

Train in Vain: The Clash Between the RIAA and the Eighth Circuit over Whether the DMCA Subpoena Provision Applies to Peer-to-Peer Networks, and the Need to Steer the DMCA Back on Track with Congressional Intent
[In re Charter Commc'ns, Inc., Subpoena Enforcement Matter, 393 F.3d 771 (8th Cir. 2005)]

Zach Chaffee-McClure*

*Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by . . . new technology.*¹

I. INTRODUCTION

While Internet piracy has cost the entertainment industry billions of dollars, the toll it has taken on Congress is best measured in units of frustration.² Internet piracy has proven difficult to thwart, leading Congress to pursue a variety of unorthodox solutions, including legislation that would allow copyright holders to hack infringers' personal computers,³ requests that the Department of Justice prosecute infringers,⁴ and intimations that piracy is terrorism.⁵

In 1998, Congress sought to terrorize Internet piracy by passing the Digital Millennium Copyright Act (DMCA),⁶ a comprehensive and controversial piece of copyright legislation.⁷ Among its many provisions, the DMCA allows a copyright holder to issue a subpoena that compels an Internet service provider (ISP) to disclose an alleged

* B.A. 2003, Kansas State University; J.D. Candidate 2007, Washburn University School of Law. The author is grateful to the editors of the *Washburn Law Journal*, particularly Jenny Williams, for their guidance and to the Chaffee-McClures for their love.

1. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 431 (1984).

2. Peter K. Yu, *The Escalating Copyright Wars*, 32 HOFSTRA L. REV. 907, 907-08 (2004).

3. *Id.* at 908 (describing the self-help measures for copyright holders proposed in H.R. 5211, 107th Cong. (2002)).

4. Benny Evangelista, *Casting a Wider Net: Recording Industry May Target Individuals in Online Piracy Battles*, S.F. CHRON., Aug. 26, 2002, at E1, available at <http://www.sfgate.com/cgi-bin/article.cgi?f=/C/a/2002/08/26/BU150108.DTL>.

5. *International Copyright Piracy: A Growing Problem with Links to Organized Crime and Terrorism: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Property of the H. Comm. on the Judiciary*, 108th Cong. 1 (Mar. 13, 2003).

6. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.).

7. For a controversial appraisal of the DMCA, see Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813 (2001). See also Yu, *supra* note 2, at 908 (characterizing the DMCA as an entertainment industry trophy).

copyright infringer's identity.⁸ The emergence of new technology has since enhanced the significance of this subpoena authority.

Today, Internet piracy commonly occurs on peer-to-peer (P2P) networks.⁹ A P2P network allows Internet users to transmit data to one another without an intermediary, permitting file-sharing directly from one home computer to another.¹⁰ This framework affords P2P network users considerable anonymity, in part because a copyright holder cannot identify a network user without the cooperation of that user's ISP.¹¹ The roster of P2P networks includes popular services like Napster, Grokster, iMesh, KaZaA, and Morpheus.¹² Approximately 10,000,000 Internet users are logged on P2P networks at any given time, sharing more than 10,000,000 gigabytes of data.¹³ In total, P2P exchanges account for sixty to eighty percent of public Internet traffic.¹⁴ The vast majority of that shared data is copyrighted material.¹⁵

In 2003, the Recording Industry Association of America (RIAA) began a campaign to stop music piracy on P2P networks.¹⁶ As part of this effort, the RIAA attempted to use the subpoena provision of the DMCA to circumvent the intrinsic anonymity of P2P networks.¹⁷ Not all ISPs cooperated with the RIAA's scheme to identify P2P network users.¹⁸ One dispute arose from the RIAA's attempt to learn the identities of various subscribers to the broadband Internet service offered by Charter Communications, Inc. (Charter).¹⁹ In *In re Charter Communications, Inc., Subpoena Enforcement Matter*,²⁰ Charter objected to the subpoenas, arguing that the DMCA allowed courts to

8. 17 U.S.C. § 512(h) (2000). An ISP offers Internet access and related services to consumers. § 512(k)(1).

9. Yu, *supra* note 2, at 921 (placing the number of Recording Industry Association of America lawsuits against P2P network users at over 2,000).

10. Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1232 (D.C. Cir. 2003); *In Praise of P2P*, ECONOMIST TECH. Q., Dec. 4, 2004, at 35, available at http://www.economist.com/displayStory.cfm?Story_id=3422905.

11. *Verizon*, 351 F.3d at 1232.

12. Peter K. Yu, *P2P and the Future of Private Copying*, 76 U. COLO. L. REV. 653, 676 (2005).

13. Press Release, CacheLogic, CacheLogic Announces New Internet Analysis Platform, Provides Exclusive Data on Worldwide P2P Usage (July 15, 2004), available at <http://www.cache logic.com/news/pr040715.php>.

14. Joanna Glasner, *P2P Fuels Global Bandwidth Binge*, WIRED NEWS, Apr. 14, 2005, <http://www.wired.com/news/business/0,1367,67202,00.html>.

15. MGM Studios, Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2772 (2005) (noting plaintiff's evidence that ninety percent of the content on the FastTrack P2P network is copyrighted); *In re Charter Commc'ns, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 773 (8th Cir. 2005) (claiming that ninety percent of the content on P2P networks is copyrighted).

16. Steve Knopper, *RIAA Will Keep on Suing*, ROLLING STONE, June 9, 2005, http://www.rollingstone.com/news/story/_/id/7380412.

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

18. *See, e.g., id.* at 1231.

19. *In re Charter*, 393 F.3d at 773.

20. 393 F.3d 771 (8th Cir. 2005).

issue subpoenas only to ISPs that store the data that is the subject of the subpoena, not an ISP like Charter that serves as a mere conduit for the transmission of data between two computers.²¹ The district court rejected Charter's protest and ordered Charter to comply with the subpoenas.²² On appeal, the United States Court of Appeals for the Eighth Circuit endorsed Charter's objection and adopted the interpretation of the DMCA first announced in *Recording Industry Ass'n of America v. Verizon Internet Services, Inc.*,²³ thereby reversing the district court.²⁴

The Eighth Circuit erred in adopting the *Verizon* interpretation of the DMCA.²⁵ The court incorrectly held that the subpoena provision of the DMCA does not apply to an ISP that transmits but does not store copyrighted data.²⁶ The court should have recognized that a court may issue a DMCA subpoena to any ISP, so long as notification is adequate. Contrary to the flawed statutory analysis of *Verizon*, notification can be adequate with regard to a conduit ISP.²⁷ By adopting the restrictive view of the DMCA subpoena provision announced in *Verizon*, the court limited copyright protection in a manner inconsistent with the language and spirit of the DMCA.²⁸

II. CASE DESCRIPTION

In June 2003, the RIAA embarked on a nationwide effort to protect its members' copyrighted works from illegal Internet file-sharing via P2P networks.²⁹ RIAA employees logged on to P2P networks, tracked copyrighted files available on those networks, and downloaded the files to verify their content.³⁰ As a result, the RIAA discerned the user names and IP addresses of approximately 200 Charter subscribers whom the RIAA suspected of infringing activity.³¹ The RIAA alleged that just ninety-three of those subscribers shared over 100,000 copyrighted recordings.³²

21. *Id.* at 775. Charter also made constitutional objections. *Id.* at 777.

22. *Id.* at 774.

23. 351 F.3d 1229 (D.C. Cir. 2003).

24. *In re Charter*, 393 F.3d at 773.

25. *See id.* at 777. "We agree with and adopt the reasoning of the United States Court of Appeals for the District of Columbia Circuit in *Verizon . . .*" *Id.*

26. *Id.*

27. *See Verizon*, 351 F.3d at 1237 (holding that a court may not issue a subpoena to a conduit ISP).

28. *See In re Charter*, 393 F.3d at 777 (adopting the *Verizon* interpretation of the DMCA subpoena provision).

29. *Id.* at 774.

30. *Id.*

31. *Id.* Every computer that sends or receives data on the Internet has an IP address, a unique number used to identify a particular computer. Webopedia, IP address, http://www.webopedia.com/TERM/I/IP_address.html (last visited Sept. 5, 2005).

32. *In re Charter*, 393 F.3d at 779 (Murphy, J., dissenting).

