

LOSING THE BATTLE AGAINST INDIVIDUAL
INFRINGERS, COPYRIGHT HOLDERS SET THEIR SIGHTS
ON INTERNET SERVICE PROVIDERS ONCE AGAIN

Michael E. Benson

| | |
|---|-----|
| INTRODUCTION | 445 |
| I. BACKGROUND | 446 |
| <i>A. Targeting Individuals for Direct Copyright Infringement</i> | 446 |
| <i>B. Targeting Intermediaries for Secondary Liability for Copyright Infringement</i> | 448 |
| II. COURTS HAVE BECOME SKEPTICAL OF USING IP ADDRESSES TO LINK INDIVIDUALS TO INFRINGING ACTS..... | 449 |
| <i>A. District Court Body Blows Against Copyright Holders</i> | 450 |
| <i>B. The Ninth Circuit's Knockout Punch</i> | 453 |
| III. COPYRIGHT HOLDERS TARGET INTERMEDIARIES (AGAIN) | 454 |
| <i>A. Internet Intermediary Liability and Safe Harbors Case Law Development</i> | 454 |
| <i>B. A Chink in the Safe Harbor Armor?</i> | 455 |
| IV. FORECASTING THE SOLUTION TO THE COPYRIGHT HOLDERS' QUANDARY | 456 |
| CONCLUSION | 457 |

LOSING THE BATTLE AGAINST INDIVIDUAL INFRINGERS, COPYRIGHT HOLDERS SET THEIR SIGHTS ON INTERNET SERVICE PROVIDERS ONCE AGAIN

*Michael E. Benson**

INTRODUCTION

The passing of the Digital Millennium Copyright Act¹ (“DMCA”) in 1998 was, in one sense, a vindication of the rights of copyright holders in pursuing individual copyright infringers.² The DMCA provides a mechanism for rights holders to determine the identity of an account holder when an account holder’s IP address is involved in infringing activity.³ However, in another sense, Congress’s passing of the DMCA harmed copyright holders by protecting intermediaries that otherwise could have been found to be secondarily liable for copyright infringement.⁴ Under the DMCA, an Internet Service Provider (“ISP”) can avoid secondary liability for the infringing activity of the ISP’s customers through statutory safe harbor provisions.⁵ While the DMCA empowered copyright holders to find and punish individual infringers, it also limited the ability of copyright holders to recover from ISPs.

Recently, there has been a shift in judicial thinking concerning copyright holders targeting alleged individual infringers. Courts have generally made it difficult for copyright holders to litigate against both direct infringers and intermediaries liable under a theory of secondary liability.⁶ This paper examines a slew of recent cases in which courts found that an IP address is not sufficient to identify an alleged online copyright infringer, thus making it much more difficult for a copyright holder to sustain a case against an individual.⁷ This paper argues that, as a result of the courts limiting copyright holders from pursuing alleged individual infringers, that

* Michael E. Benson is an associate at Wood Herron & Evans LLP. The views and opinions expressed in this article are those of the author and do not necessarily reflect the legal position of Wood Herron & Evans LLP or any of its other attorneys or clients on any matter.

¹ Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (2012) (codified in scattered sections of 17 U.S.C., 35 U.S.C., 5 U.S.C., 28 U.S.C.).

² See generally DMCA § 202(a); 17 U.S.C. § 512(h) (2012).

³ *Id.*

⁴ See generally DMCA § 202(a); 17 U.S.C. § 512(a)-(e) (2012).

⁵ *Id.*

⁶ See *infra* Part I.

⁷ See *infra* Part II.

rights holders will once again target intermediaries, specifically ISPs, under a theory of secondary liability.⁸ Further, this paper comments on the renewed possibility of copyright holders successfully holding ISPs liable for secondary infringement, as copyright holders have been unable to do in the past.⁹

Part I lays out the main issues that copyright holders face in pursuing alleged individual online infringers as well as in pursuing the intermediaries that facilitate the alleged online infringement. Part II discusses a series of cases that weakened copyright holders' ability to litigate against alleged individual infringers. Part III of this paper examines how copyright holders reacted to their newly weakened ability to hold individual infringers responsible—namely, by setting their sights on ISPs once again. Part IV of this paper presents my thoughts concerning copyright holders' renewed attempts to hold ISPs secondarily liable for the alleged infringements of their subscribers. The paper ends with a brief conclusion.

