, which would protect more valuable copyrights.⁷⁰ The interpretation would favor a “soon-to-be-released film, sound recording, or computer program” over “an article contained in a seldom-read journal,” because the former has much greater commercial value.⁷¹ As movies, music, and software are the main targets of infringement, it is easy to argue that they are the works in most need of protection. Nonetheless, simply because a movie is worth

69. As more companies begin to offer high-speed access throughout the country, the ability to switch services will arise and this assumption should hold true across the United States.

70. *H.R. 2180, The On-line Copyright Liability Limitation Act and H.R. 2281, The WIPO Copyright Treaties Implementation Act: Hearing Before the Subcomm. on Courts and Intellectual Property*, 105th Cong. (1997) (statement of Michael K. Kirk, Executive Director, American Intellectual Property Law Association) (The proportionality test compares the ISP costs to block an infringing site with the copyright holders expected losses, with more valuable works therefore being more worthy of an injunction.).

71. *Id.*

more than an article and its copyright is more frequently infringed does not necessarily mean it should be afforded more protection. If a court focuses on proportionality, it may lead to the protection of all "soon-to-be-released films," but no protection for scholarly articles. Thus the proportionality test may best determine the level of judicial protection, but it does not necessarily mean that all copyrights will be adequately protected. It is possible that the cost of blocking programs will be so low that the value of the copyright will not be a strong consideration, but if blocking costs are high, the consideration could greatly limit the protection of less commercially valuable works.

Although less likely to be used by a court, another possible interpretation of § 512(j)(2)(B) would focus on the magnitude of harm to the copyright holder in terms of his collection of copyrighted works. Under this interpretation, if a copyright holder had many copyrighted works and only one of them was being infringed, the magnitude of harm would not be as great as if it were the holder's only copyrighted work. Thus, harm would be measured in relative terms to the copyright owner. Such an interpretation would not only be difficult to administer, but would also be inequitable.⁷² Small copyright holders, to whom a small amount of infringement would constitute a great deal of harm, would be greatly protected, but copyright holders with large music catalogs, who would be less damaged by the infringement of a few works, would not be equally protected.⁷³

Essentially, it would appear that § 512(j)(2)(B) merely serves to counterbalance the interests of the ISPs in § 512(j)(2)(A). With the current state of technology, it would be difficult for a court to hold that the infringement of a copyright does not qualify as a harm of great magnitude, yet the provision allows for just such a finding. If the court finds that the burden on the ISP is too great, it can use § 512(j)(2)(B) to claim that the magnitude of the harm to the copyright holder is also small and thus strengthen its holding. Conversely, the magnitude of harm to the copyright owner may be used to support a holding and to help downplay the harm to the ISP. As there is no standard to determine whether something constitutes a high magnitude of harm,⁷⁴

72. Determining the relative value to a copyright owner could be more difficult than using market analysis to determine the market value of a copyrighted work.

73. It is difficult to believe that the major record companies would have supported the DMCA if this was the correct interpretation of how to determine magnitude of harm.

74. It should be noted that sufficient harm (in these cases, "irreparable harm") has been found in granting preliminary injunctions against Napster and Aimster. See *In re Aimster Copyright Litig.*, 334 F.3d 643, 655 (7th Cir. 2003) (discussing granting of injunctions); *A&M Records v. Napster, Inc.*, 239 F.3d 1004, 1017 (9th Cir. 2001).

the provision simply provides a court with one more argument to bolster its holding.

3. Technical Feasibility and Effectiveness

In determining whether or not an injunction would be appropriate, § 512(j)(2)(C) requires courts to consider “whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations.” Therefore, a court contemplating ordering a website blocked must consider whether such technology exists, how effective and focused that technology is, and how long it would take an ISP to implement such technological measures.

Determining technical feasibility and effectiveness requires an understanding of how a website is accessed. To begin, a web publisher creates a website which is located on either his server or the server of a web host.⁷⁵ The web hosting service either

(1) provides a Web Server to service a single website of a customer, (2) provides a Web Server the customer can use to run multiple sites, or (3) provides space on a Web Server that services the website of many different customers [through what] is commonly called virtual web hosting.⁷⁶

Servers have “a unique address—just like a telephone number—which is a rather complicated string of numbers,” which is called an Internet Protocol (“IP”) address.⁷⁷ Although the numerical-based IP addresses may be used to access websites, sites are usually accessed through their text-based Uniform Resource Locator (“URL”).⁷⁸ Through use of a large database called the Domain Name System (“DNS”), Internet users are connected to websites by a “familiar string of letters (the domain name),” rather than the string of numbers composing the IP address.⁷⁹ In other words, the DNS acts like directory assistance. An Internet user sends a request for a webpage by name (the URL), the DNS finds the proper number (the IP address), and then connects the user. As such, there are three identifiable components which deliver a website to an Internet user:

75. *Ctr. for Democracy & Tech. v. Pappert*, 337 F. Supp. 2d 606, 614 (E.D. Pa. 2004). Should the website publisher choose to use his own server, he would then need to contract with an ISP for Internet access for his server. *Id.*

76. *Id.*

77. Internet Corporation for Assigned Names and Numbers, “FAQs: What is the Domain Name System?,” <http://www.icann.org/faq/#dns> (last visited Mar. 6, 2006).

78. “A URL is the commonly used textual designation of an Internet web site’s address.” *Pappert*, 337 F. Supp. 2d at 615. For example, the URL “www.vanderbilt.edu” has the IP address “http://129.59.1.28.”

79. *Id.*

the website's IP address, the website's URL, and the DNS that links the two.