After filing a request with the clerk of the district court, the RIAA obtained subpoenas demanding that Charter disclose the names, home addresses, telephone numbers, and e-mail addresses of the suspected infringers.³³ Charter moved to quash the subpoenas.³⁴ In response to Charter's motion to quash, the United States District Court for the Eastern District of Missouri ordered Charter to provide all the requested information except the telephone numbers.³⁵ Charter filed a notice of appeal and a motion to stay the district court's order compelling Charter to comply with the subpoenas.³⁶ The district court did not act on the motion to stay before the deadline for complying with the subpoenas.³⁷ As a result, on November 21, 2003, the deadline for compliance, Charter filed an emergency motion to stay, which the circuit court denied.³⁸ Charter complied with the subpoenas and pursued an appeal.³⁹

On appeal, Charter raised five issues.⁴⁰ Charter argued that § 512(h) of the DMCA only applies to ISPs that store copyrighted material, not ISPs like Charter that act merely as a conduit for the transmission of copyrighted material between Internet users.⁴¹ The Eighth Circuit held in favor of Charter on this issue, adopting the *Verizon* interpretation of the DMCA and reversing the decision of the district court.⁴² As a result, the court remanded the case to the district court, instructing it to order the RIAA to return all information obtained via the subpoenas.⁴³

III. BACKGROUND

Much litigation has surrounded the DMCA subpoena provision. Courts evaluating the subpoena provision have considered the legislative history of the DMCA, the structure of the DMCA, and other jurisdictions' interpretations of the DMCA.

33. *Id.* at 774 (majority opinion).

34. *Id.*

35. *Id.*

36. *Id.*

37. *Id.*

38. *Id.*

39. *Id.* at 774-75.

40. Appellant's Opening Brief at iii-iv, *In re Charter*, 393 F.3d 771 (No. 03-3802).

41. *In re Charter*, 393 F.3d at 775. The majority did not address the remaining issues, and they are not a focus of this comment. The four remaining issues were (1) whether there was a case or controversy to support the subpoenas; (2) whether a subpoena pursuant to § 512(h) violates the privacy protections of the *Communications Act of 1934*; (3) whether § 512(h) violates Internet users' First Amendment rights; and (4) whether compliance with a § 512(h) subpoena requires an ISP to disclose users' e-mail addresses. Appellant's Opening Brief at iii-iv, *In re Charter*, 393 F.3d 771 (No. 03-3802).

42. *In re Charter*, 393 F.3d at 773.

43. *Id.* at 778.

A. *Legislative History of the DMCA*

When contemplating the DMCA, Congress knew of the widespread nature of Internet piracy.⁴⁴ Nonetheless, Congress did not anticipate the massive piracy that occurs today on P2P networks, as Congress enacted the DMCA before P2P networks became ubiquitous.⁴⁵ Congress was aware, however, of piracy that occurred on technological precursors to today's P2P networks.⁴⁶

In light of widespread piracy, the DMCA's twin motives were to facilitate copyright enforcement and to protect ISPs from indirect liability resulting from their customers' infringing acts.⁴⁷ To facilitate copyright enforcement, the DMCA allows a copyright holder to obtain a subpoena requiring an ISP to reveal the identity of an Internet user suspected of infringement.⁴⁸ Section 512(h)(1) provides that "[a] copyright owner . . . may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer."⁴⁹ On the other hand, Congress protected ISPs by providing certain ISPs immunity from liability.⁵⁰ These shelters, commonly known as the four safe harbor provisions, were victories for ISPs fearing costly liability.⁵¹

B. *Structure of the DMCA*

The DMCA establishes four types of safe harbors, each shielding ISPs from indirect liability that otherwise might result from a particular type of common ISP function.⁵² Section 512(a) protects ISPs from liability for "transmitting, routing, or providing connections for" in-

44. *Id.* at 782 (Murphy, J., dissenting). "The intent of Congress in enacting the DMCA was to address 'massive piracy' of copyrighted works over digital networks . . ." *Id.* (quoting S. REP. NO. 105-190, at 8 (1998)).

45. *Id.* at 773-74 (majority opinion); Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1238 (D.C. Cir. 2003).

46. See, e.g., *Copyright Piracy, and H.R. 2265, The No Electronic Theft (NET) Act: Hearing Before the Subcomm. on Courts and Intellectual Property of the H. Comm. on the Judiciary, 105th Cong. 17-18 (1997)* (statement of Kevin DiGregory, Deputy Assistant Att'y Gen., Department of Justice). Throughout the 1990s, Congress heard testimony about the use of file transfer protocol sites, electronic bulletin board services, and e-mail distribution lists for the purpose of illegally disseminating copyrighted works. *Id.*

47. *ALS Scan, Inc. v. RemarQ Cmty., Inc.*, 239 F.3d 619, 625 (4th Cir. 2001) (citing H.R. REP. NO. 105-796, at 72 (1998) (Conf. Rep.); H.R. REP. NO. 105-551, pt. 1, at 11 (1998)).

48. 17 U.S.C. § 512(h) (2000).

49. § 512(h)(1).

50. § 512(a)-(d). To qualify for immunity, an ISP must perform one of the functions described in subsections (a)-(d). Section 512(a) protects ISPs that merely transmit data; § 512(b) protects ISPs that provide caching services; § 512(c) protects ISPs that store data at the direction of users; and § 512(d) protects ISPs that provide information location tools. *Id.*

51. Jennifer Bretan, Note, *Harboring Doubts About the Efficacy of § 512 Immunity Under the DMCA*, 18 BERKELEY TECH. L.J. 43, 45-46 (2003). The court in *Charter* considered § 512(e) "[a] fifth safe harbor," one available to ISPs that are nonprofit educational institutions. *In re Charter Commc'ns, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 775 n.4 (8th Cir. 2005).

52. § 512(a)-(d).

fringing material.⁵³ Courts commonly refer to this provision as the safe harbor for conduit ISPs.⁵⁴ Sections 512(b) through (d) protect ISPs that store the data that is the subject of a subpoena request.⁵⁵ These three safe harbors for storage ISPs each make immunity from liability contingent upon the ISP promptly removing or disabling access to any infringing material once notified of the infringing material's location.⁵⁶ In contrast, § 512(a) does not predicate immunity on a conduit ISP removing or disabling access to infringing material.⁵⁷

Section 512(c)(3)(A), located within one of the safe harbors for storage ISPs, describes the requirements for adequate notification.⁵⁸ Courts commonly refer to this subsection as the notification provision.⁵⁹ A satisfactory notification "includes substantially"⁶⁰ six elements: (i) the signature of a person who can act on behalf of a copyright owner; (ii) a representative list of the works that are the subject of infringement; (iii) information sufficient to allow the ISP to locate and remove the infringing material; (iv) information sufficient to allow the ISP to contact the copyright holder; (v) a statement of good faith belief that the infringing use is not authorized; and (vi) a statement assuring the accuracy of the notification information.⁶¹ Although the notification provision lies within one of the safe harbors for storage ISPs, various provisions of § 512, including the subpoena provision, reference the notification provision.⁶² Because a storage ISP that wishes to benefit from one of the applicable safe harbors must remove or disable access to infringing material to maintain its immunity, the notification elements provide the ISP with enough information to locate and remove the material.⁶³

Section 512(h) is the subpoena provision.⁶⁴ It provides that "[a] copyright owner . . . may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection."⁶⁵ An ISP must respond to a subpoena by "expeditiously disclos[ing] . . . information sufficient to identify the alleged infringer of the material de-

53. § 512(a).

54. *See, e.g., In re Charter*, 393 F.3d at 775.

55. *Id.* at 777. For a description of the safe harbors, see *supra* note 50.

56. § 512(b)(2)(E), (c)(1)(C), and (d)(3).

57. § 512(a).

58. *In re Charter*, 393 F.3d at 775.

59. *E.g., id.*

60. § 512(c)(3)(A).

61. § 512(c)(3)(A)(i)-(vi).

62. *E.g., § 512(b)(2)(E); § 512(h)(2)(A).*

63. *In re Charter*, 393 F.3d at 776. "[T]he notification provision allow[s] an ISP . . . to remove or disable access to infringing material and thereby protect itself from liability." *Id.*

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

65. § 512(h)(1).

scribed in the notification.”⁶⁶ Before a court may issue a subpoena, the subpoena request must satisfy the notification provision discussed above.⁶⁷

Section 512(k)(1) defines a “service provider.”⁶⁸ For purposes of § 512, the meaning of the term depends upon the subsection in which it lies.⁶⁹ In § 512(a), the safe harbor for conduit ISPs, “service provider” means strictly an ISP that acts as a conduit for data.⁷⁰ For all other subsections, “service provider” assumes a broader meaning that encompasses conduit ISPs and storage ISPs.⁷¹

C. Courts’ Interpretations of the DMCA

The issue of whether the subpoena provision of the DMCA applies to conduit ISPs first arose in two companion cases referred to as *In re Verizon Internet Services, Inc.*⁷² In these two cases the RIAA used the DMCA to seek the identities of Internet users suspected of copyright infringement.⁷³ Verizon, the ISP that received the subpoenas, questioned the subpoenas’ validity.⁷⁴ The district court upheld the subpoenas.⁷⁵ The Court of Appeals for the District of Columbia Circuit reversed, thereby becoming the first court to hold that § 512(h) subpoenas do not reach conduit ISPs.⁷⁶ In so holding, the D.C. Circuit reasoned that a DMCA subpoena request must meet the notification provision of § 512(c)(3)(A).⁷⁷ The court agreed with Verizon that the RIAA subpoenas did not meet one of the notification

66. § 512(h)(3).