I. BACKGROUND

Copyright holders face one set of distinct issues when pursuing alleged individual infringers for direct infringement and a second set of distinct issues when pursuing intermediaries (e.g., ISPs) for secondary liability. First, the relevant issue that copyright holders face when pursuing an individual online infringer is meeting the pleading standard bar set by the Court in *Bell Atlantic Corp. v. Twombly*¹⁰ and *Ashcroft v. Iqbal*.¹¹ Second, the DMCA safe harbor provisions create two issues for copyright holders who attempt to hold an ISP liable for infringement by the ISP's subscribers because the DMCA established statutory safe harbors for intermediaries that shield the ISPs from liability.¹²

A. Targeting Individuals for Direct Copyright Infringement

Copyright holders pursuing individuals for direct infringement face significant issues in the pleading stage of litigation. The issues the copyright holders face come from the higher pleading standard established by the duo of Supreme Court cases, *Twombly*¹³ and *Iqbal*.¹⁴

In *Twombly*, the Court retired the lower pleading standard advanced by

⁸ See *infra* Part III.

⁹ See *infra* Part IV.

¹⁰ See generally *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007).

¹¹ See generally *Ashcroft v. Iqbal*, 556 U.S. 662 (2009).

¹² See generally 17 U.S.C. § 512(a)-(e) (2012).

¹³ *Twombly*, 550 U.S. at 570.

¹⁴ *Iqbal*, 556 U.S. at 677-680.

*Conley v. Gibson*¹⁵ and *Swierkiewicz v. Sorema*,¹⁶ by introducing a reading of Federal Rule of Civil Procedure (“FRCP”) 8(a)(2)¹⁷ that required a pleading to include a set of facts that makes the pleading’s claim plausible instead of merely possible.¹⁸ Following the *Twombly* decision, the Court decided another case regarding the pleading standard only two years later in *Iqbal*. In *Iqbal*, the Court held that in order to determine if the facts alleged in the pleading nudge the pleaded claim over the line from possible to plausible, that the judge looks only at the alleged facts and uses his own experience and common knowledge to decide if the claim is plausible on its face.¹⁹ The higher pleading standard set by the Court’s interpretation of Rule 8(a)(2) in *Twombly* and *Iqbal* creates particular trouble for copyright holders suing individuals for their alleged direct infringement.

In cases where copyright holders are suing individuals for direct infringement, often the strongest (or only) evidence that the copyright holder has tying an individual to the infringement is the IP address that accessed or downloaded the infringing material.²⁰ The question is whether or not an IP address is enough to convince a judge that it is plausible that the individual who pays an ISP for internet service and is assigned an IP address is the individual who committed copyright infringement. Courts have gone both ways on this issue.²¹ The reason for the inconsistency is that Rule 8(a)(2) requires a judge to use his or her own experience and common sense to evaluate if the claim is made plausible by the facts or merely possible.²² Recently, the trend has been for judges to find that an IP address connecting an ISP account holder to an infringing act is not enough factual support to push a claim across the line from being merely possible into being

¹⁵ *Conley v. Gibson*, 355 U.S. 41, 45-46 (1957).

¹⁶ *Swierkiewicz v. Sorema N.A.*, 534 U.S. 506, 512-13 (2002).

¹⁷ FED. R. CIV. P. 8(a)(2).

¹⁸ *Twombly*, 550 U.S. at 570 (“enough facts to state a claim to relief that is plausible on its face”).

¹⁹ *Iqbal*, 556 U.S. at 677-80 (“where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not ‘show[n]’—‘that the pleader is entitled to relief’”) (quoting FED. R. CIV. P. 8(a)(2)).

²⁰ Sean B. Karunaratne, Note, *The Case Against Combating BitTorrent Piracy Through Mass John Doe Copyright Infringement Lawsuits*, 111 MICH. L. REV. 283, 284, 286-87 (2012).

