FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

IN RE: SUBPOENA OF INTERNET SUBSCRIBERS OF COX COMMUNICATIONS, LLC AND COXCOM, LLC	No. 24-3978 D.C. No. 1:23-cv-00426-JMS-WRP
CAPSTONE STUDIOS CORP.; MILLENNIUM FUNDING, INC.; VOLTAGE HOLDINGS, LLC, *Petitioners - Appellants*, v. COXCOM LLC, *Respondent - Appellee*.	OPINION

Appeal from the United States District Court
for the District of Hawaii
J. Michael Seabright, District Judge, Presiding

Argued and Submitted June 5, 2025
Honolulu, Hawaii

Filed August 15, 2025

Before: William A. Fletcher, Morgan B. Christen, and Roopali H. Desai, Circuit Judges.

Opinion by Judge Christen

SUMMARY*

Digital Millennium Copyright Act

The panel affirmed the district court's order quashing a subpoena sought by Capstone Studios Corp., a copyright holder, and issued pursuant to § 512(h) of the Digital Millennium Copyright Act ("DMCA") to CoxCom LLC, an Internet service provider.

Capstone sought to obtain the identities of 29 Cox subscribers whose IP addresses appeared to be showing pirated copies of Capstone's movie, *Fall*. Subsection 512(h) permits the clerk of any United States district court to issue a subpoena to a "service provider" on behalf of a copyright holder. Section 512 includes four safe harbors to limit service providers' liability for their users' infringements. Upon review, the district court concluded that Cox qualified for one of § 512's four safe harbors—17 U.S.C. § 512(a)—because Cox merely provided its users with an Internet connection and played no other role in the alleged infringement.

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

The panel addressed, as an issue of first impression, whether the DMCA allows a § 512(h) subpoena to issue to a § 512(a) service provider, who plays the role of a conduit for the communications of others, as opposed to a service provider who stores or provides a link to infringing material. Thus, a § 512(a) service provider cannot participate in the notice and takedown process, because there is nothing to take down. Under the text of the DMCA's subpoena provision, a copyright holder's request for a § 512(h) subpoena must include, among other things, a copy of the notification described in subsection (c)(3)(A), which informs the service provider of the alleged infringing activity. The panel held that because a § 512(a) service provider cannot remove or disable access to infringing content, it cannot receive a valid (c)(3)(A) notification, which is a prerequisite for a § 512(h) subpoena. Accordingly, a § 512(h) subpoena cannot issue to a § 512(a) service provider as a matter of law.

The panel held that the district court did not clearly err when it found that Cox acted only as a § 512(a) service provider with respect to the alleged infringement by Cox's 29 subscribers. Because Cox's role in the alleged infringement was limited to that of a § 512(a) internet service provider, Capstone's subpoena was invalid and the district court did not abuse its discretion when it quashed the subpoena.

COUNSEL

Kerry S. Culpepper (argued), Culpepper IP PLLC, Kailua Kona, Hawaii, for Petitioners.

Christopher J. Cariello (argued), Orrick Herrington & Sutcliffe LLP, New York, New York; Abigail Colella, Orrick Herrington & Sutcliffe LLP, Washington, D.C.; Rachael Jensen, Orrick Herrington & Sutcliffe LLP, Austin, Texas; Thomas J. Kearney and Jennifer Golinveaux, Winston & Strawn LLP, San Francisco, California; Joachim P. Cox, Abigail M. Holden, Cox Fricke LLP, Honolulu, Hawaii; for Defendant-Appellee.

Rose L. Ehler and Oliver L. Brown, Munger Tolles & Olson LLP, Los Angeles, California; Kelly M. Klaus and Shannon G. Aminirad, Munger Tolles & Olson LLP, San Francisco, California; for Amici Curiae Motion Picture Association Inc. and Recording Industry Association of America.

Mitchell L. Stoltz and Victoria Noble, Electronic Frontier Foundation, San Francisco, California, for Amicus Curiae Electronic Frontier Foundation.