67. § 512(h)(4) (requiring that the clerk of the court issue a subpoena “[i]f the notification filed satisfies the provisions of subsection (c)(3)(A)”). The subpoena request must also include a proposed subpoena and “a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.” § 512(h)(2)(B)-(C).

68. § 512(k)(1).

69. *Id.*

70. § 512(k)(1)(A).

As used in subsection (a), the term “service provider” means 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.

Id.

71. § 512(k)(1)(B). “As used in this section, other than subsection (a), the term ‘service provider’ means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).” *Id.*

72. *Recording Indus. Ass’n of Am. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1229-30 (D.C. Cir. 2003) (consolidating *In re Verizon Internet Servs., Inc., Subpoena Enforcement Matter*, 257 F. Supp. 2d 244 (D.D.C. 2003) and *In re Verizon Internet Servs., Inc., Subpoena Enforcement Matter*, 240 F. Supp. 2d 24 (D.D.C. 2003)).

73. *Id.* at 1231.

74. *Id.*

75. *Id.*

76. *Id.*

77. *Id.* at 1234-35.

elements.⁷⁸ It therefore ordered the district court to quash the subpoenas.⁷⁹

After the *Verizon* interpretation spread beyond the D.C. Circuit in *Charter*, an identical statutory issue arose in *In re Subpoena to University of North Carolina at Chapel Hill*.⁸⁰ The Middle District of North Carolina concurred with *Verizon* and *Charter*.⁸¹ The court held that the DMCA subpoena power reached storage ISPs but that authorizing subpoenas to conduit ISPs “would necessarily amount to the rewriting of the statute.”⁸² The court also indicated that it had reservations about the constitutional issues raised by § 512(h) subpoenas in general.⁸³ Accordingly, the court ordered the subpoenas quashed.⁸⁴

The United States Court of Appeals for the Fourth Circuit analyzed the notification provision in *ALS Scan, Inc. v. RemarQ Communities, Inc.*⁸⁵ In that case, ALS Scan, Inc. (ALS) informed a storage ISP that ALS’s copyrighted images resided within folders on the ISP’s newsgroups.⁸⁶ The ISP argued that ALS failed to satisfy § 512(c)(3)(A)(ii) and (iii).⁸⁷ The ISP argued that merely specifying the location of copyrighted images on the ISP’s newsgroups neither provided a representative list of copyrighted works claimed to be infringed, as required by notification element (ii), nor identified the works with enough detail to allow the ISP to remove them, as required by notification element (iii).⁸⁸ The Fourth Circuit agreed that ALS technically did not comply with the notification provision.⁸⁹ Nevertheless, the Fourth Circuit held that ALS provided “notice equivalent to” the information required by the notification provision and that ALS therefore substantially satisfied all necessary elements.⁹⁰

IV. COURT’S DECISION

In *Charter*, the Eighth Circuit considered whether the subpoena provision of the DMCA applies to an ISP that transmits infringing

78. *Id.* at 1236. The D.C. Circuit held that the RIAA subpoenas did not meet the notification element located in § 512(c)(3)(A)(iii) because a conduit ISP cannot “remove” or “disable access to” material not stored on that ISP’s computers. *Id.* at 1235-36.

79. *Id.* at 1239.

80. 367 F. Supp. 2d 945 (M.D.N.C. 2005).

81. *Id.* at 955-56.

82. *Id.* at 953.

83. *Id.* at 954.

84. *Id.* at 958.

85. 239 F.3d 619 (4th Cir. 2001).

86. *Id.* at 620-21. Online newsgroups are forums “organized by topic, enabl[ing] subscribers to participate in discussions on virtually any topic.” *Id.* at 620.

87. *Id.* at 624.

88. *Id.*

89. *Id.* at 625.

90. *Id.*

data but does not store it.⁹¹ Charter argued that the DMCA allows a court to issue a subpoena only to an ISP that stores infringing data.⁹² The RIAA argued that the DMCA allows a court to issue a subpoena to any ISP, regardless of whether the ISP stores infringing data.⁹³ The court agreed with Charter and held that the DMCA allows a court to issue a subpoena only to an ISP that stores infringing data.⁹⁴

A. Parties' Arguments

1. Charter Communications, Inc.

Charter argued that the district court lacked subject matter jurisdiction to issue or enforce the subpoenas because § 512(h) only applies to ISPs that store copyrighted material.⁹⁵ Charter relied on the *Verizon* holding to assert that a copyright holder could only satisfy the notification provision when the ISP stores the infringing data.⁹⁶ Because § 512(h) requires notification pursuant to § 512(c)(3)(A) before a court may issue a subpoena, Charter argued that a court can never issue a subpoena to an ISP that does not store the data that is the subject of the subpoena.⁹⁷

Charter contended that a copyright holder cannot obtain a subpoena unless the ISP receives notification of the alleged infringement under § 512(c)(3)(A).⁹⁸ To support this assertion, Charter noted that § 512(h) refers to the notification provision three times.⁹⁹ Section 512(h)(2) provides that the subpoena request must include “a copy of a notification described in subsection (c)(3)(A).”¹⁰⁰ Section 512(h)(4) provides that the clerk of the court may only issue the subpoena if “the notification filed satisfies the provisions of subsection (c)(3)(A).”¹⁰¹ Lastly, § 512(h)(5) provides that an ISP must respond to a subpoena only after “receipt of a notification described in subsection (c)(3)(A).”¹⁰²

Charter further argued that the notification elements of § 512(c)(3)(A) prevent a court from issuing a subpoena when the ISP does not store the infringing data.¹⁰³ Charter noted that adequate notification must identify the infringing material “that is to be removed

91. *In re Charter Commc'ns, Inc.*, Subpoena Enforcement Matter, 393 F.3d 771, 772 (8th Cir. 2005).

92. Appellant's Opening Brief at 15, *In re Charter*, 393 F.3d 771 (No. 03-3802).

93. Brief of Appellee at 21, *In re Charter*, 393 F.3d 771 (No. 03-3802).

94. *In re Charter*, 393 F.3d at 776-77.

95. Appellant's Opening Brief at 14, *In re Charter*, 393 F.3d 771 (No. 03-3802).

96. *Id.* at 15.

97. *Id.*

98. *Id.*

99. *Id.* at 17.

100. 17 U.S.C. § 512(h)(2) (2000).

101. § 512(h)(4).

102. § 512(h)(5).

103. Appellant's Opening Brief at 18, *In re Charter*, 393 F.3d 771 (No. 03-3802).

or access to which is to be disabled” and provide enough information “to permit the service provider to locate the material.”¹⁰⁴ According to Charter, a conduit ISP can neither locate nor remove data transmitted over a P2P network because the material suspected of infringement resides on the ISP users’ computers, not the ISP’s computers.¹⁰⁵ Charter claimed that it had no ability to control or examine the content of its subscribers’ computers, making location and removal impossible.¹⁰⁶

Charter anticipated that the RIAA would submit the same arguments as it did in *Verizon*, and Charter relied on *Verizon* to dismiss those arguments.¹⁰⁷ First, Charter argued that the court should not equate a conduit ISP’s ability to terminate an Internet user’s account with “disabling access” for purposes of § 512(c)(3)(A)(iii) because Congress considered account termination and disabling access distinct remedies.¹⁰⁸ Second, Charter contended that the RIAA’s subpoena request did not substantially comply with the notification provision because the subpoena request’s failure to identify the type of material described in § 512(c)(3)(A)(iii) exceeded mere technical error.¹⁰⁹ Third, Charter asserted that the structure of the DMCA supported restricting the subpoena power to storage ISPs because § 512(h) makes no reference to the safe harbor for conduit ISPs.¹¹⁰ Fourth, Charter argued that no assessment of the legislative intent that precipitated the DMCA should justify an interpretation that would controvert the language of § 512.¹¹¹

2. The Recording Industry Association of America

The RIAA argued that § 512(h) applies to all ISPs, regardless of the ISP’s role in the storage of the infringing data.¹¹² According to the RIAA, the DMCA defines a service provider to include conduit ISPs; a narrow interpretation of the subpoena provision would be nonsensical; the references to § 512(c)(3)(A) do not limit the scope of § 512(h); and Congress intended the DMCA to combat piracy on home computers.

The RIAA first argued that a service provider includes conduit ISPs.¹¹³ Section 512(h) contains no express limitations to the type of service provider for which a copyright holder may request a sub-

104. *Id.* (quoting § 512(c)(3)(A)(iii)).

105. *Id.*

106. *Id.* at 18-19.

107. *Id.* at 19.

108. *Id.*

109. *Id.* at 20.