²¹ *Compare* *Malibu Media LLC v. Gilvin*, No. 3:13-CV-72 JVB, 2014 WL 1260110, at *3 (N.D. Ind. Mar. 26, 2014) (“allegations that Defendant is the internet subscriber whose internet address was being used to distribute bits of Plaintiff’s movies make it plausible that he was the infringer. These allegations are not so sketchy or implausible that they fail to give Defendant sufficient notice of Plaintiff’s claim.”) *with* *Malibu Media, LLC v. Doe*, No. 1:14-cv-20213-UU (S.D. Fla. Mar. 19, 2014) (“Plaintiff has not established good cause for the Court to reasonably rely on Plaintiff’s usage of geolocation to establish the identity of the Defendant.”)

²² *Iqbal*, 556 U.S. at 677-80.

plausible.²³ Given that trend, copyright holders are turning once again towards intermediaries.²⁴

B. Targeting Intermediaries for Secondary Liability for Copyright Infringement

Copyright holders pursuing intermediaries (e.g., ISPs) for secondary liability for another's direct infringement face significant obstacles in the form of statutory safe harbors. The DMCA established statutory safe harbors for intermediaries that shield the ISPs from secondary liability.²⁵ Further, previous court decisions have strengthened and supported the position of ISPs benefitting from the statutory safe harbors.²⁶

The statutory safe harbors included in the DMCA are codified in 17 U.S.C. § 512(a)-(e). In order for an ISP to take advantage of the statutory safe harbors, the ISP must create and enforce a policy that prevents repeat copyright infringers from using the ISP's service and allows copyright holders to use "standard technical measures" to protect the holders' rights against infringement.²⁷ As long as an ISP satisfies this relatively low standard for eligibility, the ISP can take advantage of any of the several safe harbors that are described in the statute. The three most relevant safe harbors for protecting ISPs from secondary liability²⁸ are: passive conduits,²⁹ providers storing materials,³⁰ and information location tools.³¹

The passive conduit safe harbor protects an ISP from liability if the infringing activity is carried out using the ISP's network at the direction of someone else, i.e., the ISP's customer.³² The storing materials safe harbor protects an ISP from liability for infringement if infringing material is stored using the ISP's network so long as the storage is carried out at the direction of someone else, i.e., the customer, and the ISP is unaware that the stored material is infringing.³³ The information location tools safe harbor protects an ISP from infringement liability based on providing a link to infringing material so long as the ISP was unaware that the content was infringing and the ISP does not directly benefit financially from linking the

²³ See *infra* Part II.

²⁴ See *infra* Part III.

²⁵ See generally 17 U.S.C. § 512(a)-(e) (2010).

²⁶ See, e.g., *Viacom Int'l v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012).

²⁷ See 17 U.S.C. § 512(i) (2010).

²⁸ See PATRICIA L. BELLIA ET AL., *CYBERLAW: PROBLEMS OF POLICY AND JURISPRUDENCE IN THE INFORMATION AGE* 354-55 (5th ed. 2018).

²⁹ See 17 U.S.C. § 512(a) (2010).

³⁰ See *id.* § 512(c).

³¹ See *id.* § 512(d).

³² See *id.* § 512(a).

³³ See *id.* § 512(c).

material.³⁴ The low bar set by Congress for eligibility for the statutory safe harbors as well as the broad protections that the safe harbors offer combine to create an effective barrier for ISPs against copyright holder claims of secondary liability.

II. COURTS HAVE BECOME SKEPTICAL OF USING IP ADDRESSES TO LINK INDIVIDUALS TO INFRINGING ACTS

Online copyright infringement, colloquially called “piracy,” has exploded in popularity with the widespread adoption of the internet. To combat copyright infringement and the lost sales associated with piracy, copyright holders focused initially on suing the companies that created tools to facilitate copyright infringement.³⁵ While copyright holders were often successful at shutting down the sharing websites and removing potentially harmful sharing tools,³⁶ the strategy was unable to stop digital piracy. As one service or sharing tool would get shut down, another would be ready to step in and fill the void.³⁷ Recognizing that copyright infringement could not be prevented simply by eliminating sharing websites and tools in a whack-a-mole fashion, copyright holders began to target the copyright infringers directly.³⁸