OPINION

CHRISTEN, Circuit Judge:

Capstone Studios Corp., a copyright holder, successfully petitioned a district court clerk to issue a subpoena pursuant to § 512(h) of the Digital Millennium Copyright Act to CoxCom LLC, an Internet service provider. Capstone sought to obtain the identities of 29 Cox subscribers whose IP addresses appeared to be sharing pirated copies of Capstone's movie, *Fall*, via a peer-to-peer filesharing protocol called BitTorrent. One of Cox's subscribers objected to the subpoena. Upon review, the district court concluded that Cox qualified for one of § 512's four safe harbors—17 U.S.C. § 512(a)—because Cox merely provided its users with an Internet connection and played no other role in the alleged infringement. The district court concluded that a § 512(h) subpoena cannot issue to a § 512(a) service provider as a matter of law. Because Cox acted only as a § 512(a) service provider with respect to the alleged infringement, the court deemed Capstone's subpoena invalid. The district court quashed the subpoena and Capstone appeals. We affirm the district court's order.

I.

A.

This case concerns 17 U.S.C. § 512(h), a provision of the Digital Millennium Copyright Act (DMCA) that establishes an expedited subpoena process through which a copyright holder can obtain the identities of online infringers. Subsection 512(h) permits the clerk of any United States district court to issue a subpoena to a "service provider" on behalf of a copyright holder. "Service providers" generally

include entities that maintain websites, deliver network access, or host content on their servers. *See* § 512(k). If a copyright holder's petition for a § 512(h) subpoena meets all the statutory requirements, the clerk "shall expeditiously issue" the proposed subpoena without oversight from a judge. § 512(h)(4). As the Eighth Circuit explained in *In re Charter Communications, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 775 n.3 (8th Cir. 2005), without the DMCA's expedited subpoena process, a copyright holder seeking to learn the identity of infringers sharing copyright-protected content on the Internet would have to file an infringement action against individual users suspected of infringement, naming each as a John Doe defendant, and move the court for leave to conduct early discovery.

In enacting § 512, Congress struck a compromise between copyright holders and service providers. Section 512 "preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment." S. Rep. No. 105-190, at 20 (1998). The safe harbors that Congress included in § 512 limit service providers' liability for their users' infringement in exchange for their cooperation in removing infringing content from the Internet. Most of the safe harbors require service providers to remove or disable access to infringing material upon notification from the copyright holder—referred to as the notice and takedown process. *See, e.g.*, § 512(b)(2)(E), (c)(1)(C), (d)(3). The statute's four primary safe harbors protect service providers depending on the technical role they played in the alleged infringement: § 512(a) limits the liability of service providers when they did nothing more than transmit, route, or provide connections for infringing material; § 512(b) limits the

liability of service providers for "system caching," that is, when they provided "intermediate and temporary storage of material on a system or network" under certain conditions; § 512(c) limits the liability of service providers for material that "resid[ed] on [the service provider's] systems or networks" at the direction of its users; and § 512(d) limits the liability of service providers that performed an "information location tool" function, *i.e.*, linking users to online locations containing infringing material. 17 U.S.C. § 512(a)–(d).

The alleged infringement at issue here took place via BitTorrent, a peer-to-peer (P2P) network protocol—so called because users' computers communicate directly with each other rather than through centralized servers. *See Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 919–20 (2005). The BitTorrent protocol responds to a user's request for a file by connecting to the Internet and identifying "peers"—other users who have the requested file, or part of the requested file, stored on their devices. Peers are identified by their Internet Protocol (IP) addresses. A user may obtain the requested file from multiple peers. One peer might complete one portion of the request and send one part of the file, and additional peers identified by BitTorrent may supply the remaining pieces. Eventually, by facilitating communication between the user and other peers, BitTorrent ensures that the user obtains the completed file. *See Columbia Pictures Indus., Inc. v. Fung*, 710 F.3d 1020, 1026–28 (9th Cir. 2013).