110. *Id.*

111. *Id.* at 21.

112. Brief of Appellee at 21, *In re Charter*, 393 F.3d 771 (No. 03-3802).

113. *Id.* at 22.

poena.¹¹⁴ Therefore, the RIAA contended that the definition of service provider in § 512(k) should apply.¹¹⁵ Section 512(k) contains two definitions of service provider, a narrow one that defines the term solely with respect to § 512(a) and a broader one that applies to the remainder of § 512.¹¹⁶ The RIAA argued that because the broader definition applies to § 512(h), the subpoena power extends to all ISPs.¹¹⁷

The RIAA contended that interpreting “service provider” in § 512(h) to include all ISPs makes the most sense and best effectuates Congress’s intent.¹¹⁸ The RIAA argued that Congress designed the subpoena provision to allow copyright holders to sue infringing users directly.¹¹⁹ As such, the RIAA found no reason to make the subpoena power dependent upon the ISP exercising control over the data.¹²⁰ Additionally, the RIAA asserted that the DMCA could not curb piracy if the court prevented copyright holders from discovering the identity of infringing users when only the infringing user exercises control over the data.¹²¹ Because Charter’s interpretation would create this perverse result, the RIAA argued that the court should reject it.¹²²

The RIAA then targeted the foundation of Charter’s position, claiming that references to the notification provision do not restrict the scope of § 512(h).¹²³ The RIAA contended that notification allows a conduit ISP to identify the suspected Internet user, even though the ISP need not remove the infringing data.¹²⁴ Because § 512(h) demands only that an ISP disclose user information, which an ISP can do without having any control over the user’s data, the RIAA argued that an ISP must comply with a DMCA subpoena regardless of whether it can remove or disable access to the infringing data.¹²⁵ Moreover, the RIAA disputed Charter’s inability to locate infringing material not stored on its computers because an ISP can identify which user’s computer contains the data.¹²⁶ The RIAA also disputed Charter’s inability to disable access to infringing material by arguing

114. *Id.* at 22-23.

115. *Id.* at 23.

116. *Id.*; *see supra* notes 70 and 71.

117. Brief of Appellee at 24, *In re Charter*, 393 F.3d 771 (No. 03-3802).

118. *Id.* at 25.

119. *Id.*

120. *Id.*

121. *Id.* at 26.

122. *Id.* at 27.

123. *Id.* at 28.

124. *Id.* at 31.

125. *Id.*

126. *Id.* at 31-32.

that an ISP can terminate a user's account, thereby making it impossible for others to access that user's computer.¹²⁷

According to the RIAA, the legislative history resolved any ambiguity in the text of the DMCA in the RIAA's favor.¹²⁸ The RIAA alleged that, even if Congress did not anticipate P2P technology when it enacted the DMCA, the DMCA nevertheless applies to P2P networks.¹²⁹ The RIAA argued that Congress's awareness of precursors to P2P networks indicated that it foresaw the types of subpoenas at issue.¹³⁰ The RIAA also recognized that § 512(a), the safe harbor for conduit ISPs, demonstrated that Congress anticipated Internet users exchanging copyrighted information without ISPs engaging in intermediate storage of the data.¹³¹ The RIAA reasoned that Congress wrote the DMCA with future technologies in mind.¹³²

B. *Majority Opinion*

In a 2-1 decision, the Eighth Circuit held that copyright holders cannot satisfy the notification provision when serving a DMCA subpoena upon a conduit ISP; therefore, the DMCA does not allow courts to issue subpoenas to conduit ISPs.¹³³ The court began its analysis by scrutinizing the notification provision because a subpoena request must satisfy the notification elements.¹³⁴ The court noted that three of the safe harbor provisions, those applicable to ISPs that store copyrighted material, reference the notification provision.¹³⁵ To enjoy the protection of any of these three safe harbors, an ISP must respond to notification of infringement by removing or disabling access to the infringing material.¹³⁶ Therefore, the court concluded that "a specific purpose of the notification provision is to allow an ISP . . . the opportunity to remove or disable access to infringing material and thereby protect itself from liability."¹³⁷

The court observed that § 512(a), the safe harbor that protects conduit ISPs, makes no reference to the notification provision.¹³⁸ The court rationalized this omission with the view that a conduit ISP cannot remove or disable access to infringing material stored on users'

127. *Id.* at 33.

128. *Id.* at 37.

129. *Id.* at 38.

130. *Id.* at 39-40.

131. *Id.* at 39.

132. *Id.* at 38.

133. *In re Charter*, 393 F.3d at 776-77.

134. *Id.* at 775. "[N]otification is a mandatory part of the subpoena request and a condition precedent to the issuance of a subpoena." *Id.*

135. *Id.* at 776.

136. *Id.*

137. *Id.*

138. *Id.*

computers, so notification would serve no purpose.¹³⁹ According to the court, if a conduit ISP cannot remove the infringing data, then it should be no surprise that a conduit ISP's immunity does not hinge upon cooperation in the removal of the data.¹⁴⁰ Based on the text and structure of the DMCA, the court agreed with Charter that a court can only issue a subpoena when the ISP can locate and remove the infringing data.¹⁴¹ The court suggested that John Doe lawsuits could perform a function analogous to that of the DMCA subpoena provision when the DMCA does not apply.¹⁴²

The court also summarized the *Verizon* decision.¹⁴³ The D.C. Circuit held in *Verizon* that the DMCA does not authorize a court to issue subpoenas to a conduit ISP because a conduit ISP cannot remove or disable access to data stored on an Internet user's computer.¹⁴⁴ The court in *Charter* remarked that the RIAA's argument that terminating a user's account was equivalent to disabling access as contemplated by § 512(c)(3)(A)(iii) did not persuade the court in *Verizon*.¹⁴⁵ Likewise, the Eighth Circuit observed that the D.C. Circuit also rejected the RIAA's argument that it substantially complied with the notification provision.¹⁴⁶ The Eighth Circuit noted that the court in *Verizon* did not adopt the RIAA's argument that the broad definition of service provider located in § 512(k)(1)(B) should permit a broad subpoena power.¹⁴⁷ Rather, the court in *Verizon* discarded this assertion for "border[ing] upon the silly" because a subpoena issued to an ISP, however defined, would still have to comply with the notification provision.¹⁴⁸ *Charter* also summarized the *Verizon* position that, because the safe harbor for conduit ISPs does not reference the notification provision, the structure of the DMCA supports restricting subpoenas to storage ISPs.¹⁴⁹ The court subsequently approved the *Verizon* analysis.¹⁵⁰

139. *Id.* "The absence of the remove-or-disable-access provision (and the concomitant notification provision) makes sense where an ISP merely acts as a conduit for infringing material . . . because the ISP has no ability to remove the infringing material from its system or disable access to the infringing material." *Id.*

140. *Id.*

141. *Id.* at 776-77.

142. *Id.* at 775 n.3.

143. *Id.* at 777.

144. *Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1235 (D.C. Cir. 2003).

145. *In re Charter*, 393 F.3d at 777.

146. *Id.*

147. *Id.*

148. *Verizon*, 351 F.3d at 1236.

149. *In re Charter*, 393 F.3d at 777.

150. *Id.* "We agree with and adopt the reasoning of the United States Court of Appeals for the District of Columbia Circuit in *Verizon* as it pertains to this statutory issue." *Id.*

After endorsing the *Verizon* analysis, the court chose not to address Charter's constitutional objections to the subpoenas.¹⁵¹ Nevertheless, the court indicated that it might agree in part with Charter's constitutional objections.¹⁵² The court then remanded the case so that the district court could order the RIAA to make no use of any information acquired via the subpoenas.¹⁵³

C. *Dissenting Opinion*

In a lengthy dissent, Judge Diana E. Murphy explained that she would uphold the subpoenas and force Charter to comply with them.¹⁵⁴ The dissent noted that the subpoena provision does not explicitly limit the type of ISP that can receive a subpoena.¹⁵⁵ According to the dissent, Congress could easily have limited DMCA subpoenas to storage ISPs if that were its intention.¹⁵⁶ Therefore, the dissent concluded that the broad definition of service provider applies, and a conduit ISP like Charter falls within the reach of the court's subpoena power.¹⁵⁷

To refute the majority's limitation of the subpoena power, the dissent looked to the notification provision.¹⁵⁸ The dissent relied on a different interpretation of § 512(c)(3)(A)(iii), the requirement that notification identify "the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed."¹⁵⁹ In the dissent's view, use of the word "or" indicated that the material must either be "claimed to be infringing" or "the subject of infringing activity and that is to be removed."¹⁶⁰ Judge Murphy read this disjunction to allow a court to issue a subpoena when the ISP cannot remove the data, so long as the data is "claimed to be infringing."¹⁶¹ Furthermore, the dissent found support for this reading of

151. *Id.* Charter argued that no case or controversy supported the DMCA subpoenas, and the subpoenas violated Internet users' First Amendment rights. Appellant's Opening Brief at 22-27, 39-44, *In re Charter*, 393 F.3d 771 (No. 03-3802).

