16-1972

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

BMG RIGHTS MANAGEMENT (US) LLC, and ROUND HILL MUSIC LP,

Plaintiff–Appellees,

v.

COX COMMUNICATIONS, INC. and COXCOM, LLC,

Defendants–Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA, ALEXANDRIA DIVISION

BRIEF OF *AMICUS CURIAE* INTERNET COMMERCE COALITION IN SUPPORT OF DEFENDANTS-APPELLANTS' APPEAL SEEKING REVERSAL

Andrew L. Deutsch
DLA PIPER LLP (US)
1251 Avenue of the Americas
New York, NY 10020
(212) 335-4500

RULE 29(c)(5) STATEMENT

Pursuant to Fed. R. App. P. 29(c)(5), *amicus curiae* states that no party's counsel authored the brief in whole or in part; no party's counsel contributed money that was intended to fund preparing or submitting the brief; and no person—other than *amicus*, its members, or its counsel—contributed money that was intended to fund preparing or submitting the brief.

STATEMENT OF CONSENT TO FILE *AMICUS* BRIEF

All parties to this appeal have consented to the filing of this *amicus curiae* brief.

CORPORATE DISCLOSURE STATEMENT

The Internet Commerce Coalition is a nonprofit corporation incorporated under the laws of Maryland. It has no parent corporation, and no publicly held corporation owns 10 percent or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

17 U.S.C.:

TABLE OF AUTHORITIES

Page(s)

CASES

OTHER AUTHORITIES

INTEREST OF *AMICUS CURIAE*

The Internet Commerce Coalition ("ICC") works to promote policies that allow Internet service providers, their customers, and other users to do business on the global Internet under reasonable rules governing liability and use of technology that encourage the growth of this vital medium. The Coalition's members include a cross-section of leading Internet service providers and e-commerce companies and trade associations. The ICC has an interest in ensuring that Congress's comprehensive regulation of copyright obligations on the Internet, and the nationally-applicable safe harbor procedures of the Digital Millennium Copyright Act ("DMCA"), are applied in accordance with Congress's intention to foster growth of the Internet with a minimum of regulation, and promoting a consistent construction of the DMCA throughout the United States.

Many of the ICC's members are what is commonly called "conduit ISPs"– companies that provide broadband Internet access or Internet backbone transmission services and that route user communications from sender to recipient. Conduit ISPs do not store information. Internet access provider conduit ISPs are only able to identify the primary account holder of an Internet access account. They do not have the practical ability, consistent with privacy obligations and the volume of communications, to examine content during the minimal time it is transmitted through their systems, much less to check for potential infringement of

a third-party's intellectual property rights. They cannot remove or disable access to allegedly infringing material as it passes through their networks. And they cannot examine material stored on their subscribers' computers.

In enacting the DMCA, Congress recognized the special circumstances and importance of conduit ISPs and created a separate safe harbor for them (17 U.S.C. § 512(a)). Unlike the other DMCA safe harbors, the § 512(a) safe harbor does not require the conduit ISP to process or even accept requests from copyright owners or their agents to take down allegedly infringing content, although such requests are integral to the operation of other DMCA safe harbors.

ICC submits this *amicus* brief because the appealed-from decisions and judgment of the Eastern District of Virginia erroneously interpreted the § 512(a) safe harbor, as well as the requirement of 17 U.S.C. § 512(i) that to benefit from any of the DMCA safe harbors, a conduit ISP must adopt and reasonably implement a policy that requires the termination of repeat copyright infringers in appropriate circumstances. This mistaken interpretation ignores the language and structure of the DMCA, Congressional intent, and the practical limitations that conduit ISPs face in addressing infringement. These errors lie at the heart of the district court's denial of Cox's summary judgment motion and its post-trial motion.

Unless the erroneous rulings below are addressed and reversed by this Court, the ICC members, as well as many other conduit ISPs, will face a greatly

heightened risk of infringement liability simply because persons (including those who are not their customers or subscribers) have routed potentially infringing communications through the ISPs' systems. The negative consequences of affirmance would not fall only on conduit ISPs. In the twenty-first century digital economy, the Internet is vital to communication, business and entertainment. It is how people access culture, speak their political beliefs, communicate with friends, and conduct business. If the decision below is not reversed, conduit ISPs, when they receive unverified, machine-generated infringement claims from profit-seeking agents of copyright holders, will be strongly incentivized to cut off vital Internet service to users, rather than face costly damages suits. This is not the system Congress intended when it enacted the DMCA, and it should not be one imposed through a misinterpretation of Congress's plain words.