The aggressive litigation strategy the copyright holders and their representatives used, particularly the Recording Industry Association of America (“RIAA”), frightened average citizens who had illegally downloaded music or movies into paying settlements.³⁹ Some consumers fought back against the accusations of copyright infringement and were successfully able to get the lawsuits that had been filed against them dismissed, but at great personal expense.⁴⁰ Recently, copyright holders began using (or abusing) permissive joinder under Rule 20,⁴¹ in order to create large, unwieldy cases with upwards of a thousand (or more) unnamed defendants.⁴² With a lawsuit filed against only an IP address, a copyright holder could then use the subpoena provision under 17 U.S.C. §512(h) in order to force

³⁴ See *id.* § 512(d).

³⁵ See Olufunmilayo B. Arewa, *Youtube, UGC, and Digital Music: Competing Business and Cultural Models in the Internet Age*, 104 NW. U. L. REV. 431, 444 (2010).

³⁶ See, e.g., *A&M Records v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

³⁷ See, e.g., *MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005).

³⁸ See Arewa, *supra* note 35, at 444-45.

³⁹ *Id.* at 445-46. (The total amount of money alleged infringers paid to the RIAA eclipsed \$100 million).

⁴⁰ See, e.g., *Capitol Records, Inc. v. Foster*, No. Civ. 04-1569-W, 2006 WL 4558154 (W.D. Okla. July 13, 2006).

⁴¹ FED. R. CIV. P. 20.

⁴² See, e.g., *VPR Int'l v. Does 1-1017*, No. 11-2068, 2011 WL 8179128 (C.D. Ill. Apr. 29, 2011).

ISPs to provide copyright holders with the names of the account holders associated with the IP addresses that, allegedly, infringed the copyright.⁴³ Once the copyright holder had a name to associate with the IP address the copyright holder could continue the suit or attempt to settle without further litigation. By naming more than a thousand defendants in a suit, a copyright holder assumes that at least some of the defendants will settle or lose in litigation, thus justifying the cost of the suit as well as providing the copyright holder with a tidy sum for their efforts.

A. District Court Body Blows Against Copyright Holders

Using the strategy of pursuing individual infringers, copyright holders have generally been successful in district courts across the country.⁴⁴ However, a growing number of district courts have grown concerned with the way copyrights holders have been playing fast and loose with the *Twombly*⁴⁵ and *Iqbal*⁴⁶ pleading standard as it relates to using IP addresses to identify individuals for purposes of a lawsuit.⁴⁷ Several district courts issued decisions rebuking the use of IP addresses to identify individual copyright infringers.⁴⁸

In *In re BitTorrent*, the court expressed its suspicions that an IP address can be used to identify an individual infringer using an analogy.⁴⁹ The judge wrote “it is no more likely that the subscriber to an IP address carried out a particular computer function . . . than to say an individual who pays the telephone bill made a specific telephone call.”⁵⁰ It is wrong to assume that an account holder is the copyright infringer simply because the IP address of the infringer is associated with the account holder’s account.⁵¹ Further, the judge wrote “while the ISPs will provide the name of its subscriber, the alleged infringer could be the subscriber, a member of his or

⁴³ *Id.*

⁴⁴ See Adam Langston, Note, *Return of the John Doe: Protecting Anonymous Defendants in Copyright Infringement Actions*, 41 STETSON L. REV. 875, 876–77 (2012).

⁴⁵ See generally *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007).

⁴⁶ See generally *Ashcroft v. Iqbal*, 556 U.S. 662 (2009).

⁴⁷ See Langston, *supra* note 44, at 893–95.