Without the need for a centralized server, P2P network users can circumvent storage costs, exchange files faster than on other types of networks, and avoid the risk that a malfunction in the server will disable the network. *Grokster*, 545 U.S. at 920. Given these benefits in security, cost, and

efficiency, P2P networks are employed by universities, government agencies, corporations, and libraries, among others. *Id.* But the lack of a centralized server also makes it difficult to monitor, regulate, and remove the content exchanged between P2P users, which makes this type of networking attractive for exchanging infringing material. To police infringement taking place via BitTorrent, copyright holders monitor torrent trackers. A torrent tracker is software that assists in the communication between peers. Torrent trackers monitor which peers have which pieces of the file and identify who needs which pieces. Any peer can contact a tracker at any time to obtain a list of peers who are sharing a particular file. *See* Chao Zhang et al., *Unraveling the BitTorrent Ecosystem*, 22 IEEE Transactions on Parallel and Distributed Systems 1164, 1166 (2011). Thus, by monitoring torrent trackers, copyright holders can identify peers, collect their IP addresses, discover their identities, and bring infringement claims against them.

B.

Appellant Capstone Studios Corp. owns the copyright to the movie *Fall* (2022).[1] Capstone alleges that *Fall* has been subjected to massive Internet piracy through the BitTorrent protocol. Capstone specifically identified 29 IP addresses that it suspected of sharing *Fall* through BitTorrent using an Internet connection provided by CoxCom, LLC, an Internet service provider (ISP). Capstone petitioned the district court clerk in the District of Hawaii to issue a § 512(h) subpoena to Cox in order to obtain the identities of the subscribers associated with each of the 29 IP addresses. The clerk issued

[1] Millennium Funding, Inc. and Voltage Holdings, LLC jointly hold the copyright with Capstone. We refer to the copyright holders together as "Capstone."

the subpoena on April 13, 2023. Cox gave notice to its affected subscribers, informing them of the subpoena and requesting that they notify the court if they had any objection to Cox responding to the subpoena. One of the affected subscribers, "John Doe," wrote a letter informing the district court that he did not download *Fall.* John Doe stated that, upon receipt of the subpoena, he realized that he had forgotten to add a password to his Wi-Fi router, leaving his network open for anyone to use. John Doe asked the court to quash the subpoena and objected to the release of his personal information. No other subscriber objected, and Cox substantially complied with the subpoena by disclosing the identities associated with the other 28 IP addresses to Capstone.

A magistrate judge construed John Doe's letter as a motion to quash and directed Capstone to respond. Capstone did, and it argued that Doe did not assert a legal basis for quashing the subpoena or identify an undue burden or expense that would result from complying with it.

On August 31, 2023, the magistrate judge issued findings and a recommendation (F&R) that the subpoena was invalid and should be quashed. Although not raised by John Doe or Capstone, the magistrate judge concluded that the subpoena was invalid because Cox's role in disseminating the copyrighted material was confined to providing the Internet connection, which qualified Cox for one of § 512's four primary safe harbors—§ 512(a). Relying on the text of the statute and case law from other circuits, the magistrate judge concluded that a § 512(a) service provider cannot be subject to a § 512(h) subpoena as a matter of law.

Capstone objected to multiple findings and conclusions in the F&R, including the magistrate judge's legal

conclusion that the DMCA does not permit a § 512(h) subpoena to issue to a § 512(a) service provider and the factual finding that Cox acted only as a § 512(a) service provider with respect to the infringement at issue. For the first time, Cox appeared in the proceeding and filed a response to Capstone's objections. The district court adopted the F&R over Capstone's objections. Capstone filed a motion for reconsideration pursuant to Federal Rule of Civil Procedure 59(e), which the district court denied. Capstone timely appealed.[2]

II.