ARGUMENT

I

THE DMCA DOES NOT REQUIRE CONDUIT ISPS TO RECEIVE OR PROCESS TAKEDOWN NOTICES THAT PURPORT TO COMPLY WITH § 512(c) OF THE COPYRIGHT ACT

A. Historical Context

The decision below threatens to unbalance the statutory compromise worked out by Congress in 1998 between the interests of copyright owners and those of service providers and the customers they serve. The World Wide Web, which permits computer users to use the Internet to access documents and other digital files stored in remote locations, became broadly available to ordinary users with the mid-1990's release of the Netscape web browser software. Almost immediately, there ensued a boom in websites and e-commence began its rapidly increasing expansion. Existing and new service providers rose to meet this growing demand, including companies that provided Internet access to millions of individual users, businesses, and educational institutions.

The vast majority of Internet activity then (and now) raises no copyright concerns. However, like previous communications technologies, Internet technologies can be misused by consumers, including for purposes of committing copyright infringement. Courts quickly recognized that imposing infringement liability on service providers because they provided the technology making

Internet communications and websites possible was not appropriate. As one influential decision said, "[w]here the infringing subscriber is clearly directly liable for the same act, it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the Internet." *Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc.*, 907 F. Supp. 1361, 1372 (N.D. Cal. 1995) (declining to impose direct liability on an ISP where all infringing acts were those of the user).

Because the risks of infringement litigation could stunt the growth of the Internet, Congress concluded that a systematic, nationwide approach was needed to protect both the Internet economy and the rights of creators. Congress' solution was enacted into law in 1998 as part of the DMCA and codified as 17 U.S.C. § 512. The motivating principle behind § 512 was clear: Congress "was loath to permit the specter of liability to chill innovation that could also serve substantial socially beneficial functions," and decided that "'by limiting [service providers'] liability,' it would 'ensure[ ] that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand.'" *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1020 (9th Cir. 2013) (quoting S. Rep. 105-190, at 8 (1998)); *see also Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 82 (2d Cir. 2016).

B. The Statutory Safe Harbors

The core of § 512 is a series of safe harbor limitations for service providers against monetary liability for copyright infringement where specified criteria are met and where the service providers adopt and reasonably implement a policy of terminating repeat infringers in appropriate circumstances.

Congress tailored these safe harbors, and the requirements for qualifying under them, with recognition that different types of service providers have differing relationships with, and differing abilities to control, the user-transmitted or user-stored content that interacts with their systems. The safe harbor at issue in this appeal is 17 U.S.C. § 512(a), which applies to conduit ISPs that transmit, route or provide connections for third-party material through their systems, and do not retain any copies of that material for more than the interval necessary for the ISPs' processing, routing and transmitting functions.

The three other safe harbors deal with service providers who have more control over allegedly infringing material: those that provide system caching that permits quicker delivery of the material to user requests (§ 512(b)); those that provide longer-term storage of material posted by third parties, such as web hosts (§ 512(c)); and those that provide hyperlinks to material posted elsewhere, such as in search engine results or a directory. (§ 512(d)). What these latter three safe harbors have in common is a requirement that if a copyright owner or its agent

delivers a notification that identifies material stored on the service provider's system that is infringing and complies with other criteria, the service provider must remove or disable access to ("take down") the material. These other three safe harbors also contain an important safeguard against false allegations of infringement: if the user timely disputes the claim of infringement with a counter-notification, the service provider may restore access to the material, unless the copyright owner timely pursues the infringement claim directly against the subscriber in court. The online service provider that complies with these procedures is immunized from monetary liability for copyright infringement. *See* § 512(c), (g). Crucially for purposes of this appeal, Congress did not make this notification-removal-counter-notification procedure applicable to the §512(a) safe harbor for conduit ISPs, and created no counter-notification safeguard against inaccurate infringement notices in § 512(a).