Previous efforts to implement blocking software have seen limited success. Perhaps the most notable attempt to block Internet content was seen with Pennsylvania's Internet Child Pornography Act.⁸⁰ Similar to the notice and takedown requirement at issue in DMCA subpoena provision cases,⁸¹ the statute required the disabling of access to illegal content.⁸² The Act required that:

[a]n Internet service provider shall . . . disable access to child pornography items . . . accessible through its service . . . to persons located within this Commonwealth within five business days of when the Internet service provider is notified . . . that child pornography items . . . are accessible through its service.⁸³

After receiving notice of the presence of child pornography on particular websites, ISPs responded by implementing filters.⁸⁴ The ISPs tried different forms of filtering, which met with varied levels of success—in terms of blocking the sites at issue and in limiting the blocking to only those particular sites.⁸⁵ Since the law required ISPs to block offending sites within five days of notice, filtering options were limited.⁸⁶ The technology simply did not exist to block only offending sites; non-offending sites were blocked by the technology, too. This lack of effective filtering technology led the Eastern District of Pennsylvania to strike down the law in *Center for Democracy & Technology v. Pappert*.⁸⁷ The court held that “the Act suppresses substantially more protected material than is essential to the furtherance of the government’s interest in reducing child sexual abuse,” and thus violated many people’s freedom of expression.⁸⁸

In *Pappert*, the court examined the varying forms of filtering, which are the same forms of filtering that a court would examine in

80. 18 PA. CONS. STAT. §§ 7621-30 (2002).

81. See *Recording Indus. Ass’n of Am., Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1236 (D.C. Cir. 2003); *In re Charter Commc’ns, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 777 (8th Cir. 2005) (adopting the reasoning of *Verizon*).

82. 17 U.S.C. § 512(c)(3)(iii) (2005) (requiring that for effective notice, “[i]dentification of the material that is claimed to be infringing or to be the subject of infringing activity and that . . . access to which is to be disabled”).

83. 18 PA. CONS. STAT. § 7622 (2002).

84. *Ctr. for Democracy & Tech. v. Pappert*, 337 F. Supp. 2d 606, 639-42 (E.D. Pa. 2004) (describing ISP filtering in response to notice).

85. *Id.* (describing the number of other sites affected by the ISP’s filtering).

86. *Id.* at 637 (“It took three days for [the block] . . . to propagate to all of the DNS servers in the Comcast network, and with only five days to comply with an Informal Notice, Comcast concluded that implementation of DNS filtering was too slow.”).

87. *Id.* at 655.

88. *Id.* The court also noted that “[m]ore than 1,190,000 innocent websites were blocked in an effort to block less than 400 child pornography websites.” *Id.*

ordering an ISP to block a site under the Foreign Site Provision. As filtering options vary in effectiveness and cost, courts must determine which option best fits the particular situation.⁸⁹ Although new means of blocking websites may be created, at this time three options exist: IP filtering, URL filtering, and DNS filtering.⁹⁰

a. IP Filtering

One option ISPs have in blocking foreign websites is the use of IP filtering. To IP filter, an ISP determines the IP address to which a specific URL resolves and then makes entries in its own routing equipment to stop outgoing requests for that particular IP address.⁹¹ As most ISPs already engage in IP filtering to manage their networks, the requisite hardware for such filtering is often already in place.⁹² Importantly, IP filtering does not affect network performance.⁹³

While IP filtering is easy to implement, it “leads to a significant amount of overblocking.”⁹⁴ The problem of overblocking stems from the fact that many websites use the same IP address.⁹⁵ Therefore, when an infringing site at a particular IP address is blocked, so are all the other sites located at the same address.⁹⁶ As the record in *Pappert* indicates, there may be hundreds of thousands of websites located at the same IP address.⁹⁷ As such, IP filtering is unable to differentiate between individual websites that should and should not be blocked, if they are all located at the same IP address.⁹⁸ Such a problem contributed to the *Pappert* court’s holding that the Pennsylvania

89. The problems seen with the varying forms of filtering may ultimately lead a court to find that blocking foreign sites is simply not a viable option at this time.

90. *Pappert*, 337 F. Supp. 2d at 628.

91. *Id.*

92. *Id.* at 629. These filters are used to protect networks from viruses and spam. *Id.*

93. *Id.*

94. *Id.* at 633.

95. The use of one server and IP address for many websites is called virtual hosting, as discussed *supra* Part III.B.3, “Technical Feasibility and Effectiveness.”

96. IP overblocking occurred in *Pappert*, where a community center and school website (and at least 15,574 other sites) were blocked because they shared an IP address with a blocked child pornography site. *Pappert*, 337 F. Supp. 2d at 638.

97. AOL’s blocking of one IP address “led to the blocking of hundreds of thousands of websites.” *Id.* at 639. In its use of IP blocking, Comcast blocked 491,850 websites at one IP address and 334,395 at another. *Id.* at 641.

98. It should also be noted that websites may change their IP address to avoid filters. While such a tactic may help a site avoid some filters, an ISP can institute “a process to track the IP addresses of the sites it block[s] . . . so that it [can] change the block if the IP addresses of the targeted URLs [are] changed.” *Id.* at 625-26.