We have jurisdiction pursuant to 28 U.S.C. § 1291. Although we generally review orders granting or denying a motion to quash a subpoena for abuse of discretion, *In re Grand Jury Subpoena, Dated Apr. 18, 2003*, 383 F.3d 905, 909 (9th Cir. 2004), the subject order on the motion to quash

[2] Capstone argues that Cox should not have been permitted to participate in the proceedings for two reasons: (1) Cox waived any opportunity to challenge the validity of the subpoena because its objection was untimely; and (2) Cox lacked standing because it complied with the subpoena except as to Capstone's request for John Doe's identity, which Capstone subsequently withdrew. We reject both arguments. While the district court was under no obligation to permit Cox to participate, Capstone does not explain how the court abused its discretion when it found good cause to consider Cox's untimely objections. *See McCoy v. Sw. Airlines Co.*, 211 F.R.D. 381, 385 (C.D. Cal. 2002). Cox had standing to participate because the district court's ruling on whether Cox acted as a § 512(a) or (d) service provider had the potential to impose a legal obligation on Cox to respond to the subpoena, which is a concrete and redressable injury. *See Seila L. LLC v. Consumer Fin. Prot. Bureau*, 591 U.S. 197, 211 (2020) (concluding that a party's obligation to comply with a civil investigative demand and provide documents it would prefer to withhold is a concrete injury); *see also Arakaki v. Lingle*, 477 F.3d 1048, 1056 (9th Cir. 2007) (reviewing standing de novo).

involved two questions with different standards of review: (1) whether a § 512(h) subpoena may properly issue to a § 512(a) service provider is a matter of statutory interpretation that we review de novo, *see McKinney-Drobnis v. Oreshack*, 16 F.4th 594, 603 (9th Cir. 2021); and (2) whether Cox acted only as a § 512(a) service provider is a factual finding that we review for clear error, *see Thomas v. City of Tacoma*, 410 F.3d 644, 647 (9th Cir. 2005).

III.

The validity of Capstone's subpoena turns on two issues: first, as a matter of law, whether the DMCA allows a § 512(h) subpoena to issue to a § 512(a) service provider; and second, as a matter of fact, whether Cox acted only as a § 512(a) service provider with respect to the infringement at issue.

A.

We have not yet had occasion to address whether a § 512(h) subpoena may issue to a § 512(a) service provider. To answer this, we need to look no further than the text of the DMCA. Subsection 512(a) states that "[a] service provider shall not be liable . . . for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider." A service provider seeking to qualify for the § 512(a) safe harbor must also meet additional requirements. For example, the transmission must have been initiated by a person other than the service provider and the service provider cannot maintain a copy of the material for a longer period than is reasonably necessary for the transmission. *See* § 512(a)(1)–(5).

Subsection 512(a) is materially different from the other primary safe harbors, § 512(b)–(d). Subsections 512(b)–(d) all contain a "notice and takedown" provision that conditions qualification for the safe harbor. Upon notification of claimed infringement, the service provider must "respond[] expeditiously to remove, or disable access to, the material that is claimed to be infringing." § 512(b)(2)(E), (c)(1)(C), (d)(3). This provision is notably absent from § 512(a). The reason for this omission is clear from the text of the safe harbors and the different functions Congress sought to exempt from liability. Subsections 512(b) and 512(c) limit liability for service providers who provide "intermediate and temporary storage of material on [the service provider's] system or network" and "storage at the direction of a user of material that resides on [the service provider's] system or network." If a service provider qualifies for § 512(b) or § 512(c) because infringing material is stored or otherwise resides on the service provider's system or network, that service provider has the ability to remove the material from its system or network (or otherwise disable access to it) upon receipt of notice of infringement. Similarly, § 512(d) limits liability for service providers who "refer[] or link[] users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link." A service provider who qualifies for § 512(d) can disable access to the infringing material by removing or disabling its directory or hyperlink that links the user to the infringing content.