Finally, to be eligible for the safe harbors, all service providers, including those who are conduit ISPs, must meet two conditions. The condition relevant to this appeal is found in § 512(i), which requires the service provider to have "adopted and reasonably implemented," and inform users of, "a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers." This provision does not specify what the repeat infringer policy must

be, nor define what it means to "reasonably implement[]" the policy, what are "appropriate circumstances," or who is a repeat infringer. As shown below, use of general rather than specific language was a deliberate choice by Congress, to afford service providers maximum flexibility in dealing with the problem of repeat infringement.

C. A Conduit ISP Does Not Forfeit The 512(a) Safe Harbor By Declining To Receive or Not Acting on Purported § 512(c) Notices

Appellant Cox is a conduit ISP and in the court below it claimed the safe harbor protection of § 512(a). JA-704-05. To be eligible for any of the DMCA safe harbors, a service provider must show that it "adopted and reasonably implemented . . . a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers." 17 U.S.C. § 512(i)(1)(A).

The district court rejected this defense on several grounds. The first relied on a finding that Cox failed or refused to process alleged DMCA takedown notices from copyright holders or their agents. JA 684-85, 719. The district court found that this factual finding was evidence that Cox had failed to "implement" its repeat infringer policy as required by § 512. The court asserted that "implementation" requires a conduit ISP to show, among other things, that it has "'a procedure for dealing with DMCA-compliant notifications.'" JA-705 (quoting *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1109 (9th Cir. 2010) ("*CCBill*")).

This conclusion was an erroneous interpretation of the law that failed to follow well-settled rules of statutory construction. Federal statutes are to be interpreted to give effect to Congress's intent. *United States v. Abdelshafi*, 592 F.3d 602, 607 (4th Cir. 2010). If the statutory language is unambiguous, the plain meaning of the words is applied unless there is a clearly express contrary legislative intent. *Id.* at 607. To determine whether the language of a statute is plain, the court must look to the language itself, its context, and the context of the statute as a whole. *Holland v. Big River Minerals Corp.* 181 F.3d 597, 603 (4th Cir. 1999). Courts should avoid reading limitations into rights granted by statute where Congress has not done so expressly. *United States v. Murphy*, 35 F.3d 143, 145 (4th Cir. 1994).

The district court erred by failing to apply the plain meaning rule. The DMCA unambiguously states that if an ISP meets the statutory definition of a conduit contained in § 512(a)(1)-(5), it "shall not be liable for monetary relief, or, except as provided in subsection (j), for infringement of copyright," by reason of its routing, transmitting or providing connections or transient storage for material carried in a third-party communication. *Id.* § 512(a). The § 512(a) safe harbor is not conditioned on the conduit ISP receiving and complying with notices of infringement from copyright owners and their agents, nor is it lost by an assertion

that the ISP knew or should have known that material passing through its system was infringing.

In contrast, as described above, Congress conditioned the other three DMCA safe harbors on a service provider processing and complying with proper infringement notices and acting without actual or "red flag" knowledge of infringement. 17 U.S.C. § 512(b) (service provider is not liable for system caching provided that it observes the "conditions" in § 512(b)(2) and removes or disables access to material upon receipt of a § 512(c)(3) notice of infringement and/or information that the material has already been removed from an originating site); §512(c) (safe harbor for service provider that stores material at the direction of users conditioned on absence of actual knowledge of infringement or facts from which infringement is apparent, and compliance with § 512(c)(3) notices of infringement); § 512(d) (safe harbor for service provider that provides information location tools similarly conditioned on compliance with § 512(c)(3) notices by removing links and absence of known or apparent infringement).

Congress's decision not to require compliance with § 512(c)(3) notices, or impose an actual or "red flag" knowledge requirement on conduit ISPs, was not an oversight. Conduit ISPs are different. Congress's differing treatment of the § 512(a) safe harbor reflects a recognition that a conduit ISP either does not store content or does so for only a transient instant, and in either case is unable to act on

a copyright owner notice and remove – much less block – an infringing transmission. As the Eighth Circuit stated in *In re Charter Communications, Inc. Subpoena Enforcement Matter*, 393 F.3d 771, 776 (8th Cir. 2005) ("*Charter*"):

> The absence of the remove-or-disable access provision (and the concomitant notification provision) [from § 512(a)] makes sense where an ISP merely acts as a conduit for infringing material – rather than directly storing, caching or linking to infringing material – because the ISP has no ability to remove the infringing material from its system or disable access to the infringing material.