Internet Child Pornography Act was unconstitutional⁹⁹ and may lead to a finding under § 512(j)(2)(C) that IP filtering “interfere[s] with access to noninfringing material at other online locations.”¹⁰⁰

b. URL Filtering

Another blocking option is the use of URL filtering. Through this method, an ISP will block access to a website “if the requested URL in the web request matches one of the URLs specified in a blocking order.”¹⁰¹ While some ISPs do not conduct any URL filtering, others, such as America Online (“AOL”), use URL filtering for their “parental controls” to limit objectionable content.¹⁰² While such use works to filter small parts of networks, doing so for all users may be very difficult and costly.¹⁰³ To accomplish URL filtering requires ISP routers and switches to perform many computations.¹⁰⁴ As Computer Science Professor Mitchell Marcus testified in *Pappert*, “[p]erforming these computations . . . slow[s] down each switch and router substantially and decrease[s] the overall capacity of the network.”¹⁰⁵ Therefore, while URL filtering is the most precise way to block websites, it is also the most costly to implement.

c. DNS Filtering

DNS filtering is a third option by which to block a website. As mentioned previously, most Internet users type a URL to access a site. DNS servers then convert the URL into an IP address. As the *Pappert*

99. The Pennsylvania Supreme Court concluded that the regulation did not “further an important government interest unrelated to the suppression of free expression and [that] the incidental restriction on First Amendment freedoms . . . [were] greater than [was] essential to the furtherance of that interest.” *Id.* at 655 (citation omitted).

100. 17 U.S.C. § 512(j)(2)(C) (2005). The consideration of whether a blocking mechanism interferes with access does not specify to what degree the mechanism must interfere. As no language speaks to the issue, it must be read to mean that any level of interference should be considered in determining whether an injunction blocking access to an infringing foreign site would be appropriate.

101. *Pappert*, 337 F. Supp. 2d at 628.

102. *Id.* at 630.

103. *Id.* Although neglecting to place a number on the costs involved with implementation of URL filtering across AOL, one of its engineers stated that doing so would “take years to implement” and “require expenditures for development, installation, new hardware and software, management costs, performance assessments, customer support, and further re-engineering of the network.” *Id.* At the time of trial, Verizon did not perform any URL filtering and stated that it would cost “‘well into seven figures’ to implement URL filtering across its entire network.” *Id.* at 631.

104. *Id.* at 630.

105. *Id.* at 630-31.

court stated, “[t]ypically, an ISP gives its customers the IP addresses of DNS servers controlled by the ISP. The addresses are entered in the customers’ computers during the Internet access set-up process, a process that is often automated.”¹⁰⁶ Through DNS filtering, URL requests to these DNS servers are answered with error messages or incorrect addresses.¹⁰⁷

While DNS filtering may not have a significant effect on an ISP’s performance, there are many downsides to its use.¹⁰⁸ Although ISPs generally control which DNS servers their subscribers access, some ISPs use other DNS servers.¹⁰⁹ Additionally, “DNS filtering is a ‘much more specialized technique,’ ” which would require some ISPs to design new systems, configure additional DNS servers, and “potentially reconfigure the systems of millions of customers.”¹¹⁰ Therefore, while “the cost of implementing IP filtering and DNS filtering is approximately equal,” the use of DNS filtering would greatly burden those ISPs that currently do not perform the function.¹¹¹ Finally, DNS filtering may also result in a great deal of overblocking, if the domain name blocked includes “independent content as sub-pages on the service’s site.”¹¹²

4. Availability of Less Burdensome and Comparably Effective Means

The final consideration examines “whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.”¹¹³ While application of this factor will vary according to the technology of the time, some elements of the analysis will always be present.

As there will always be an offending foreign site in a § 512(j)(1)(B)(ii) case, there will always be the option of persuading the operator to remove the infringing content or shutting the site down.

106. *Id.* at 617.

107. *Id.* at 628.

108. *Id.* at 630.

109. *Id.* at 631-32. *Pappert* states that “[l]arge businesses often operate their own [DNS servers]” and that an individual user may “redirect his computer to a DNS server not controlled by his ISP.” *Id.* It is noted that redirection is a difficult process which “requires knowledge that it is possible, an understanding of how to accomplish it, knowledge of the IP address of an alternate DNS server, and knowledge of the steps, often complicated, that must be taken to enter that IP address into the user’s computer.” *Id.* at 632.

110. *Id.* at 629-30.

111. *Id.* (internal quotations omitted).

112. *Id.* at 633. The example used by the court was the blocking of a domain name such as GeoCities.com due to an offensive sub-page. As the site “allows many different users to have websites on sub-pages,” DNS filtering would block all sites located at GeoCities.com. *Id.*

113. 17 U.S.C. § 512(j)(2)(D) (2005).

Generally, these options will not be available to a copyright holder seeking an injunction under the Foreign Site Provision. Copyright holders wish to protect their content worldwide, so it is unlikely that they would try to eliminate U.S. access without attempting to eliminate worldwide access by shutting down the site in the host country.¹¹⁴ In fact, it is this very difficulty of shutting down infringing foreign sites that makes the provision relevant in today's world.

Another option for "preventing or restraining access" to foreign sites would be through the use of the Individual User Provision. This section allows for the termination of an infringing subscriber's account.¹¹⁵ From a purely technical standpoint, it would not be burdensome for the ISP to simply terminate an infringing user's accounts. There would be no need for advanced blocking technologies and the service could continue to operate as it always had. However, from a financial standpoint, such an option could be highly burdensome. Every time a subscriber is found to have infringed, the ISP would have to terminate service and, in turn, lose a customer. The customer would then simply use a competing ISP, until caught again. Such an option mandates that the ISP lose a customer. Regardless of the effect on subscribers seen through application of the Foreign Site Provision, ISPs are not certain that they will lose all of their infringing customers. As such, blocking individual subscribers may be less technically burdensome, but more financially burdensome due to the certain loss of subscribers.¹¹⁶ The financial burden to ISPs of using the Individual User Provision may therefore generally weigh against finding it to be a less burdensome means of preventing infringement than the use of the Foreign Site Provision.