⁴⁸ See, e.g., *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80 (E.D.N.Y. 2012), report and recommendation adopted sub nom. *Patrick Collins, Inc. v. Doe 1*, 288 F.R.D. 233 (E.D.N.Y. 2012); see also *AF Holdings LLC v. Doe*, No. 2:12-cv-5709-ODW(JCx), 2012 WL 12884893 (C.D. Cal. Oct. 19, 2012); see also *AF Holdings LLC v. Rogers*, No. 12cv1519 BTM(BLM), 2013 WL 358292 (S.D. Cal. Jan. 29, 2013); see also *Elf-Man, LLC v. Cariveau*, No. C13-0507RSL, 2014 WL 202096 (W.D. Wash. Jan. 17, 2014).

⁴⁹ See *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. at 84. *Patrick Collins, Inc.*, 288 F.R.D. 233.

⁵⁰ *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. at 84.

⁵¹ *Id.*

her family, an employee, invitee, neighbor or interloper.”⁵² Again, the IP address tells the copyright holder no information about who is actually using the computer to infringe the copyright. While it is certainly possible that the infringing act was committed by the account holder, it is not plausible that the act was committed by the account holder without additional facts that support that assertion.

In *AF Holdings LLC v. Doe*, the court echoed the same sentiment that was expressed by the Eastern District of New York in *In re BitTorrent*.⁵³ The judge writes “[a]n IP address alone may yield subscriber information, but that may only lead to the person paying for the internet service and not necessarily the actual infringer, who may be a family member, roommate, employee, customer, guest, or even a complete stranger.”⁵⁴ Thus, the account holder is not necessarily the same individual who committed the alleged copyright infringement. Here, the judge goes further and discusses the implications of the decision if he had ruled differently. He states:

given the subject matter of [the] accusations and the economics of defending such a lawsuit, it is highly likely that the subscriber would immediately pay a settlement demand—regardless whether the subscriber is the actual infringer. This Court has a duty to protect the innocent citizens of this district from this sort of legal shakedown.⁵⁵

The judge’s strong words illustrate what motivated his decision—protecting members of the public from unscrupulous copyright holders who have been able to extract large settlements from fearful defendants for more than a decade.⁵⁶

In *AF Holdings LLC v. Rogers*, the court directly addresses the link, or lack thereof, between an IP address and the identity of an account holder with an ISP.⁵⁷ The judge writes that:

[the] Court is concerned about the lack of facts establishing that Defendant was using that IP address at that particular time. Indeed, the [Plaintiff] does not explain what link, if any, there is between Defendant and the IP address. . . . just because an IP address is registered to an individual does not mean that he or she is guilty of infringement when that IP address is used to commit infringing activity.⁵⁸

In other words, the plaintiff did not allege sufficient facts to make the claim of copyright infringement plausible on its face. Additionally, the judge

⁵² *Id.*

⁵³ *AF Holdings LLC v. Doe*, No. 2:12-cv-5709-ODW(JCx), 2012 WL 12884893, at *1 (C.D. Cal. Oct. 19, 2012).

⁵⁴ *Id.*

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ *AF Holdings LLC v. Rogers*, No. 12cv1519 BTM(BLM), 2013 WL 358292, at *2 (S.D. Cal. Jan. 29, 2013).

⁵⁸ *Id.*

expressed a concern about punishing the wrong individuals. He writes “[d]ue to the risk of ‘false positives,’ an allegation that an IP address is registered to an individual is not sufficient in and of itself to support a claim that the individual is guilty of infringement.”⁵⁹ Thus, much like the court in *AF Holdings LLC v. Doe*, the court in *AF Holdings LLC v. Rogers* expresses a concern about protecting the public from false findings of guilt founded on suspect factual allegations.

Finally, in *Elf-Man, LLC v. Cariveau*, the court reiterates what several other district courts have previously held. The judge writes:

simply identifying the account holder associated with an IP address tells us very little about who actually downloaded [the movie] using that IP address. While it is possible that the subscriber is the one who participated in the [infringing conduct], it is also possible that a family member, guest, or free-loader engaged in the infringing conduct.⁶⁰

In other words, identifying the account holder associated with a particular IP address provides incomplete information about who actually committed the copyright infringement. While it is possible that the account holder committed the infringement, it is just as likely someone else who uses the same internet network as the account holder committed the act. In sum, an IP address is not sufficient to make a claim of copyright infringement plausible on its face. Thus, any claim of copyright infringement based solely on an IP address associated with an account holder must necessarily fail the pleading standard set by *Twombly* and *Iqbal*.