See also Recording Industry Ass'n of Am. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1234-35 (D.C. Cir. 2003) ("*RIAA*"); *Interscope Records v. Does 1-7*, 494 F. Supp. 2d 388, 391 (E.D. Va. 2007); *In re Subpoena to Univ. of N. Carolina at Chapel Hill*, 367 F. Supp. 2d 945, 955 (M.D.N.C. 2005).

It is also true that a conduit ISP, unlike a service provider host, in most cases does not know at any given time the identities of all the Internet users who are transmitting information over its system. In fact, because the Internet is a "network of networks," much, if not most, of the information transiting a conduit ISP's system at any given moment has not been generated by or originated with an account holder of the ISP. A conduit ISP can identify the Internet Protocol address ("IP address") of the device or group of devices that requested or sent a transmission at a particular date and may be able to correlate that information with a customer who is its primary account holder. However, an Internet access

provider typically has no visibility into what information is stored on the computers or other connected devices identified by that IP address. It therefore faces serious limitations on assessing whether the infringement claimed in a notice of infringement is colorably accurate or actually present. It has no ability to identify the actual user who made the transmission. In addition, a conduit ISP has no right to "take down" material on a user's computer in response to a § 512(c)(3) notice.

This recognition that § 512(c)(3) notices are not relevant to conduit ISPs is also shown by a separate section of the DMCA, § 512(h). This provision permits a copyright owner to apply to a federal court to issue a subpoena requiring a service provider to identify an alleged infringer. The application must contain a copy of a § 512(c)(3) notification. § 512(h)(2)(A). However, because conduit ISPs are not required to comply with § 512(c)(3) notifications, the D.C. Circuit, Eighth Circuit, and district courts have read § 512(h) as not authorizing subpoenas to conduit ISPs, and have denied or quashed §512(h) subpoenas directed to such ISPs. *See, e.g.*, *Charter*, 393 F.3d at 776; *RIAA*, 351 F.3d at 1234-35; *Interscope Records*, 494 F. Supp. 2d at 391; *In re Subpoena to Univ. of N. Carolina at Chapel Hill*, 367 F. Supp. 2d at 955.

Although the court below acknowledged that Congress did not require conduit ISPs to receive and process takedown notices in order to qualify for the

§ 512(a) safe harbor, JA-719 n. 19, it imposed virtually the same requirement on conduit ISPs by holding that a conduit ISP does not implement a repeat infringer termination policy under § 512(i), and is not eligible for the safe harbor, if it does not have "'a procedure for dealing with DMCA-compliant notifications.'" JA-705-06 (quoting *CCBill*, 488 F.3d at 1109).

There is no evidence that Congress, having exempted conduit ISPs from compliance with § 512(c)(3) notices in defining the § 512(a) safe harbor, silently reversed course and imposed a requirement of compliance on ISPs through the backdoor of § 512(i)(1). In fact, Congress included express language in § 512(m) stating that the safe harbor protections of § 512 are not to be construed as imposing affirmative obligations such as monitoring traffic or seeking out infringements on a service provider. The House Report explaining the DMCA, H.R. Rep 105-551(II), at 61 (1998) ("House Report"), directly connects the concepts of § 512(m) to the language of § 512(i), stating that the latter provision was not intended to "undermine the . . . knowledge standard of [§ 512(c)] by suggesting that a provider must investigate possible infringements, monitor its service, or make difficult judgments as to whether conduct is or is not infringing."