114. See *Russian DA Clears AllOfMP3.com of Copyright Infringement Charges*, ONLINE REPORTER, Mar. 12, 2005, http://www.onlinereporter.com/article.php?article_id=1021 (indicating that foreign courts and copyright law may make it difficult to shut down foreign sites).

115. Under § 512(j)(1)(B)(i), injunctive relief may be in the form of "[a]n order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order." *Id.*

116. In actuality, to have the same effect on ISP subscriptions would require copyright holders to file suit against massive numbers of infringers. Although this results in a loss of customers to the ISP, it puts the burden on the copyright holder to identify all infringers before they may be blocked. Placing the burden on copyright holders would greatly increase the time it would take to stop the infringement and result in greater losses for the copyright holder. In other words, blocking one individual at a time would not be a "comparably effective means of preventing or restraining access to the infringing material." § 512(j)(2)(D).

IV. MISGUIDED ARGUMENTS AGAINST THE USE OF THE PROVISION

Use of the provision will no doubt raise concerns on two fronts. First, the filtering of content may be construed as a restraint on free speech. Second, the filtering may be construed as having a chilling effect on technology. Both of these arguments are frequently seen in similar copyright cases and will certainly be raised with the use of the Foreign Site Provision. Analysis of the provision in light of both the First Amendment and its effect on technology indicates that these arguments will fail.

A. Use of the Provision Does Not Violate the First Amendment

In *Martin v. City of Struthers*, the Supreme Court recognized that the freedom of speech “embraces the right to distribute literature and necessarily protects the right to receive it.”¹¹⁷ Those opposing pro-copyright laws and judicial decisions generally invoke this right to distribute and receive literature when file-sharing sites are in question.¹¹⁸ Recently, this argument was made in the American Civil Liberties Union’s (“ACLU”) amicus brief in support of *Grokster*.¹¹⁹ The ACLU argued that a ruling that limited technologies in the name of copyright would constrain people’s ability to express themselves.¹²⁰ In other words, strong copyright protection could mean the end of (or prevent the creation of) technologies used for expression. The Court failed to address this issue in *Grokster*, thus keeping the argument alive.

Unlike *Grokster*, any sites blocked by the Foreign Site Provision will be located outside the United States. As a result, the freedom of speech will not be implicated because the provision prevents speech in a foreign location (not subject to U.S. law). Nonetheless, the First Amendment may be implicated if the provision’s use prevents Internet users in the United States from hearing First Amendment-protected speech from foreign countries.¹²¹

As the Court stated in *Martin v. City of Struthers*, “[t]he privilege [to distribute and receive speech] may not be withdrawn . . .

117. *Martin v. City of Struthers*, 319 U.S. 141, 143 (1943) (internal citation omitted).

118. U.S. CONST. amend. I.

119. Brief for American Civil Liberties Union et al. as Amici Curiae Supporting Respondents, *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005) (No. 04-480), 2005 WL 539135.

120. *Id.* at 28.

121. A site such as AllOfMP3.com, a for-profit site, and others like it only offer copyrighted works for sale. As such, blocking the site only prevents infringement, not the transfer of protected speech, so First Amendment issues do not arise.

[but] the community may imperatively require regulation of the time, place and manner of distribution.”¹²² Therefore, if the Foreign Site Provision is found to interfere with a U.S. Internet user’s right to hear, the Court would likely apply its holding in *Ward v. Rock Against Racism*, which dealt with a time, place, or manner restriction on speech.¹²³ In *Ward*, the Court held that:

even in a public forum the government may impose reasonable restrictions on the time, place, or manner of protected speech, provided the restrictions “are justified without reference to the content of the regulated speech, that they are narrowly tailored to serve a significant governmental interest, and that they leave open ample alternative channels for communication of the information.”¹²⁴

Further, it held that “[a] regulation that serves purposes unrelated to the content of expression is deemed neutral, even if it has an incidental effect on some speakers or messages but not others.”¹²⁵ To satisfy the “narrow tailoring” requirement, the regulation need only “promote[] a substantial government interest that would be achieved less effectively absent the regulation.”¹²⁶ Therefore, even if a court finds that a less speech-restrictive regulation is possible, that alone will not be sufficient to invalidate the regulation.¹²⁷

The Foreign Site Provision is constitutional under the *Ward* test. It is a content neutral regulation, as its purpose is to protect copyrighted works, not to prevent any particular speech or the reception of it. Furthermore, the Foreign Site Provision is narrowly tailored, as it promotes the substantial government interest of protecting copyrighted works from infringement, which would be less effectively protected without the regulation. Although it could be argued that there are less-speech-restrictive alternatives to protect copyrighted works from infringement (blocking only the direct infringers, shutting down the infringing sites, etc.), the presence of these alternatives does not render the Foreign Site Provision unconstitutional.¹²⁸ Further, blocking infringing sites still “leaves open alternative channels for communication” through non-infringing foreign or domestic sites. Thus, the Foreign Site Provision’s restriction on speech would be constitutional, as it substantially promotes the

122. 319 U.S. at 143 (internal citations omitted).

123. *Ward v. Rock Against Racism*, 491 U.S. 781, 797-98 (1989).

124. *Id.* at 791 (quoting *Clark v. Cmty. for Creative Non-Violence*, 468 U.S. 288, 293 (1984)).

125. *Id.*

126. *Id.* at 799 (quoting *United States v. Albertini*, 472 U.S. 675, 689 (1985)).