152. *In re Charter*, 393 F.3d at 777-78.

We comment without deciding that this provision *may* unconstitutionally invade the power of the judiciary by creating a statutory framework pursuant to which Congress, via statute, compels a clerk of a court to issue a subpoena, thereby invoking the court's power. Further, we believe Charter has at least a colorable argument that a judicial subpoena is a court order that must be supported by a case or controversy at the time of its issuance.

Id.

153. *Id.* at 778.

154. *Id.* at 786 (Murphy, J., dissenting).

155. *Id.* at 780.

156. *Id.* at 782.

157. *Id.* at 780.

158. *Id.* at 780-81.

159. *Id.* at 781 (quoting 17 U.S.C. § 512(c)(3)(A)(iii) (2000)).

160. *Id.* (quoting § 512(c)(3)(A)(iii)).

161. *Id.* (quoting § 512(c)(3)(A)(iii)).

§ 512(c)(3)(A)(iii) in the division between conduit ISPs and storage ISPs apparent throughout the DMCA.¹⁶²

To resolve any ambiguity that the DMCA created by referencing the notification provision within the subpoena provision, the dissent analyzed legislative history.¹⁶³ The dissent argued that Congress intended the DMCA to fight piracy while protecting ISPs from third party liability.¹⁶⁴ Judge Murphy observed that ISPs receive liability protection “in exchange for their assistance” in fighting infringement.¹⁶⁵ According to the dissent, the majority opinion undermined the DMCA by allowing conduit ISPs to reap the benefits of immunity without first aiding copyright holders by identifying infringing users.¹⁶⁶ Following its statutory analysis and discussion of legislative history, the dissent refuted Charter’s remaining objections to the subpoenas, ultimately concluding that the majority should have upheld the subpoenas.¹⁶⁷

V. COMMENTARY

The Eighth Circuit erred in holding that the DMCA does not authorize copyright holders to serve subpoenas upon conduit ISPs.¹⁶⁸ The court incorrectly concluded that a copyright holder cannot satisfy the notification provision of the DMCA when requesting a court to issue a subpoena to a conduit ISP.¹⁶⁹ Rather than adopting the flawed statutory analysis of *Verizon*, the court should have held that the DMCA authorizes subpoenas regardless of whether the ISP stores the infringing data.

A. *The Plain Language of the DMCA Authorizes Courts to Issue Subpoenas to Conduit ISPs*

The text of the DMCA authorizes subpoenas for conduit ISPs. The subpoena provision itself places no restrictions on the type of ISP to which a court may issue a subpoena.¹⁷⁰ Moreover, in creating an implicit restriction on the type of ISP subject to the subpoena power, the Eighth Circuit misread the notification provision to demand that

162. *Id.*

The distinction within § 512(c)(3)(A) between material “claimed to be infringing” and material that is “the subject of infringing activity and that is to be removed or access to which is to be disabled” appears to carry forward the initial distinction in the DMCA between § 512(a) conduit ISPs and § 512(b)-(d) storage ISPs.

Id.

163. *Id.* at 782.

164. *Id.*

165. *Id.*

166. *Id.*

167. *Id.* at 783-86.

168. *See id.* at 776-77 (majority opinion).

169. *Id.* at 777.

170. 17 U.S.C. § 512(h) (2000).

the ISP store the infringing material.¹⁷¹ The notification provision requires neither that the ISP be able to locate the infringing data nor that the ISP be able to remove the infringing data.¹⁷² Alternatively, if the notification provision requires that the ISP be able to locate or remove the infringing data, the court did not examine whether conduit ISPs can locate or remove the data.¹⁷³

1. The DMCA Expressly Defines “Service Provider” to Include Conduit ISPs

Section 512(k)(1) sets forth the scope of ISPs contemplated in the DMCA.¹⁷⁴ This section provides two definitions of service provider, the first of which, § 512(k)(1)(A), describes a conduit ISP.¹⁷⁵

As used in subsection (a), the term “service provider” means 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.¹⁷⁶

Thus, in § 512(a), the safe harbor for conduit ISPs, service provider strictly means an ISP that acts as a conduit.¹⁷⁷ For the remainder of the statute, however, a broader definition applies.¹⁷⁸ “As used in this section, other than subsection (a), the term ‘service provider’ means a provider of online services or network access, or the operator of facilities therefor, *and includes an entity described in subparagraph (A).*”¹⁷⁹ For all subsections except the safe harbor for conduit ISPs, including § 512(h), service provider means conduit ISPs and non-conduit ISPs.¹⁸⁰ Therefore, the provision for “a subpoena to a service provider” should, absent other restrictions, apply to any type of ISP.¹⁸¹

2. The Subpoena Provision’s References to the Notification Requirements Do Not Restrict the DMCA Subpoena Power

To limit the applicability of the subpoena provision, *Charter* focused on the subpoena provision’s reference to the notification re-

171. *In re Charter*, 393 F.3d at 776-77.

172. § 512(c)(3)(A).

173. *See In re Charter*, 393 F.3d at 776-77.

174. § 512(k)(1).

175. *Id.*

176. § 512(k)(1)(A).

177. *Id.*

178. § 512(k)(1)(B).

179. *Id.* (emphasis added). By including “an entity described in [§ 512(k)(1)](A),” this provision establishes that “service provider” includes conduit ISPs. *Id.*

180. *Id.*

181. § 512(h)(1).

quirement.¹⁸² Specifically, the court concluded that a copyright holder cannot satisfy § 512(c)(3)(A)(iii) when serving a conduit ISP because a conduit ISP can neither locate nor remove the infringing material.¹⁸³ With respect to a conduit ISP, however, a copyright holder's subpoena request necessarily meets the requirements of § 512(c)(3)(A)(iii).¹⁸⁴ Moreover, the subpoena request need only substantially fulfill the notification requirement.¹⁸⁵

The Eighth Circuit failed to recognize that a subpoena request necessarily meets the demands of § 512(c)(3)(A)(iii). To be adequate with regard to any ISP, this subsection demands that the notification include “[i]dentification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.”¹⁸⁶ Both the majority and the dissent misinterpreted this subsection.

a. *The Majority Misread § 512(c)(3)(A)(iii)*

The majority read § 512(c)(3)(A)(iii) to require that every subpoena must involve material “that is to be removed or access to which is to be disabled.”¹⁸⁷ Because the court concluded that a conduit ISP can never remove or disable access to material on a subscriber's computer, it held that no copyright holder could satisfy the notification requirements with respect to a conduit ISP.¹⁸⁸ This holding was in error because if a conduit ISP cannot remove or disable access to the specified material, then the subpoena request necessarily fulfills § 512(c)(3)(A)(iii).¹⁸⁹ When a court issues a subpoena to a conduit ISP, there simply is no material “that is to be removed or access to which is to be disabled.”¹⁹⁰ Section 512(c)(3)(A)(iii) does not demand that a copyright holder identify any material at all, unless that material “is to be removed or access to [it] is to be disabled.”¹⁹¹ If there is no material to identify, as is the case when a court issues a subpoena to a conduit ISP, then the RIAA can hardly fail to identify it.¹⁹²

Subpoena requests directed at conduit ISPs can satisfy all of the notification elements without identifying any data. The Eighth Circuit

182. *In re Charter Commc'ns, Inc.*, Subpoena Enforcement Matter, 393 F.3d 771, 777 (8th Cir. 2005).

183. *Id.*

184. *See infra* Part V.A.2.a.

185. § 512(c)(3)(A).

186. § 512(c)(3)(A)(iii).

187. *In re Charter*, 393 F.3d at 776-77.

188. *Id.*

189. *See* § 512(c)(3)(A)(iii) (requiring that a subpoena request only identify material “that is to be removed or access to which is to be disabled”).

190. *Id.*

191. *See supra* note 189.