The structure of the statute also makes clear that § 512(i) did not condition a conduit ISPs' eligibility for the § 512(a) safe harbor on adopting a policy that requires termination of the accounts of customers who have been accused of

infringement in notices by rights holders or their agents. Section § 512(g) contains a detailed procedural protection for end users to challenge an inaccurate notice sent to a § 512(c) service provider via a counter-notification.[1] When properly made, a counter-notification permits the service provider to restore access to or replace the allegedly infringing material, unless the copyright owner timely commences an infringement action that seeks an injunction against access to the material. § 512(g)(2)(C). In contrast, there is no procedure in the statute for an Internet end user to challenge an inaccurate infringement notice sent to a § 512(a) service provider. If the district court's analysis were correct, the user would have no recourse against such a notice. A conduit ISP receiving multiple notices against an IP address would be required to terminate Internet service to all users (not just the primary account holder, but also his or her entire household) at that address. Congress could not have intended to impose this highly disruptive restriction, which would be far more punitive than mere blocking of access to a particular identified infringing file, *sub silentio*.

Moreover, a service provider must meet the § 512(i) conditions to qualify for *any* of the safe harbors. Under the reasoning of the district court, a conduit ISP would lose *all* protection under § 512(a) simply because it does not process notices

[1] The leading copyright treatise takes the view that the notification-takedown-counter-notification procedures also applies to the § 512(b) and (d) safe harbors. 4 Nimmer on Copyright § 12B.07[D][2] (2006).

that all other courts agree are irrelevant to the § 512(a) safe harbor. *See supra* at 11. In contrast, a service provider who claims the §§ 512(b), (c) or (d) safe harbor but ignores an accurate § 512(c) notice about an instance of infringement faces only exposure to a damages judgment for that single instance. Congress could not have intended to impose on conduit ISPs the dilemma of either terminating subscribers on the basis of allegations of infringement that may be reckless or inaccurate (because the conduit ISP has no means of verifying the accusations and end-users have no means of rebutting them through a counter-notification), or assuming potentially unlimited direct copyright liability.

The sole precedent cited by the district court for its conclusion also failed to find any language or intention in the statute to require conduit ISPs to handle and respond to notices of infringement. In *CCBill*, cited at JA-705-06, the Ninth Circuit did not undertake any analysis of how § 512(i) fits into the overall structure of the DMCA's safe harbors. Rather, citing a single district court case, it concluded that to "implement" a repeat infringer policy, any service provider must have "a procedure for dealing with DMCA-compliant notifications." 488 F.3d at 1009.

However, the district court decision cited in *CCBill* does not support this sweeping conclusion. In *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090 (W.D. Wash. 2004), *rev'd in part on other grounds, Cosmetic Ideas, Inc. v.*

IAC/Interactivecorp., 606 F.3d 612 (9th Cir. 2010), defendant Amazon asserted only the § 512(c) safe harbor for material stored at the direction of a user. *Id.* at 1109. Even so, *Corbis* did not hold that Amazon was required to comply with § 512(c)(3) notices in order to show that it satisfied § 512(i). The decision simply stated that a service provider carries its burden of showing that it reasonably implemented a policy to terminate repeat infringers where it demonstrates that it "adopted a procedure for receiving complaints and conveying those complaints to users." *Id.* at 1102. *Corbis* found that Amazon had properly implemented its policy because "Amazon does respond to allegations of copyright infringement," communicates complaints to users, and warns them of the risk of cancellation for repeated violations. *Id.* at 1103.

Corbis refused to read § 512(i) as requiring compliance with § 512(c) notices in order to "reasonably implement" a repeat infringer policy. The decision noted that in drafting § 512(i), Congress intentionally omitted the detail of the takedown notice provisions of § 512(c) and used less specific language, and that this choice demonstrated a legislative "intent to leave the policy requirements, and the subsequent obligations of the service providers, loosely defined." *Id.* at 1101. *Corbis* also concluded that "[a]ctual knowledge of blatant, repeat infringement cannot be imputed merely from the receipt of notices of infringement." *Id.* at 1105.

The reading of § 512(i) adopted in *Corbis*, unlike that of the court below or the overly broad statement in *CCBill*, is consistent with the DMCA's language, the overall structure of the DMCA online infringement provisions, and Congressional intent. Congress intentionally decided not to require conduit ISP compliance with § 512(c)(3) takedown notices in order to obtain the § 512(a) safe harbor. This deliberate choice recognized that the purpose of such notices is to permit removal or denial of access to stored infringing material. Conduit ISPs do not store material, but merely transmit it or route it to other systems or computers. They do not have the ability to examine the vast number of bits that pass through their systems and come to any conclusion about whether infringement is occurring, much less remove or block that material from the stream of communications. Nor can they look into end user computers, even where those users are their Internet access customers.