127. *Id.* at 800.

128. *Id.*

government's interests in a content neutral manner without eliminating alternative channels for communication.¹²⁹

B. Use of This Provision Will Not Have a "Chilling Effect" on Technology

History has shown that copyright holders will bring suit to protect their copyrighted works from access via new technologies.¹³⁰ While these suits are brought against individual direct infringers,¹³¹ they are also brought against those who make such infringement possible. Suing the entities that make online infringement possible allows copyright holders to stop direct infringement by millions through one suit, rather than through millions of individual suits. Frequently, these secondary liability cases are described as cases of creativity versus technology.¹³² The fear in these cases, however, is that a broader application of secondary liability will have a "chilling effect" on technology. As the Court stated in *Sony*, broadening secondary liability too much can "enlarge the scope of [copyright] monopolies to encompass control over an article of commerce that is not the subject of copyright protection. Such an expansion of the copyright privilege is beyond the limits of the grants authorized by Congress."¹³³ In other words, there is a persistent worry that broad secondary liability will discourage inventors from creating new technologies for fear of liability through unintended infringing uses. Evidence of this worry was recently seen in *Grokster*.¹³⁴ Although *Grokster* did not reach the *Sony* decision, it highlighted the fact that

129. Following the same reasoning, use of 17 U.S.C. § 512(j)(1)(B)(ii) (2005) to prevent access to a site distributing file-sharing software proven to be used for copyright infringement would be constitutional.

130. See *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005) (decentralized peer-to-peer network); *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984) (VCR); *A&M Records v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001) (centralized peer-to-peer network); *Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys.*, 180 F.3d 1072 (9th Cir. 1999) (portable mp3 player).

131. Grant Gross, *RIAA Files New Round of Lawsuits, P-to-P Use Down*, INFOWORLD, Dec. 15, 2005, available at http://www.infoworld.com/article/05/12/15/HNriaalawsuits_1.html (stating that in a two year span the RIAA had sued over 17,000 alleged direct infringers).

132. *Grokster*, 545 U.S. at 928 ("The more artistic protection is favored, the more technological innovation may be discouraged; the administration of copyright law is an exercise in managing the trade-off").

133. *Sony*, 464 U.S. at 421.

134. Brief of Respondent-Appellee at 22-23, *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd.*, 380 F.3d 1154 (9th Cir. 2004) (Nos. 03-55894, 03-56236, 03-55901), 2003 WL 22753807 ("Sony-Betamax Prevents Copyright Owners from Using Their Statutory Monopoly to Stifle Innovation").

these fears exist and will be raised in the future when liability is applied to new technologies.¹³⁵

With the Foreign Site Provision, a new technology would not be at issue, but a further restraint on an old technology (peer-to-peer networks) would occur. In contrast to cases in which courts have held secondary infringers financially liable, the provision simply finds that a user is liable and that the site must therefore be blocked. The operator of the ISP need not be involved in any way with the infringement for his site to be blocked. Many would view this as a low bar to clear before the law can be used to interfere with technology.

An examination of the provision and the “chilling effect on technology” argument indicates that the Foreign Site Provision would not have the significant impact on technology that some may argue. First, the provision only applies to websites through which infringement has occurred. While the provision does not require secondary liability for the infringing service to be blocked, it does require a finding that infringement has occurred. Services not used for infringement are not subject to this provision. Second, the provision applies only to foreign websites. Therefore, not every website or Internet technology will be damaged by this provision—in fact, no U.S. websites will be subject to it. Third, the provision does not hold the service liable; it simply blocks access to it. As a result, the application of this provision may lessen the return an inventor sees on his creation, but it will not subject him to liability.¹³⁶ As the provision does not involve secondary liability, the “chilling effect on technology” argument is misplaced.

V. APPLICATION OF § 512(J)(1)(B)(II)

As legal victories for copyright holders continue, it has become more difficult for infringing file-sharing sites to operate in the U.S. without fear of liability. While this does not spell an end to infringing file-sharing services, it drives them out of the United States and the reach of its laws.¹³⁷ Although some foreign courts have taken action against these sites, they still exist and many more will be created.¹³⁸

135. *Grokster*, 545 U.S. at 933-34.

136. He would still be subject to secondary liability, but not as a result of this particular provision.

137. Yagan, *supra* note 15 (predicting that, as a result of the *Grokster* decision, individual developers of P2P applications “will go offshore and underground and become harder to find”).

138. *File-Swappers Sentenced to Jail*, CHINA POST (Taiwan), Sept. 10, 2005 (reporting the determination of software company Kuro, distributor of Taiwan’s most popular peer-to-peer software program, to continue to advertise the program, despite several of its executives being sentenced to jail for copyright violation); Louise Crossen and Tara Ravens, *Site Pulls the Plug on*

U.S. courts cannot reach the infringing services, but through the Foreign Site Provision they can keep the services from reaching the United States. The Foreign Site Provision may be the only way a copyright holder can protect his work from infringement in the United States through foreign services. Showing direct infringement by subscribers of the largest U.S. service providers and using the Foreign Site Provision will allow copyright holders to block many would-be infringers from accessing centralized peer-to-peer services, pay sites, and websites offering decentralized peer-to-peer software, and thereby protect copyrighted works from massive U.S. infringement.