192. *See supra* note 139.

interpreted the DMCA to require that the RIAA identify something that does not exist, and it concluded that the RIAA failed to meet this baffling requirement.¹⁹³ Because § 512(c)(3)(A)(iii) demands that a copyright holder only identify material if it is “to be removed or access to [it] is to be disabled,” that subsection demands nothing from a copyright holder that seeks information from a conduit ISP.¹⁹⁴ Therefore, § 512(c)(3)(A)(iii) does not restrict the scope of the subpoena provision.¹⁹⁵ Section 512(h) supports this interpretation by demanding that the ISP reveal customer information “regardless of whether [it] responds to the notification” by removing or disabling access to the infringing material.¹⁹⁶ If the court correctly concluded that a conduit ISP can neither locate nor remove infringing material, then the court cannot sustain its interpretation of § 512(c)(3)(A)(iii) as a limitation to the subpoena provision.¹⁹⁷

Further, the RIAA substantially satisfied § 512(c)(3)(A)(iii).¹⁹⁸ To adequately notify an ISP, a DMCA subpoena request need only “include[] substantially” the six notification elements.¹⁹⁹ This caveat supports the inference that a subpoena request need not specify the material that is to be located and removed when no such material exists.²⁰⁰ Relying on *Verizon*, the court in *Charter* overlooked the significance of the word “substantially.”²⁰¹ The court in *Verizon* concluded that Congress inserted “substantially” merely to allow for “technical errors . . . such as misspelling a name.”²⁰² The demand for merely substantial compliance could indicate that under some circumstances courts need not read all elements strictly.²⁰³

Rather than endorsing the *Verizon* view of “substantially,” the Eighth Circuit should have adopted a broader view of the notification elements akin to that of the Fourth Circuit.²⁰⁴ In *ALS Scan*, the Fourth Circuit held that a copyright holder can substantially comply with the notification elements in § 512(c)(3)(A)(ii) and (iii) simply by specifying which newsgroups housed infringing works.²⁰⁵ The Fourth

193. *In re Charter*, 393 F.3d at 777.

194. § 512(c)(3)(A)(iii).

195. *Contra In re Charter*, 393 F.3d at 777 (reasoning that § 512(c)(3)(A)(iii) restricts the scope of the subpoena provision).

196. § 512(h)(5).

197. *See supra* note 139.

198. § 512(c)(3)(A).

199. *Id.*

200. *Id.*

201. *In re Charter Commc'ns, Inc.*, Subpoena Enforcement Matter, 393 F.3d 771, 777 (8th Cir. 2005).

202. *Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1236 (D.C. Cir. 2003) (citing S. REP. NO. 105-190, at 47 (1998); H.R. REP. NO. 105-551, pt. 2, at 56 (1998) (alteration in original)).

203. *See ALS Scan, Inc. v. RemarQ Cmty., Inc.*, 239 F.3d 619, 625 (4th Cir. 2001) (rejecting a strict interpretation of substantial compliance).

204. *Id.*

205. *Id.*

Circuit apparently does not share the *Verizon* view that substantial compliance allows merely for technical errors.²⁰⁶ Under a similarly relaxed view of the notification requirements, the Eighth Circuit could have held that, when the ISP can neither locate nor remove the infringing material, a subpoena request substantially meets § 512(c)(3)(A)(iii).²⁰⁷ Instead, the court erroneously concluded that the notification provision acted as an indirect limitation upon the subpoena provision.²⁰⁸ A more accurate conclusion would have been that the RIAA complied with the notification provision literally and substantially.

b. *The Dissent Misread § 512(c)(3)(A)(iii)*

The dissent interpreted the subpoena provision to allow courts to issue subpoenas to conduit ISPs but founded its conclusion on a more manifest misreading of § 512(c)(3)(A)(iii) than the majority's reading.²⁰⁹ The dissent interpreted the first "or" of § 512(c)(3)(A)(iii) as creating a divide between "material that is claimed to be infringing" and material that is claimed "to be the subject of infringing activity and that is to be removed or access to which is to be disabled."²¹⁰ The dissent concluded that material did not need to be subject to removal, so long as it was "claimed to be infringing."²¹¹

The dissent overlooked the implication of the parallel usage of "that" in § 512(c)(3)(A)(iii).²¹² This subsection requires "[i]dentification of the material *that* is claimed to be infringing or to be the subject of infringing activity *and that* is to be removed or access to which is to be disabled."²¹³ The dissent should have recognized that, regardless of whether the material is infringing per se or related to infringing activity, § 512(c)(3)(A)(iii) demands that the material also be subject to either removal or disabled access.²¹⁴ Although the dissent correctly concluded that the DMCA allows a court to issue a subpoena to a conduit ISP, the dissent misread the notification requirements to reach this result.²¹⁵ While advancing this flawed interpretation, the dissent assumed that the majority's reading created a limitation to the subpoena power and neglected to point out that the court's holding

206. *Id.*

207. *Id.*

208. *In re Charter Commc'ns, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 777 (8th Cir. 2005).

209. *Id.* at 786 (Murphy, J., dissenting).

210. 17 U.S.C. § 512(c)(3)(A)(iii) (2000); *In re Charter*, 393 F.3d at 781 (Murphy, J., dissenting).

211. *In re Charter*, 393 F.3d at 781.

212. *See* § 512(c)(3)(A)(iii).

213. *Id.* (emphasis added).

214. *Id.*

215. *In re Charter*, 393 F.3d at 786 (Murphy, J., dissenting).

does not follow from the majority's construction of § 512(c)(3)(A)(iii).²¹⁶

3. The Court Did Not Examine Whether a Conduit ISP Can Locate or Remove Infringing Material

The Eighth Circuit's interpretation of the notification provision, even if accurate, fails to support its holding because the court did not examine whether a conduit ISP can locate or remove infringing material.²¹⁷ If conduit ISPs can neither locate nor remove infringing material that resides on a customer's computer, then a request for a subpoena to a conduit ISP necessarily meets the notification provision.²¹⁸ Alternatively, if conduit ISPs can locate and remove infringing material that resides on a customer's computer, then a copyright holder's request for a subpoena to a conduit ISP fulfills the notification provision in the same way as a request for a subpoena to a storage ISP.²¹⁹ In either case, the *Charter* holding is erroneous.

a. Conduit ISPs Can Remove or Disable Access to Infringing Material

Despite the Eighth Circuit's conclusion to the contrary, it is not clear that conduit ISPs cannot remove or disable access to infringing material that resides on a customer's computer.²²⁰ An ISP has the power to terminate an Internet user's account.²²¹ The RIAA argued that to do so would disable access to any infringing material the user made available.²²² Arguably, terminating a subscriber's account would also remove the infringing material from availability to other P2P network users.²²³ Regardless, *Charter* held that a conduit ISP can neither remove nor disable access to infringing material.²²⁴ Demonstrating that a conduit ISP can do either refutes the court's holding because the DMCA only requires that an ISP do one or the other.²²⁵

The Eighth Circuit relied on *Verizon* to rebut the RIAA on this issue, stating that the DMCA prescribed terminating a subscriber's account and disabling access as distinct remedies.²²⁶ The court noted in

216. *Id.*

217. *See id.* at 777 (majority opinion) (reasoning that a conduit ISP cannot remove or disable access to infringing material residing on a user's computer).

218. *See supra* Part V.A.2.a.

219. *See infra* Parts V.A.3.a-b.

220. *See supra* note 217.

221. *In re Charter*, 393 F.3d at 781 (Murphy, J., dissenting).

222. Brief of Appellee at 33, *In re Charter*, 393 F.3d 771 (No. 03-3802).

223. *See* 17 U.S.C. § 512(c)(3)(A)(iii) (2000). Because Congress did not specify from what the material must be removed or from what access must be disabled, it is unclear how Congress intended to distinguish between removing material and disabling access to material. *See id.*

224. *In re Charter*, 393 F.3d at 777.

225. § 512(c)(3)(A)(iii).

226. *In re Charter*, 393 F.3d at 777.

Verizon that the DMCA distinguishes injunctions “restraining [the] ISP ‘from providing access to infringing material’” from those “restraining [the] ISP ‘from providing access to a subscriber or account holder . . . by terminating the accounts of the subscriber or account holder.’”²²⁷ The court reasoned in *Verizon* that these distinct types of injunctions available under § 512(j)(1)(A) established that the two remedies were not interchangeable.²²⁸ The court in *Verizon* therefore reasoned that Congress did not intend for conduit ISPs to disable access to infringing material by terminating the account of the user that stores the infringing material.²²⁹ The Eighth Circuit endorsed this position.²³⁰

The Eighth Circuit failed to notice that the injunction provisions cited by the court in *Verizon* do not contemplate conduit ISPs.²³¹ The specified injunctions only apply to ISP conduct “*other than* that which qualifies for the limitation on remedies set forth in subsection (a).”²³² Section 512(a) is the safe harbor for conduit ISPs, so the injunctions cited in *Verizon* do not apply to conduit ISPs.²³³ Conduit ISPs are subject to the remedies in § 512(j)(1)(B) instead.²³⁴ Notably, this subsection does not distinguish between terminating a user’s account and disabling access to particular data.²³⁵ Therefore, with respect to conduit ISPs, Congress did not necessarily intend the two procedures to be separate remedies.²³⁶ Because a conduit ISP indisputably can terminate an Internet user’s account, *Charter* erred in assuming that a conduit ISP cannot remove or disable access to infringing material that resides on a user’s computer.²³⁷

b. *Conduit ISPs Can Locate Infringing Material*

Despite the Eighth Circuit’s conclusion to the contrary, it is not clear that conduit ISPs cannot locate infringing material that resides

227. Recording Indus. Ass’n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1235 (D.C. Cir. 2003) (quoting § 512(j)(1)(A)(i) and (ii)).