By contrast, § 512(a) limits liability for service providers who "transmit[], rout[e], or provid[e] connections for, material through a system or network controlled or operated by or for the service provider." Congress intended to limit

the § 512(a) safe harbor to service providers who "play[] the role of a 'conduit' for the communications of others," S. Rep. No. 105-190, at 41, as opposed to service providers who store infringing material or provide a link to a location where infringing material is stored. Unlike § 512(b)–(d) service providers, § 512(a) service providers furnish only the connection through which infringers exchange content. By definition, there is no infringing material that resides on a § 512(a) service provider's system or network, nor is there a "link" or "directory" that a § 512(a) service provider maintains. Thus, a § 512(a) service provider cannot participate in the notice and takedown process, because there is nothing for a § 512(a) service provider to take down.

With this understanding of § 512(a) and the notice and takedown process, we turn to the text of the DMCA's subpoena provision. A copyright holder's request for a § 512(h) subpoena must include, among other things, "a copy of a notification described in subsection (c)(3)(A)," which informs the service provider of the alleged infringing activity. § 512(h)(2)(A). That (c)(3)(A) notification is the same notification to which § 512(b)–(d) service providers must "respond[] expeditiously" by removing or disabling access to the identified infringing content. *See* § 512(b)(2)(E), (c)(1)(C), (d)(3).

The (c)(3)(A) notification itself must satisfy six requirements.[3] One requirement is that the copyright holder

[3] The statute states that the notification must "include[] substantially the following" and lists the six requirements. § 512(c)(3)(A). We have held that an effective notification must contain all of the listed items. *See Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1112 (9th Cir. 2007) ("[S]ubstantial compliance means substantial compliance with *all* of § 512(c)(3)'s clauses, not just some of them.").

provide "[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." § 512(c)(3)(A)(iii). The (c)(3)(A) notification requirement presents a problem for a copyright holder who seeks to subpoena a § 512(a) service provider because a § 512(a) service provider merely furnishes an Internet connection to its subscribers. Such a provider cannot "remove" or "disable access to" any infringing content those subscribers might share, because there is nothing for the § 512(a) service provider to remove. Without the ability to provide a valid (c)(3)(A) notification to § 512(a) service providers, copyright holders cannot satisfy the requirements for issuance of a § 512(h) subpoena.

The § 512(h) subpoena provision is inextricably intertwined with the (c)(3)(A) notification, cross-referencing (c)(3)(A) three times: (1) the request for the § 512(h) subpoena must contain a copy of the (c)(3)(A) notification; (2) the clerk shall issue the subpoena only "[i]f the notification filed satisfies the provisions of subsection (c)(3)(A)"; and (3) the service provider shall expeditiously respond "[u]pon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A)." § 512(h)(2)(A), (4), (5). This statutory text confirms that a § 512(a) service provider is not a contemplated recipient of a proper (c)(3)(A) notification. For these reasons, the DMCA does not permit a § 512(h) subpoena to issue to a § 512(a) service provider.

Two other circuits have reached the same conclusion. *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1237 (D.C. Cir. 2003); *Charter*, 393 F.3d at 777. In *Verizon*, Recording Industry Association

of America (RIAA) served two subpoenas on Verizon, an ISP, to discover the names of two subscribers who appeared to be trading .mp3 files of copyrighted music via P2P file sharing programs, such as KaZaA. 351 F.3d at 1231. The parties did not dispute that Verizon acted as a § 512(a) service provider with respect to the infringement, and Verizon argued that "§ 512(h) does not authorize the issuance of a subpoena to an ISP acting solely as a conduit for communications the content of which is determined by others." *Id.* The D.C. Circuit concluded based on the text of § 512(h) and the overall structure of § 512 that "a subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity," and not to a § 512(a) service provider. *Id.* at 1233.