A. How Copyright Holders Should Use § 512(j)(1)(B)(ii)

The text of the Foreign Site Provision indicates that it is to apply to all of the subscribers of a service provider, once a case of infringement has been proven.¹³⁹ As a result, a judgment finding direct infringement by one subscriber of AOL would make it possible for the copyright holder to use the Foreign Site Provision to block all AOL subscribers from the site used for infringement. In other words, the content industry need only have one judgment against a user of a foreign site to use the Foreign Site Provision to block the site from AOL's 15.2 million other subscribers.¹⁴⁰ Should a judgment be found against a Comcast subscriber and an AT&T subscriber, an infringing site could be blocked from over 19.1 million additional subscribers.¹⁴¹ Therefore, copyright owners could keep over 34 million people from using an infringing site by just showing infringement through three service providers.

Before the Foreign Site Provision may be invoked, there must be a finding of direct infringement. While direct infringement occurs frequently on file-sharing services, it can be difficult to identify the infringing user.¹⁴² While copyright holders "can readily obtain the

File Sharers, COURIER MAIL (Australia), Dec. 7, 2005, at 5 (noting that Kazaa's act of prohibiting Australian users from downloading the software, rather than complying with an Australian court order to install content filters in the software, was merely a token measure that still allowed Australian users to download copyrighted music).

139. See *supra* Part III.A.2., "Whose Internet Access Is to Be Restrained?"

140. Alex Goldman, *Top 22 U.S. ISPs by Subscriber: Q3 2006*, ISP PLANET, Dec. 28, 2006, <http://www.isp-planet.com/research/rankings/usa.html> (listing AOL as the largest ISP, as of the third quarter of 2006, having 15.2 million subscribers).

141. *Id.* (listing the number of Comcast and SBC (AT&T) subscribers at 11 million and 8.1 million, respectively).

142. As the Supreme Court noted,

MGM's evidence gives reason to think that the vast majority of users' downloads are acts of infringement, and because well over 100 million copies of the software in

screen name of an individual user . . . [and] trace the user to his ISP," only the ISP can provide the user's real identity.¹⁴³ To aid copyright holders in identifying the infringer, the DMCA includes a subpoena provision.¹⁴⁴ Although the provision is still applicable where the ISP is "storing on its servers material that is infringing or the subject of infringing activity," circuit court decisions indicate that this is the only time that the provision will apply.¹⁴⁵ While the DMCA subpoena provision's use has been limited, "John Doe" suits make it possible for copyright holders to identify infringers without it.¹⁴⁶ Therefore, copyright holders may still identify direct infringers, obtain a judgment, and then use that judgment to get an injunction under the Foreign Site Provision.

While the use of "John Doe" suits makes it possible to identify direct infringers, the best way for a copyright holder to defend his copyright and use the foreign suit provision would be to simply find a volunteer who has infringed his copyright. Such an action would prevent any difficulties in proving direct infringement and is the same strategy successfully used in *Sony Corp. of America v. Universal City Studios, Inc.*¹⁴⁷

In *Sony*, Universal City Studios claimed that Sony's manufacture and distribution of VCRs constituted contributory and vicarious copyright infringement.¹⁴⁸ Proving either form of secondary

question are known to have been downloaded, and billions of files are shared each month, the probable scope of copyright infringement is staggering.

Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 923 (2005).

143. *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1232 (D.C. Cir. 2003).

144. 17 U.S.C. § 512(h) (2005) (providing that "[a] copyright owner . . . may request the . . . district court to issue a subpoena to a service provider for identification of an alleged infringer").

145. *Verizon*, 351 F.3d at 1233 (declining to hold that § 512(h) authorizes issuance of a subpoena "to an ISP that transmits infringing material but does not store any such material on its servers"); see also *In re Charter Commc'ns, Inc.*, Subpoena Enforcement Matter, 393 F.3d 771, 777 (8th Cir. 2005) (adopting the reasoning of *Verizon*).

146. Louis Trager, *MPAA Seen Wielding Gentler Hand Than RIAA in File-Sharing Suit Campaign*, CONSUMER ELECTRONICS, June 8, 2006 (noting that both the MPAA and the RIAA employ the "John Doe" subpoena to prosecute file-sharers). Through the "John Doe" litigation process, copyright holders file suit, and the court then issues a subpoena to the defendant's service provider to determine his identity. Nick Mamatas, *Meet John Doe*, VILLAGE VOICE, Mar. 9-15, 2005, available at http://www.villagevoice.com/music/0510_mamatas.61813.22.html (describing his experience as a "John Doe" defendant). In other words, the only difference in the process is that "[i]nstead of issuing a subpoena first to learn an infringer's identity, [a copyright holder] file[s] a lawsuit first and then issue[s] the subpoena subsequently." Recording Industry Association of America, *Frequently Asked Questions about the Recording Industry's Use of "John Doe" Lawsuits*, http://www.riaa.com/news/newsletter/012104_faqs.asp (last visited Feb. 23, 2007).

147. *Sony Corp. of Am. v. Universal City Studios, Inc.*, 480 F. Supp. 429, 437 (C.D. Ca. 1979), *rev'd*, 659 F.2d 963 (9th Cir. 1981), *aff'd*, 464 U.S. 417 (1984).

148. *Id.* at 432.

liability required a showing of direct infringement, which was difficult for Universal to demonstrate.¹⁴⁹ To solve the problem of locating a direct infringer, Universal's law firm contacted one of its clients, William Griffiths, to be a nominal defendant in the case.¹⁵⁰ It would work as follows: "Griffiths would be named in the court papers, he would be called to testify about his activities as a taper, and the court, if Universal had its way, would find him guilty of copyright infringement; but Universal would promise, up front, not to seek any damages from him."¹⁵¹ Griffiths made it possible for Universal to "establish a chain of responsibility from consumer to retailer and on to advertiser, distributor, and, ultimately, manufacturer."¹⁵²

Just like in *Sony*, finding an online direct infringer could be time-consuming—something which could be financially prohibitive to a copyright holder. Therefore, finding a direct infringer who will volunteer to be sued in exchange for a waiver of any claim for damages is extremely valuable. If a copyright holder finds someone who will admit to infringing a copyrighted work through a particular foreign service, the copyright holder could quickly obtain a judgment and block the site. With protection from monetary liability for past infringement, it is not difficult to imagine direct infringers coming forward and admitting to the illegal use of foreign sites.¹⁵³ The use of direct infringers as nominal defendants will make it possible to block sites more quickly and thus limit the site's effect on the U.S. market.