Overall, the above selected cases illustrate a shift in judicial opinion concerning the use of IP addresses to identify individual copyright infringers. Since the passing of the DMCA, copyright holders have benefited from a concerning, simple method for holding alleged copyright infringers responsible. One could simply record the alleged infringer's IP address, obtain the identity of the account holder associated with that IP address from an ISP, threaten or file suit against that individual, and then wait for the settlement or secure an easy victory in court. Not until recently has the judiciary taken a careful look at what is actually occurring in these copyright infringement cases when account holders are held responsible for the actions taken by someone using their IP address. Once members of the judiciary had a firm grasp on the theory behind the jump that plaintiffs were making from IP address to account holder, the courts stepped in and have (mostly) corrected the issue. However, without the intervention of an appellate court, the district court decisions preventing copyright holders from using IP addresses to identify copyright infringers would remain

⁵⁹ *Id.* at *3.

⁶⁰ *Elf-Man, LLC v. Cariveau*, No. C13-0507RSL, 2014 WL 202096, at *2 (W.D. Wash. Jan. 17, 2014).

disjointed.

B. *The Ninth Circuit's Knockout Punch*

Though the idea that an IP address is not sufficient to identify an individual for purposes of the *Twombly* and *Iqbal* pleading standard was gaining traction in the district courts, it was a decision out of the Ninth Circuit Court of Appeals that dealt the final blow to copyright holders seeking to hold individual infringers liable.

The Ninth Circuit Court of Appeals in *Cobbler Nevada v. Gonzalez* held that the copyright holder's claim of direct infringement must fail the *Twombly* and *Iqbal* pleading standard.⁶¹ Judge McKeown wrote the defendant's "status as the registered subscriber of an infringing IP address, standing alone, does not create a reasonable inference that he is also the infringer."⁶² As multiple district courts have previously held, the tenuous link between the IP address of an infringer and the account holder associated with that IP address is just not strong enough to support a legal claim against a defendant.⁶³ Further, the judge stated "simply establishing an account does not mean the subscriber is even accessing the internet, and multiple devices can access the internet under the same IP address."⁶⁴ Here, the court introduces an additional degree of doubt concerning the link between the IP address and the account holder. Since multiple individuals can access the internet under the same IP address, it is not possible to determine what acts an individual committed online using only an IP address. There is just no way to tell what person is behind that IP address without additional information.

Judge McKeown understood the difficult position that copyright holders are in when it comes to proving a particular individual committed an act of infringement online when the only evidence available is an IP address. However, the judge balanced that consideration with what the law requires and wrote "this complication does not change the plaintiff's burden to plead factual allegations that create a reasonable inference that the defendant is the infringer."⁶⁵ Though the state of the law leaves no simple way for a copyright holder to support a claim that a particular individual infringed a copyright using a particular IP address, as seen in *Cobbler Nevada*, the judiciary has been generally unsympathetic (i.e., too bad for the copyright holders).⁶⁶ Judge McKeown's holding in *Cobbler Nevada* represents the

⁶¹ *Cobbler Nevada, LLC v. Gonzales*, 901 F.3d 1142, 1145 (9th Cir. 2018).

⁶² *Id.*

⁶³ *See supra* Part II.A.

⁶⁴ *Id.* at 1146.

⁶⁵ *Id.* at 1146-47.

⁶⁶ *See supra* Part II.A.

strongest and most persuasive rebuke of using IP addresses to identify individual copyright infringers and effectively eliminates the possibility for copyright holders to use this strategy again in the future.

The Ninth Circuit Court of Appeals decision in *Cobbler Nevada* represents the culmination of all the scattered district court decisions seeking to prevent individuals from being taken advantage of by copyright holders. The weight of an appellate court decision lends additional credibility to the district court decisions decided using the same rationale and thought process. *Cobbler Nevada* is the final nail in the coffin of copyright holders using IP addresses to identify individual copyright infringers.