228. *Id.*

229. *Id.*

230. *In re Charter*, 393 F.3d at 777.

231. See § 512(j)(1)(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” *Id.*

232. *Id.* (emphasis added).

233. § 512(a).

234. § 512(j)(1)(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” *Id.*

235. *Id.*

236. *Id.*

237. See Recording Indus. Ass’n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1235 (D.C. Cir. 2003) (discussing a conduit ISP’s ability to terminate a user’s Internet access).

on a customer's computer.²³⁸ *Charter* exceeded the *Verizon* holding in concluding that a conduit ISP cannot locate the infringing material stored on a customer's computer.²³⁹ *Verizon* did not hold that a conduit ISP cannot locate the material.²⁴⁰ Rather, *Verizon* concluded that because the material did not reside on the ISP's hardware, a conduit ISP could not remove or disable access to the material.²⁴¹ The two positions are distinguishable in that *Charter* perceived an additional obstacle in § 512(c)(3)(A)(iii): an ISP's purported inability to locate the material.²⁴²

There are multiple ways that a conduit ISP can locate infringing material that resides on an Internet user's computer. First, an ISP can locate the infringing material in the same manner that the copyright holder can discover the material.²⁴³ When a user shares a file on a P2P network, any party who wishes to download that file must first locate it.²⁴⁴ In *Charter*, the RIAA used a tracking program to detect copyrighted files on P2P networks.²⁴⁵ The RIAA also downloaded the suspect files.²⁴⁶ A conduit ISP may use one or both of the same techniques, or some technological equivalent, to locate files on a subscriber's computer.²⁴⁷ Second, to comply with a subpoena, an ISP must locate the infringing data because the ISP must identify which customer corresponds to the suspect IP address.²⁴⁸ "Only the ISP . . . can link a particular IP address with an individual's name and physical address."²⁴⁹ Thus, an ISP can locate the material with greater specificity than any other party by identifying the Internet user that stores the infringing data.²⁵⁰ In this case, *Charter* complied with the subpoenas, thereby demonstrating the ability to locate subscribers.²⁵¹ *Charter* erred in assuming that a conduit ISP cannot locate infringing material that resides on a user's computer.

It is unknown what more Congress could have intended ISPs to do to remove or locate infringing material. The court erred in *Charter* when it reasoned that a conduit ISP can neither remove nor locate

238. *In re Charter Commc'ns, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 776-77 (8th Cir. 2005) "[T]he DMCA require[s] the ISP to be able both to locate and remove the allegedly infringing material." *Id.* at 777.

239. *Id.* at 776-77.

240. *See Verizon*, 351 F.3d at 1235.

241. *Id.*

242. *See supra* note 238.

243. Trevor A. Dutcher, Comment, *A Discussion of the Mechanics of the DMCA Safe Harbors and Subpoena Power, as Applied in RIAA v. Verizon Internet Services*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 493, 502-03 (2005).

244. *In re Charter*, 393 F.3d at 773.

245. *Id.* at 779 (Murphy, J., dissenting).

246. *Id.* at 780.

247. Dutcher, *supra* note 243, at 502-03.

248. *In re Charter*, 393 F.3d at 774.

249. *Id.*

250. *Id.*

251. Brief of Appellee at 32, *In re Charter*, 393 F.3d 771 (No. 03-3802).

infringing material because it did not consider what Congress meant by removing the material, disabling access to the material, or locating the material.²⁵² Had the court made any of these determinations, it could have found support for its conclusion that conduit ISPs can neither locate nor remove infringing data. For instance, the safe harbor for conduit ISPs is the only safe harbor that does not refer to the notification provision, suggesting that Congress agreed that a conduit ISP can neither locate nor remove infringing data.²⁵³

Nevertheless, either conclusion defeats the *Charter* holding. Either a conduit ISP can locate and remove infringing data, in which case the ISP can receive adequate notification, or a conduit ISP can neither locate nor remove infringing data, in which case the ISP necessarily receives adequate notification.²⁵⁴ Failing to articulate the basis for its conclusion that a conduit ISP can neither locate nor remove or disable access to infringing material stored on a customer's computer, the Eighth Circuit left its holding susceptible to both alternative arguments.

B. *The Structure of § 512 Supports Authorizing Courts to Issue Subpoenas to Conduit ISPs*

The structure of § 512 resolves the ambiguity surrounding whether the subpoena provision applies to conduit ISPs.²⁵⁵ Rather than reproduce the notification elements throughout § 512, Congress referred to the elements as listed in § 512(c)(3)(A) when another provision dealt with notification.²⁵⁶ In reaching its holding, the Eighth Circuit relied on the ambiguity created by this structure.²⁵⁷ The court failed to notice that Congress's practice of referring to the notification elements as listed in § 512(c)(3)(A) resolves the ambiguity against the court's holding.²⁵⁸ For instance, if § 512(c)(3)(A)(iii) provided that a copyright holder must identify *any* material that is to be removed instead of "*the* material . . . that is to be removed," then notification would clearly not preclude a court from issuing a subpoena to a conduit ISP.²⁵⁹ Because Congress couched the notification elements in § 512(c), a safe harbor for storage ISPs, the language therein assumes

252. See *In re Charter*, 393 F.3d at 776-78.

253. *Id.* at 776 (noting that the safe harbor for conduit ISPs does not reference the notification provision).

254. See *supra* Parts V.A.2.a-3.b.

255. *In re Charter*, 393 F.3d at 782 (Murphy, J., dissenting).

256. E.g., 17 U.S.C. § 512(h)(2)(A) (2000).

257. *In re Charter*, 393 F.3d at 780 (Murphy, J., dissenting). "[T]he majority relies on the § 512(h) reference to the notice provision in § 512(c)(3)(A) to read a limitation into the availability of subpoenas." *Id.*

258. *Id.* at 781.

259. § 512(c)(3)(A)(iii) (emphasis added).

that the ISP is a storage ISP.²⁶⁰ The Eighth Circuit should have recognized that its holding relied on a consequence of § 512(h) borrowing language from a narrower provision.²⁶¹

What the structure of § 512 does not provide is as revealing as what the structure does provide. The DMCA contains provisions throughout § 512 that explicitly apply only to conduit ISPs or only to storage ISPs.²⁶² Section 512(h), in contrast, applies to “service provider[s]” generally.²⁶³ Had Congress intended to restrict the subpoena provision to storage ISPs, structurally bifurcating § 512(h) would have easily and unquestionably established that intent.²⁶⁴ The absence of such a distinction in the subpoena provision, especially when present in other provisions, indicates that the subpoena provision applies equally to conduit and storage ISPs.²⁶⁵

C. Congressional Intent Supports Authorizing Courts to Issue Subpoenas to Conduit ISPs

The blatant contrast between the Eighth Circuit’s holding and Congress’s intent in passing the DMCA amplifies any doubt regarding the soundness of the court’s statutory analysis in *Charter*. The legislative history resolves any ostensible ambiguity in the DMCA’s text in favor of allowing courts to subpoena ISPs generally.²⁶⁶

1. Charter Results in a Nonsensical DMCA

The *Charter* holding is inconsistent with Congress’s motivations for enacting the DMCA. Congress designed the DMCA to enable copyright holders to directly sue otherwise anonymous Internet users and to protect ISPs from indirect liability for their users’ acts.²⁶⁷ The subpoena provision serves the former goal, and the safe harbor provisions serve the latter.²⁶⁸ Together, these provisions form a quid pro quo relationship.²⁶⁹ Despite overtly recognizing the implicit balance in the DMCA between ISPs and copyright holders, *Charter* produced

260. § 512(c) (creating a safe harbor for one type of storage ISP).

261. *In re Charter*, 393 F.3d at 781 (Murphy, J., dissenting).

262. *E.g.*, § 512(j)(1)(A)-(B); § 512(k)(1)(A)-(B).

263. § 512(h)(1).

264. *In re Charter*, 393 F.3d at 780 (Murphy, J., dissenting).

265. *Id.*

266. *Id.* at 782.

267. *ALS Scan, Inc. v. RemarQ Cmtys., Inc.*, 239 F.3d 619, 625 (4th Cir. 2001) (citing H.R. REP. NO. 105-796, at 72 (1998) (Conf. Rep.); H.R. REP. NO. 105-551, pt. 1, at 11 (1998)).