In reviewing the decision below, the Court should restore the lines that Congress drew and that the district court erased. It should rule that only service providers claiming the safe harbors of §§ 512(b)-(d) are required to process and comply with § 512(c)(3) takedown notices. Conduit ISPs are not required to comply with infringement notices by any provision of the DMCA. The court should find that a conduit ISP does not fail to reasonably implement a repeat infringer policy because it does not accept or take action on notices that purport to

comply with § 512(c)(3). Failing to reverse the erroneous reasoning below would mean that conduit ISPs would lose the protection of their special safe harbor, and, contrary to Congress's expressed intent, would face massive infringement liability merely for carrying out functions that are essential to the Internet.

II

A CONDUIT ISP DOES NOT ACQUIRE ACTUAL KNOWLEDGE OF INFRINGEMENT FROM RECEIPT OF § 512(c)(3) NOTICES

The decision below ignored another important difference between the § 512(a) safe harbor and those of §§ 512(c) and (d). Service providers can only avail themselves of the latter safe harbors where they do not have actual knowledge that material stored on their systems, or to which they provide links, is infringing, or "red flag" knowledge, namely knowledge of facts or circumstances from which infringement is apparent. §§ 512(c)(1)(A)(i); 512(d)(1)(A). However, Congress chose not to apply *any* knowledge disqualifiers to the conduit ISP safe harbor. The reason is that with actual or "red flag" knowledge, a storage or information location tool ISP can locate, remove or block access to infringing material on its own servers and thereby protect the interests of the copyright holder. Congress considered that for a service provider to allow such material to remain on its servers with confirmed or inescapable knowledge of a user's infringement would be sufficiently culpable to forfeit the safe harbor. House Report at 53-54. The conduit ISP, however, is differently situated. It "has no

ability to remove the infringing material from its system or disable access to the infringing material." *Charter*, 393 F.3d at 776. Accordingly, Congress chose not to condition the § 512(a) safe harbor on an ISP's lack of knowledge.

Notwithstanding this limitation, the district court held that purported § 512(c)(3) notices confer knowledge of infringement that may be used to strip a conduit ISP of its safe harbor. It ruled that a conduit ISP fails to reasonably implement its repeat infringer policy where it receives notices claiming repeated customer infringements and then fails to take steps to terminate the customer in appropriate circumstances. JA-706. The court noted that there was a split in judicial opinions as to whether copyright holder notices are enough to give a service provider actual knowledge of infringement, but jumped to the conclusion that at a minimum, such notices are "'powerful evidence of a service provider's knowledge.'" JA-719 (citation omitted).

The Court should reject this conclusion as inconsistent with the statutory language and structure. Beyond the intentional omission of a knowledge requirement in § 512(a), Congress also expressly prohibited notifications that fail to substantially comply with § 512(c)(3)(A) from being used as evidence that an ISP had actual knowledge of infringement. § 512(c)(3)(B)(i). A copyright holder or agent's notice to a conduit ISP, concerning material that is not stored on the conduit ISP's system, does not meet the requirements of § 512(c)(3)(A)(iii)

because it does not identify material "to be removed or access to which is to be disabled" by the ISP. *RIAA*, 351 F.3d at 1234-35. Accordingly, "any notice to an ISP concerning its activity as a mere conduit . . . is therefore ineffective." *Id.* at 1236. Such a notice to a conduit ISP provides no evidence of knowledge of infringement, and therefore cannot be used to show that the conduit ISP failed to comply with its repeat infringer policy.[2]