B. Which Sites Copyright Holders May Block with § 512(j)(1)(B)(ii)

The Foreign Site Provision was written before the advent of peer-to-peer services. As a result, it does not apply well to all peer-to-peer technology. Nonetheless, it could be used to block centralized peer-to-peer systems, pay websites, and sites offering the software for decentralized peer-to-peer systems. The Foreign Site Provision applies to "specific, identified, online locations," so it would be applicable to

149. JAMES LARDNER, FAST FORWARD: HOLLYWOOD, THE JAPANESE, AND THE ONSLAUGHT OF THE VCR 32 (1987) (detailing the efforts of a private investigator to observe the direct infringement of Universal's copyrighted works).

150. *Id.*

151. *Id.*

152. *Id.* at 33.

153. Although it came under fire and was ultimately ended, 1108 people participated in the Recording Industry Association of America's "Clean Slate" program. Participants "acknowledge[d] in writing that they shared music files online and then remove[d] the files from their computers. In exchange, the RIAA pledged not to target them in its lawsuit campaign." Alex Veiga, *Recording Industry Drops Amnesty Program for File-Sharers*, USA TODAY, Apr. 20, 2004, http://www.usatoday.com/tech/webguide/music/2004-04-20-clean-slate-dropped_x.htm.

peer-to-peer systems that operate with a centralized server.¹⁵⁴ While such technology seems to have disappeared with the folding of Napster, should anyone try to use it again in a foreign country, the Foreign Site Provision would be able to block it. Additionally, the Foreign Site Provision would work to block pay websites, such as AllofMP3.com, where the infringing files are located on the service provider's servers. Therefore, the Foreign Site Provision could be used to block access to many infringing foreign sites, but it could not be used to block a decentralized peer-to-peer service.

Decentralized peer-to-peer services do not have a "specific, identified, online location," as such systems run off of all users' computers.¹⁵⁵ Thus, the Foreign Site Provision cannot be used to block the most current file-sharing technology when in use. For this reason, the Foreign Site Provision is only applicable to decentralized peer-to-peer systems if it is used to block the site on which the file-sharing software is being offered.

As the decentralized file-sharing software at issue would be used largely for infringement, it is to be assumed that its distributor would be located in a foreign country where he can avoid the imposition of secondary liability by U.S. courts. While being in a foreign country does not require that the distributor use a foreign server for his software downloading site, use of a U.S. server would subject the distributor to U.S. jurisdiction and all other applicable U.S. copyright law. Therefore, the software for foreign infringing peer-to-peer services will likely be located at a "specific, identified, online location outside the United States."¹⁵⁶

To use the Foreign Site Provision to block the site offering the infringing software would require showing direct infringement through the use of the software obtained from that site. Once direct infringement has been proven, the copyright holder may show that transmission of the software through the service provider will result

154. 17 U.S.C. § 512(j)(1)(B)(ii) (2005).

155. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 922 (2005) ("Grokster and StreamCast use no servers to intercept the content of the search requests or to mediate the file transfers conducted by users of the software, there being no central point through which the substance of the communications passes in either direction.").

156. § 512(j)(1)(B)(ii).

in further infringement and should thus be blocked through the use of the Foreign Site Provision.¹⁵⁷

From the language of the DMCA it appears that a copyright holder would not need to show that the site offering the software is liable for its involvement with the direct infringement. The provision is concerned with stopping direct infringement.¹⁵⁸ Thus, a showing of direct infringement facilitated by a particular website might be sufficient to block the site.

Difficulty should not arise even if a court were to require that the site be liable in some manner in order to be blocked. Infringing services have located overseas to avoid the imposition of liability. Therefore, it is doubtful that they would enter U.S. courts to defend against a copyright holder's claim of inducement to infringe copyrights, contributory liability, or vicarious liability. Copyright holders can make these claims, show that these software-providing sites bring about infringement, and succeed in having them blocked under the Foreign Site Provision.

The holding in *Grokster* permits the attachment of liability for one who induces copyright infringement, which would be an easy argument to apply to a site offering a service used widely for infringement.¹⁵⁹ Should the requisite affirmative steps of inducement not be present, a finding of contributory liability would not be difficult in this context. Imposition of contributory liability will be easier than in *Sony*, because *Sony's* requirement that the service have substantial non-infringing uses is not applicable.¹⁶⁰ Direct infringement through the use of the software is all that is necessary to block the site, as the only consideration of the effect of the Foreign Site Provision on non-infringing content is seen in § 512(j)(2)(C). Focusing on the technical feasibility and effectiveness of an injunction, § 512(j)(2)(C) requires an examination of whether blocking a foreign site will "interfere with access to non-infringing material at other online locations." As the DMCA only concerns itself with the non-infringing material at *other* online locations, it plainly indicates that it does not concern itself with non-infringing material at the blocked location.¹⁶¹ As such, the fact

157. The DMCA could be found applicable to these sites either because they transmit a file known to facilitate copyright infringement, § 512(a), or because providing the software is essentially the same as providing an information location tool, § 512(d).