268. *Id.*

269. Brief for the United States as Intervenor and Amicus Curiae at 28, *In re Charter*, 393 F.3d 771 (No. 03-3802). “In return for limiting the liability of ISPs for their role in the online dissemination of infringing materials, Congress sought to encourage ISPs ‘to cooperate [with copyright owners] to detect and deal with copyright infringements’” *Id.* (quoting H.R. REP. NO. 105-796, at 72 (1998) (Conf. Rep.)).

a result incongruous with this relationship.²⁷⁰ Under *Charter*, conduit ISPs can freely reap the benefits of a safe harbor without cooperating to identify allegedly infringing Internet users.²⁷¹ There is no reason that Congress would intend to restrict the DMCA subpoena provision to storage ISPs.²⁷² It is even more unfathomable why Congress would choose to express this restriction in the roundabout way contemplated by the court in *Charter*.²⁷³ The Eighth Circuit should have rejected this interpretation for its absurdity.

If the *Charter* interpretation of the DMCA is accurate, then a court's subpoena power does not reach one of the most profuse sources of Internet piracy. That Congress failed to foresee the emergence of P2P networks does not explain this odd result, although the Eighth Circuit argued otherwise.²⁷⁴ The court in *Charter* refused to "rewrite the DMCA 'in order to make it fit a new and unforeseen internet [sic] architecture.'"²⁷⁵ This characterization is wrong for two reasons. First, as discussed above, one can read the DMCA to address P2P network piracy, so rewriting the statute is far from necessary to reach a result at odds with *Charter*.²⁷⁶ Second, and more importantly, the DMCA's text refutes the assertion that piracy via conduit ISPs was unforeseen.²⁷⁷

Congress likely did not anticipate the explosion of P2P technology before Napster emerged.²⁷⁸ Nevertheless, § 512(a) establishes beyond a doubt that Congress anticipated piracy by Internet users whose ISPs acted only as conduits.²⁷⁹ The safe harbor for conduit ISPs excuses them from liability that would arise from merely transmitting infringing material.²⁸⁰ Therefore, Congress knew that an Internet user could transmit infringing material without an ISP storing the material.²⁸¹ It is irrelevant that Congress was unaware at the time of the DMCA's enactment that such a practice would eventually become the most popular method of file-sharing.²⁸² Because Congress anticipated

270. *In re Charter*, 393 F.3d at 774.

271. Brief for the United States as Intervenor and Amicus Curiae at 29, *In re Charter*, 393 F.3d 771 (No. 03-3802).

272. *In re Verizon Internet Servs., Inc.*, 240 F. Supp. 2d 24, 35 (D.D.C. 2003).

273. *In re Charter*, 393 F.3d at 782 (Murphy, J., dissenting). "Had Congress wanted to limit the reach of the subpoena power to ISPs engaged in storage functions, it could have easily stated that." *Id.*

274. *Id.* at 777 (majority opinion).

275. *Id.* (quoting *Recording Indus. Ass'n of Am. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1238 (D.C. Cir. 2003)).

276. *See supra* Part V.A.2.a.

277. *See* 17 U.S.C. § 512(a) (2000) (creating a safe harbor for conduit ISPs).

278. *In re Charter*, 393 F.3d at 773.

279. § 512(a).

280. *Id.*

281. *Id.*

282. *See In re Charter*, 393 F.3d at 773-74 (noting that Congress passed the DMCA before the emergence of P2P technology).

P2P-type exchanges, the Eighth Circuit erred in attributing the paradoxical result of its holding to congressional inadvertence.²⁸³

2. Allowing Courts to Issue Subpoenas to Conduit ISPs Better Fits Congressional Intent

Interpreting the DMCA to allow courts to issue subpoenas to conduit ISPs is more consistent with the DMCA's two goals than is the *Charter* holding.²⁸⁴ Congress intended the DMCA "to limit the liability of service providers" and "to assist copyright owners in protecting their copyrights."²⁸⁵ The requirement that a subpoena request contain notification of the infringing activity serves the first goal.²⁸⁶ Due to the notification requirement, any storage ISP can take steps to ensure the corresponding safe harbor's protection and thereby excuse itself from potential liability.²⁸⁷ *Charter*, however, viewed the notification requirement as a limitation to the subpoena provision that prevents copyright holders from protecting their copyrights by learning the identities of infringing conduit ISP users.²⁸⁸ Thus, the court interpreted a mechanism that Congress intended to serve the first goal of the DMCA, limiting ISP liability, in a way that contravenes the second goal, copyright protection.

Despite the Eighth Circuit's assurance to the contrary, its holding in *Charter* leaves copyright holders with no comparable alternative that comports with legislative intent.²⁸⁹ "The legislative history shows that the purpose of the subpoena power in the DMCA was to obtain the assistance of ISPs in an expeditious process to stop infringement."²⁹⁰ The *Charter* interpretation of the DMCA does not provide any such mechanism with respect to conduit ISPs.²⁹¹ The court suggested John Doe lawsuits as "alternative avenues" to the DMCA subpoena provision.²⁹² John Doe lawsuits, however, demand more from copyright holders and are slower than the simple procedure of § 512(h).²⁹³ John Doe lawsuits also deny the opportunity for settlement before initiating the lawsuit because a copyright holder cannot

283. *Id.* at 777.

284. *Id.* at 782 (Murphy, J., dissenting).

285. *In re Verizon Internet Servs., Inc.*, 240 F. Supp. 2d 24, 36 (D.D.C. 2003).

286. *In re Charter*, 393 F.3d at 776. "[A] specific purpose of the notification provision is to allow an ISP, after notification, the opportunity to remove or disable access to infringing material and thereby protect itself from liability for copyright infringement." *Id.*

287. Brief of Appellee at 31, *In re Charter*, 393 F.3d 771 (No. 03-3802).

288. *In re Charter*, 393 F.3d at 777.

289. *Id.* at 779 (Murphy, J., dissenting). "The only viable way for copyright owners to vindicate their intellectual property rights in a timely manner when infringing materials are transmitted across peer to peer networks is to subpoena the ISPs for disclosure of the identities of alleged infringers." *Id.*

290. *Id.* at 782 (citing S. REP. NO. 105-190, at 51 (1998)).

291. *Id.*

292. *Id.* at 775 n.3 (majority opinion).

293. Yu, *supra* note 12, at 674-75.

attempt to settle with an Internet user that it cannot identify.²⁹⁴ More importantly, the court should not force copyright holders to rely on an inferior alternative when Congress provided a superior mechanism.²⁹⁵ The holding in *Charter* is such a departure from congressional intent that a juxtaposition of the two casts doubt on the court's analysis.

VI. CONCLUSION

The United States Court of Appeals for the Eighth Circuit incorrectly held that the DMCA's subpoena power does not reach conduit ISPs. The DMCA's text simply does not support this holding. The result reached by the court renders the DMCA both nonsensical and largely useless as a tool for copyright enforcement.

In *Charter*, the Eighth Circuit sidestepped significant constitutional questions surrounding the DMCA. Reading the DMCA to allow a court to issue a subpoena to a conduit ISP would have forced the court to consider Charter's constitutional objections.²⁹⁶ Instead, the court's commentary on the constitutionality of the DMCA subpoena provision was mere dicta.²⁹⁷ Because the Eighth Circuit never reached these issues, the constitutional questions surrounding the DMCA remain unanswered.²⁹⁸

More lamentably, *Charter* embraced the faulty analysis of *Verizon*, thereby foregoing the opportunity to create a circuit split on the scope of the DMCA subpoena provision and perpetuating a judicial deprivation of a copyright holder's right to learn the identity of an alleged infringer who uses P2P technology. Now that two circuits share the wrong interpretation, jurisdictions that must decide the same issue in the future are less likely to adopt a rational interpretation of the DMCA.²⁹⁹ The judiciary will effectively deprive copyright holders of a statutory right if no jurisdiction remedies the erroneous *Charter/Verizon* interpretation of the DMCA and recognizes that the DMCA indisputably authorizes courts to issue subpoenas to conduit ISPs. Until further litigation gives rise to an accurate interpretation of the DMCA, judicial misunderstanding will remain yet another obstacle in Congress's frustrated attempts to curb Internet piracy.

294. *Id.* at 674.

295. *In re Charter*, 393 F.3d at 782 (Murphy, J., dissenting). "The suggestion that copyright holders should be left to file John Doe lawsuits to protect themselves from infringement by subscribers of conduit ISPs like Charter, instead of availing themselves of the mechanism Congress provided in the DMCA, is impractical and contrary to legislative intent." *Id.*

296. *See supra* note 21.

297. *See supra* note 152.

298. For a discussion of the constitutionality of the DMCA subpoena provision, see Jeffrey M. Levinsohn, Comment, *Protecting Copyright at the Expense of Internet Anonymity: The Constitutionality of Forced Identity Disclosure Under 512(h) of the Digital Millennium Copyright Act*, 23 TEMP. ENVTL. L. & TECH. J. 243 (2004).

299. *See In re Subpoena to Univ. of N.C. at Chapel Hill*, 367 F. Supp. 2d 945, 952-53 (M.D.N.C. 2005) (concurring with *Verizon* and *Charter* on this statutory issue).