This conclusion is also supported by practical experience. Automated notices generated by computer systems and then sent by copyright owners to service providers *en masse*, such as the at least 1.8 million notices that Rightscorp sent to Cox, are by no means reliable evidence of actual infringement. As an example, many of the Rightscorp notices in this case alleged that a Cox user was making music files available for download, JA-722, 724, yet the district court found that "making available" is not an infringement of a copyright holder's exclusive rights. JA-727-32. The problem of unreliable notices is not unique to Rightscorp. Urban, Karaganis & Schofield, et. al., *Notice and Takedown in Everyday Practice*, at 2, 11-12 (2016), http://papers.ssrn.com/sol3/papers.cfm ?abstract_id=2755628, reported the results of a study of randomly selected takedown requests from a set of over 108 million requests. Over 4% of these

[2] Case law also rejects the view that a service provider that receives notices of infringement thereby obtains actual knowledge that the subject is infringing. *See, e.g., UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1025 (9th Cir. 2013).

notices targeted content that did not match the identified work; almost 30% were of questionable validity. Additional notices suggested possible fair use and questions as to whether the notifying entity owned the copyright or was authorized by the owner. What is more, in this very case, one of the plaintiffs was found to be asserting copyrights that it did not own. JA-704. The issuance of multiple such questionable notices against the same user or IP address is not sufficient to establish that the receiving ISP has actual knowledge that the subject is a repeat infringer.

III

THE DECISION BELOW INCORRECTLY APPLIED SECTION 512(I)(1)(a)'S "REPEAT INFRINGERS" REQUIREMENT

The opinion below concluded that Cox had failed to terminate "particular account holders who blatantly or repeatedly infringed," JA-718, and therefore forfeited its safe harbor. This was an improperly restrictive interpretation of the statutory language, and is incompatible with the remainder of § 512.

A notice sent by a copyright owner or its agent under §512, claiming that a user of a service provider's system or network is engaging in infringement, does not equate to a determination that the user is in fact an infringer. Just as a notice alleging infringement does not mean that a user is an infringer, multiple notices do not render a user a repeat infringer for purposes of § 512(i). The Act is careful to distinguish between "claimed infringement" and an "alleged infringer," on the one

hand, 17 U.S.C. §§ 512(b)(2)(E), (c)(1)(C), (c)(3)(A), (d)(3), (h)(1), and whether a user is, in fact, an infringer, on the other. § 512(i). *See* § 512(g)(1) (recognizing that material or activity claimed to be infringing may ultimately be determined not to be infringing). Nor do allegations of infringement trigger a duty on the part of the service provider to monitor its system or to make determinations of whether conduct is or is not infringing. *See* 17 U.S.C. § 512(m). The DMCA does not obligate a service provider to be judge, jury and executioner.

This is particularly true in the case of conduit ISPs, where the allegedly infringing material briefly transits the service provider's system, and by the time a notice was received, that material cannot be reviewed by the ISP in order to confirm or reject the claim of infringement. To put it plainly, the fact that Rightscorp or another agent for a copyright owner sends notices to an ISP alleging infringement does not mean that the subscribers whose IP addresses are identified in the notices are in fact infringers. *A fortiori*, it does not mean that where two or more such notices are sent against a single IP address, the users of that IP address are "repeat infringers" under § 512(i). A conduit ISP is not required to adopt a policy for the termination of accused "repeat infringers" on the basis of such notices, especially when there has been a long history of inaccurate accusations of infringement.

IV

THE DISTRICT COURT INCORRECTLY APPLIED THE "APPROPRIATE CIRCUMSTANCES" REQUIREMENT OF §512(i)

The district court effectively erased from the statute books the language of § 512(i)(1)(A) that to be eligible for its safe harbor, a service provider must provide "for the termination *in appropriate circumstances* of . . . repeat infringers." It held as a matter of law that "appropriate circumstances" always exist where an "account holder is repeatedly or flagrantly infringing copyright." (by which the court meant a user who is repeatedly accused in infringement notices). JA-718. This is manifestly incorrect as an ordinary matter of statutory interpretation. Had Congress wanted a service provider to be required to terminate whenever an "account holder is repeatedly . . . infringing copyrights," it would not have had to use the term "in appropriate circumstances." An interpretation of a statute that renders these statutory words superfluous is to be avoided at all costs. *Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253 (1992).