III. COPYRIGHT HOLDERS TARGET INTERMEDIARIES (AGAIN)

Given that copyright holders have effectively lost the ability to go after individual infringers following the Ninth Circuit Court of Appeals decision in *Cobbler Nevada*, copyright holders will likely (once again) set their sights on intermediaries, specifically ISPs. Copyright holders have previously sued intermediaries for copyright infringement with varying degrees of success.⁶⁷ Copyright holders have been generally unsuccessful when suing ISPs for copyright infringement under a secondary theory of liability.⁶⁸ However, a recent decision from the Fourth Circuit provides a glimmer of hope that copyright holders can defeat the statutory safe harbor provisions provided to intermediaries under the DMCA.⁶⁹

A. Internet Intermediary Liability and Safe Harbors Case Law Development

The trouble that copyright holders have in suing intermediaries generally is illustrated by the court's decision in *Viacom Int'l v. YouTube, Inc.*⁷⁰ The broad protections offered by the DMCA to intermediaries are difficult to surmount. Without overcoming the DMCA safe harbor protections, it is nearly impossible for a copyright holder to hold an intermediary (specifically an ISP) liable for copyright infringement based on a theory of secondary liability.

In *Viacom*, the court addressed the storing materials safe harbor

⁶⁷ *A&M Records, Inc. v. Napster, Inc.*, 284 F.3d 1091 (9th Cir. 2002); *see also* *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007).

⁶⁸ *See e.g.*, *UMG Recordings v. Veoh Networks Inc.*, 93 U.S.P.Q. 2d 1010 (C.D. Cal. Sept. 11, 2009).

⁶⁹ *BMG Rights Mgmt. (US) LLC v. Cox Commc'ns Inc.*, 881 F.3d 293 (4th Cir. 2018).

⁷⁰ *Viacom Int'l v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012).

provided to intermediaries under 17 U.S.C. § 512(c).⁷¹ The court held an intermediary was disqualified from asserting the safe harbor if they had “actual knowledge or awareness of facts or circumstances indicating specific and identifiable infringements.”⁷² In short, the court set the bar for disqualification from the statutory safe harbor incredibly high. Not only does the court require “actual knowledge,” but “actual knowledge” of “specific infringements.”⁷³ Given this high bar, it would be difficult for an intermediary to be disqualified from protection under this safe harbor.

The *Viacom* decision only directly addressed the storing materials safe harbor provision. However, the Second Circuit Court of Appeals strong aversion to stripping YouTube of safe harbor protections indicates that the court’s opinion in *Viacom* is illustrative of how modern courts may generally address protection for intermediaries under any of the statutory safe harbors. Based on the decision of the court in *Viacom*, it will likely be extremely difficult to defeat the safe harbor protections offered by the DMCA and find intermediaries liable for copyright infringement.

B. A Chink in the Safe Harbor Armor?

The uphill battle that copyright holders face in holding ISPs accountable for the infringing activities of their subscribers has not prevented copyright holders from trying to litigate the issue. A recent case demonstrates that targeting intermediaries for copyright infringement may, in fact, be a viable option despite the strong safe harbor protections that intermediaries enjoy.

In *BMG Rights Mgmt. (US) LLC v. Cox Commc’ns, Inc.*, the Fourth Circuit Court of Appeals found that Cox was not entitled to DMCA safe harbor protection.⁷⁴ In order to qualify for safe harbor protection, an intermediary must “adopt[] and reasonably implement[] . . . a policy that provides for the termination in appropriate circumstances of subscribers . . . who are repeat infringers.”⁷⁵ Here, the court found that Cox was effectively not enforcing its own termination policy for repeat infringers.⁷⁶ Since Cox was not enforcing its own termination policy, the court found that Cox was not “implementing” a termination policy as required by the DCMA for the safe harbor and thus not entitled to protection.⁷⁷ While the *BMG Rights Mgmt.*

⁷¹ *Id.* at 25.

⁷² *Id.* at 30 (international quotations and edits omitted).

⁷³ *Id.*

⁷⁴ *BMG Rights Mgmt. (US) LLC v. Cox Commc’ns, Inc.*, 881 F.3d 293, 305 (4th Cir. 2018).