Roughly a year later, the Eighth Circuit agreed. *Charter*, 393 F.3d at 777. In *Charter*, RIAA again requested that a district court clerk issue a subpoena to Charter Communications, Inc., an ISP, to produce the names, physical addresses, telephone numbers, and email addresses of approximately 200 Charter subscribers. *Id.* at 774. The Eighth Circuit observed that the notice and takedown provision did not apply to § 512(a) service providers and that the "remove" or "disable access" requirement prevented a § 512(a) service provider from receiving a proper (c)(3)(A) notification. *Id.* at 776–77. *Charter* adopted the reasoning of *Verizon* wholesale and concluded that "where Charter acted solely as a conduit for the transmission of material by others (its subscribers using P2P file-sharing software to exchange files stored on their personal computers), . . . the subpoena was not properly issued." *Id.* at 777.

Capstone argues that, despite the lack of a statutory provision requiring a § 512(a) service provider to remove or disable access to infringing material, a § 512(h) subpoena

can issue to a § 512(a) service provider because a § 512(a) service provider can, as a practical matter, "disable access to" the infringing material. In support of this argument, Capstone provided a declaration from its expert witness, David Cox, the owner of an information technology network consulting service. The declaration explained two different methods an ISP could use to "disable access to" infringing content short of terminating its users' Internet connection: destination null routing and port blocking.[4]

Capstone's expert explained that destination null routing prevents users from reaching specific destination IP addresses. Because an IP address can be associated with a computer as well as a website, an ISP can null route any user that tries to reach a website or computer hosting the infringing material. Instead of reaching that particular IP address, the user is routed away or the transmission is dropped. In the case of P2P networking, Capstone's expert stated that an ISP could null route the traffic of any subscriber that tries to reach the IP address that contains the infringing material. If destination null routing is employed, users are still able to access all other online locations on the Internet.

Capstone's expert also explained that an ISP has the option of port blocking. A port is a virtual point where network connections start and end. Ports are numbered and standardized across all network-connected devices, and allow computers to easily differentiate between different

[4] The technical capabilities of § 512(a) service providers cannot override the plain text of the statute—no statutory provision requires a § 512(a) service provider to remove or disable access to infringing material in response to a (c)(3)(A) notification. Even considering Capstone's practical argument, it is unpersuasive.

kinds of traffic. Many ports are associated with a specific process or service. For example, email goes through port 25, unsecured web traffic goes through port 80, secured web traffic goes through port 443, and remote desktop protocols go through port 3389. *See* Service Name and Transport Protocol Port Number Registry, Internet Assigned Numbers Auth., https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml (last visited Aug. 10, 2025). Ports are typically "open," meaning they can receive and transmit data. Port blocking is the process of an ISP "closing" a port for a particular user. Because BitTorrent traffic is commonly directed through ports 6882–6889, Capstone's expert explained that an ISP could block those ports for a particular user without terminating the user's access to the Internet.[5]

[5] The district court struck David Cox's declaration because the court concluded that Capstone could have raised its arguments concerning destination null routing and port blocking in its objections to the F&R. Capstone argues on appeal that the declaration was necessary to show that the district court made a factual mistake when it stated that null routing "effectively terminates a network connection." *See* Fed. R. Civ. P. 60(b)(1). Capstone's argument overlooks that, at the time the district court adopted the F&R, the parties and the court were using the term "null routing" to refer to *source* null routing, which prevents a user from reaching any location on the Internet. The court referred to a document Capstone cited in its objections which stated that source null routing "effectively terminat[es] a network connection." Only in its motion for reconsideration did Capstone clarify that there are different types of null routing and present evidence that an ISP could engage in *destination* null routing, which prevents a user from reaching only a particular online destination. Thus, the district court did not abuse its discretion by striking the declaration. *See Hambleton Bros. Lumber Co. v. Balkin Enters., Inc.*, 397 F.3d 1217, 1224 n.4 (9th Cir. 2005) (reviewing a district court's order striking a declaration for abuse of discretion). Regardless, the court's decision to strike the declaration made no