158. See § 512(a)-(d).

159. *Grokster*, 545 U.S. at 919 ("[O]ne who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement of third parties.").

160. *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984).

161. *TRW Inc. v. Andrews*, 534 U.S. 19, 28 (2001) ("Congress implicitly exclude[s] a general . . . rule by explicitly including a more limited one.").

that non-infringing content exists on a peer-to-peer service will not prevent the blocking of a site which offers the service's software.¹⁶² Finally, vicarious liability could also be applied because the site offering the software is often operated by the owner of the software. As such, the owner receives a direct financial benefit from selling advertisements on his software and on the site on which it is offered.¹⁶³ Further, he would have the right and ability to supervise conduct because he is placing the product online for download. Thus, the Foreign Site Provision may be used to block centralized peer-to-peer systems, pay websites, and sites offering the software for decentralized peer-to-peer systems.

VI. CONCLUSION

Despite the liability that may be imposed on illegal downloaders in the United States, they will continue to download and infringe.¹⁶⁴ Although rights holders can file suit against these direct infringers, the suits affect only a small portion of the total number of infringers in the United States.¹⁶⁵ As such, the problem of illegal downloading persists. To protect their content, copyright holders have turned to the courts in an effort to shut down the sites that make it possible for such widespread infringement. Recent judicial decisions¹⁶⁶ protecting copyrights have forced infringing sites to close, operate legally, or go abroad.¹⁶⁷ This foreign relocation of infringing websites

162. The capability of noninfringing uses would be relevant only if a case were brought against the service itself and/or the site offering the program for such noninfringing uses.

163. In fact, the Ninth Circuit, in *Napster*, found direct financial benefit even without a current revenue stream. *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023 (2001). The Ninth Circuit affirmed the district court's finding that "Napster's future revenue is directly dependent upon 'increases in userbase.'" *Id.*

164. Saul Hansell, *Putting the Napster Genie Back in the Bottle*, N.Y. TIMES, Nov. 20, 2005, § 3, at 7 (stating that there is not "much impetus for hard-core users to start paying for their music").

165. The RIAA has filed 17,100 lawsuits against direct infringers between September 2003 and December 2005. "In October [of 2005 alone], members of 5.7 million U.S. households downloaded at least one unauthorized song using P-to-P services." Grant Gross, *RIAA Files New Round of Lawsuits, P-to-P Use Down*, INFO WORLD DAILY, Dec. 15, 2005, http://www.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/05/12/15/HNriaalawsuits_1.html&source=searchresult. While the suits may be argued to have a deterrent effect (as members of 6.4 million households illegally downloaded in June 2005, *id.*, they are still the equivalent of a band-aid on a chest wound).

166. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 941 (2005); *Napster*, 239 F.3d at 1022.

167. Brian Deagon, *File-Share Services Can Be Held Liable For Illegal Copying; Supreme Court Rules 9-0; Music, Movie Giants Win Landmark Case over Firms Aiding Copyright Violators*, INVESTOR'S BUSINESS DAILY, June 28, 2005, at A01 ("file sharing is not going to go away. The [*Grokster*] decision has no effect on the hundreds of foreign providers of P2P

puts copyright holders at continued risk of massive infringement of their works.

The Foreign Site Provision may be used to stop the U.S. infringement that occurs through the use of foreign sites and services. Interpreted correctly, the provision may be used to block infringing sites as well as those that offer the programs used to infringe. After obtaining a judgment against just one direct infringer, a copyright holder may have a service provider enjoined from providing access to the infringing site.¹⁶⁸ While blocking an infringing site will not stop copyright infringement through that site worldwide, it will stop infringement through that site in the United States, where 2005 album sales were at their lowest level since 1996.¹⁶⁹

The Foreign Site Provision will not solve all the problems of copyright holders. Aside from handling continued worldwide infringement, copyright holders using the Foreign Site Provision will undoubtedly face unfounded claims of censorship and damage to innovation from their actions. Nonetheless, the provision was written to protect copyrighted works and should be used accordingly. Copyright holders have yet to hesitate in using the courts to protect their works. Every successful suit alters the landscape for infringers and their services. Suits have changed peer-to-peer file-sharing from centralized to decentralized to foreign-based. While the infringing sites continue to exist, the methods of delivering infringing content to users are dwindling. The Foreign Site Provision is the next step in this ongoing fight against digital piracy and copyright holders should take it.

*Todd Ryan Hambidge**

software.”); Alex Veiga, *Lords of File-Sharing Going Legit or Out*, Jan. 4, 2006, <http://www.law.com/jsp/article.jsp?id=1136282707979> (“[S]everal Napster heirs have shut down and others are contemplating what they once couldn’t abide—doing business by the entertainment industry’s rules to survive.”).

168. However, for such an injunction to occur, the court would have to weigh the considerations of 17 U.S.C. § 512(j)(2) (2005) in favor of the copyright holder.

169. Rhys Blakely, *Fight against Internet Music Piracy Hits Fans on the Move*, TIMES (UK), Feb. 11, 2006, at 36 (including digital downloads in the total figure). While the number of albums sold continues to decline (2006 saw an additional 4.9% decline from 2005), the sale of digital singles increased overall music sales by over nineteen percent from 2005. *Album Sales Continue Fall, Downloads Climb*, MSNBC, Jan. 5, 2007, <http://www.msnbc.msn.com/id/16474850/>.

* J.D. Candidate, May 2007, Vanderbilt University Law School. I would like to thank the many members of the Law Review whose work made publication of this Note possible.