⁷⁵ *Id.* at 301 (quoting 17 U.S.C. § 512(i)(1)(A)).

⁷⁶ *Id.* at 303.

⁷⁷ *Id.*

case provides an extreme example of what will disqualify an ISP from safe harbor protection, it does show that the safe harbor armor is vulnerable to attack and puts ISPs on notice that they are not untouchable.

Thus, the court's decision in *BMG Rights Mgmt.* is important, not necessarily for the end result, but instead for the message that the decision sends to copyright holders and ISPs. Copyright holders, who all but completely lost the ability to pursue individual infringers following *Cobbler Nevada*, may now have another way to recover for copyright infringement. The avenue that copyright holders thought was closed off by statutory safe harbors may in fact be more accessible than first thought. At a minimum, the decision in *BMG Rights Mgmt.* shows that the statutory safe harbors are not immune to attack, and that ISPs can lose their safe harbor protections. Instead of targeting individual infringers, copyright holders are likely to resurrect their fight against intermediaries.

IV. FORECASTING THE SOLUTION TO THE COPYRIGHT HOLDERS' QUANDARY

Following *Cobbler Nevada*, copyright holders have limited legal options in terms of recovering for copyright infringement. The strategy of pursuing individual copyright infringers that had worked since the DMCA passed is now, more than likely, not going to work. Courts are no longer buying the argument that you can identify an individual infringer based solely on an IP address.⁷⁸ The next best option for copyright holders is to (once again) try to recover from intermediaries—specifically, ISPs. In my view, *BMG Rights Mgmt.* was a test case. Copyright holders wanted to see if it was possible to crack the safe harbor armor provided to ISPs by the DMCA. The experiment worked. The *BMG Rights Mgmt.* case showed that it is possible for an ISP to lose their safe harbor protection.

Moving forward, it is likely that more cases like *BMG Rights Mgmt.* will be brought against ISPs. Further, copyright holders have a decent chance of succeeding in the suits that they bring. Copyright holders have tried and failed in the past to hold intermediaries liable for copyright infringement, but copyright holders have shown (with *BMG Rights Mgmt.*) that they can learn from their past failures and develop winning strategies for holding ISPs liable for copyright infringement.

The single biggest factor that weighs in the favor of copyright holders in their battle against ISPs is the rapid change in technology that has happened over the past decade or so (e.g., the capability of ISPs to better monitor for the presence of infringing material). With the degree to which technology has changed, there is an argument to be made that ISPs could use technology to do more to prevent or catch copyright infringement. With the

⁷⁸ See *supra* Part II.

technology changes, courts could find that ISPs should be doing more to earn their statutory safe harbor protections besides merely terminating users who repeatedly infringe copyrights.⁷⁹ Technology has changed, and ISPs should have to keep up with the pace in order to keep benefitting from their statutory safe harbor protections.

Inevitably, copyright holders will find a way to recover for copyright infringement. Based on the Ninth Circuit's decision in *Cobbler Nevada* and the Fourth Circuit's decision in *BMG Rights Mgmt.*, copyright holders will move in the direction of pursuing intermediaries (specifically, ISPs) and move away from pursuing individual copyright infringers.

CONCLUSION

Since the passing of the DMCA in 1998, copyright holders have generally pursued individual copyright infringers in lieu of pursuing the ISPs that facilitate online copyright infringement. A recent shift in how the judiciary handles copyright holders targeting alleged individual infringers has largely left copyright holders unable to pursue suits against individual infringers. As a result of the courts limiting copyright holders from pursuing alleged individual infringers, rights holders are once again targeting ISPs under a theory of secondary liability for copyright infringement. A recent case has shown that ISPs are not invulnerable to secondary liability for copyright infringement as was previously believed due to the protection of ISPs under statutory safe harbors. In the future, we are more likely to see additional suits against ISPs as opposed to individual infringers due to the increased difficulty of pursuing individual infringers and the recent discovery that the ISPs' safe harbor protections are susceptible to attack.

⁷⁹ 17 U.S.C. § 512(i) (2010).