Congress clearly intended "in appropriate circumstances" to give service providers substantial flexibility in deciding how to deal even with persons believed to be repeated infringers. First, it recognized that not all user infringements – even repeated ones – should be deemed of equal gravity. House Report, at 61 ("The Committee recognizes that there are different degrees of on-line copyright infringement, from the inadvertent and noncommercial, to the willful and

commercial."). Second, it did not wish to impose a one-size-fits-all policy on service providers which are of widely varying purpose, size, and sophistication. Third, as described above, the termination of an entire household's Internet service is a draconian remedy. Making such termination mandatory would be inconsistent with Congress's decision to permit service providers to use their discretion in determining what are "appropriate circumstances" for termination, including considering other federal policies that recognize the critical nature of broadband services to American life and encourage providers to make those services more widely available.

Other courts have recognized that the "appropriate circumstances" language is not a straitjacket. It is instead a flexible standard that allows a service provider to take into account whether the proof of infringement is convincing or equivocal, and the seriousness of infringement that is actually proven. *See, e.g., Corbis*, 351 F. Supp. 2d at 1104 (a service provider does not fail to observe its own policy unless it is proven that it "fails to terminate a user even though it has sufficient evidence to create actual knowledge of that user's blatant, repeat infringement of a willful and commercial nature.").

Because the ruling below ignored Congress's own words and made "appropriate circumstances" into a requirement that any accused repeated infringer be immediately terminated, it was clearly erroneous. If the Court concludes, as

Cox contends, that only an adjudicated infringer can be a repeat infringer, then the Court should reverse and remand for entry of judgment in Cox's favor, because there was no evidence below that Cox failed to terminate any adjudicated infringer. If the Court concludes that adjudication is not a prerequisite to infringer status, it should reverse and remand for a redetermination of whether Cox qualifies for the § 512(a) safe harbor under a proper legal standard. The Court need not determine each and every circumstance that would constitute appropriate circumstances for a conduit ISP to invoke a repeat infringer termination policy. These inquiries are more appropriately matters for fact-finding at the district court level, which should include, for example, reception of expert testimony as to the limitations that conduit ISPs face in dealing with allegations of infringement.

CONCLUSION

For the foregoing reasons, the Court should reverse the judgment below and either (a) remand for entry of judgment for Cox or (b) remand for a redetermination of whether Cox qualifies for the § 512(a) safe harbor under a proper standard.[3]

---

[3] ICC also agrees with and asks the Court to adopt Cox's argument that under *Sony Corp. of Am. v. Universal City Studios*, 464 U.S. 417 (1984) and *Metro-Goldwyn-Mayer Studios Inc. v. Grokster Ltd.*, 545 U.S. 913 (2005), the district court erred by (1) failing to instruct the jury that an ISP should not be held to have contributory liability for its customers' infringing acts by making an Internet system that was capable of substantial non-infringing uses available to its customers, (2) permitting the case to go to the jury in the absence of any evidence

Respectfully submitted,

s/ Andrew L. Deutsch
ANDREW L. DEUTSCH
DLA Piper LLP (US)
1251 Avenue of the Americas
New York, NY 10020
(202) 335-4500
andrew.deutsch@dlapiper.com

---

that the ISP encouraged or induced customers to directly infringe copyrights, and (3) finding that *Sony* was inapplicable because the ISP "maintains an ongoing relationship with users." JA-2792. See Brief of Defendants-Appellants at 35-44.

CERTIFICATE OF COMPLIANCE WITH FED. R. APP. P. 32(a)(7)

Pursuant to Fed. R. App. P. 32(a)(7)(C), I, Andrew L. Deutsch, an attorney, certify that I have complied with the above-referenced rule, and that according to the word processor used to prepare this brief, Microsoft Word, this brief contains 5,963 words and therefore complies with the type-volume limitation of Rule 32(a)(7)(B) and (C).

Dated: November 14, 2016

s/ Andrew L. Deutsch
Andrew L. Deutsch

CERTIFICATE OF SERVICE

I, Andrew L. Deutsch, an attorney, certify that on this day the foregoing Brief for *Amicus Curiae* Internet Commerce Coalition was served electronically on all parties via CM/ECF.

Dated: November 14, 2016

s/ Andrew L. Deutsch
Andrew L. Deutsch