The DMCA does not define the phrase "disable access to" in § 512(b)–(d), but in *Verizon*, the D.C. Circuit considered whether an ISP can "disable access" to infringing material by terminating the offending subscriber's Internet account. 351 F.3d at 1235. The D.C. Circuit rejected RIAA's argument that disabling users' access to the Internet "disabled access" to infringing material for purposes of the (c)(3)(A) notification because termination of customers' accounts is a different remedy already set forth in a different provision of § 512. *Id.* The D.C. Circuit concluded that "Congress considered disabling an individual's access to infringing material and disabling access to the internet to be different remedies for the protection of copyright owners, the former blocking access to the infringing material on the offender's computer and the latter more broadly blocking the offender's access to the internet." *Id.*; *compare* 17 U.S.C. § 512(j)(1)(A)(i) (authorizing injunction restraining ISP "from providing access to infringing material"), *with* 17 U.S.C. § 512(j)(1)(A)(ii) (authorizing injunction restraining ISP "from providing access to a subscriber or account holder . . . who is engaging in infringing activity . . . by terminating the accounts of the subscriber or account holder").

Neither *Verizon* nor *Charter* specifically grappled with destination null routing or port blocking, measures that do not go as far as terminating a subscriber's account. But in our view, these measures do not go far enough because they do not "disable access" to infringing material within the meaning of § 512. As the district court recognized, destination null routing and port blocking cannot "disable

---

difference to the result of the motion for reconsideration because the court considered and rejected the expert's declaration.

access" within the meaning of (c)(3)(A)(iii) because an ISP can use these methods only to prevent its own subscribers (and not subscribers of other ISPs) from reaching destination IP addresses containing infringing material or using ports that commonly route infringing material. In other words, an ISP cannot "disable access" to infringing material via port blocking or destination null routing; it can only disable *its subscribers'* access to infringing material. Capstone points to nothing in the text or legislative history of § 512 suggesting that Congress contemplated such a piecemeal application of the notice and takedown procedure.

Because a § 512(a) service provider cannot remove or disable access to infringing content, it cannot receive a valid (c)(3)(A) notification, which is a prerequisite for a § 512(h) subpoena. We therefore conclude from the text of the DMCA that a § 512(h) subpoena cannot issue to a § 512(a) service provider as a matter of law.

Capstone makes several textual arguments to the contrary, none of which disturb our conclusion. First, Capstone points to § 512(k)'s two definitions of "service provider." As used in § 512(a), a "service provider" is:

> 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.

§ 512(k)(1)(A). As used in the remainder of § 512, "service provider" means:

> a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in [the definition of "service provider" applicable to § 512(a)].

§ 512(k)(1)(B). Capstone argues that because the latter definition applies to all provisions within § 512 *other than* § 512(a), the latter definition applies to "service provider" as used in § 512(h). From there, Capstone argues that because § 512(h) permits a copyright owner to request the clerk to issue a subpoena to a "service provider," and the definition of "service provider" applicable to § 512(h) includes the broader list of entities described in § 512(k)(1)(B), it follows that a § 512(h) subpoena can issue to a § 512(a) service provider.

RIAA made the same argument in *Verizon*. 351 F.3d at 1236. There, the D.C. Circuit stated that the argument "borders upon the silly," because it does not resolve the main conflict: a § 512(a) service provider cannot "remove" or "disable access to" infringing material. *Id.* ("Define all the world as an ISP if you like, the validity of a § 512(h) subpoena still depends upon the copyright holder having given the ISP, however defined, a notification effective under § 512(c)(3)(A)."). Capstone does nothing to differentiate its argument from the one rejected in *Verizon*, nor does Capstone explain how its read of § 512(k) overcomes the notification requirement or any of the other textual indications within § 512 that a § 512(a) service provider cannot be the subject of a § 512(h) subpoena.

Capstone also argues that § 512(a) service providers must be subject to § 512(h) subpoenas because concluding otherwise contradicts language in § 512(e) and § 512(m).

Subsection 512(e) creates a fifth safe harbor for educational institutions whose faculty or employee graduate students engage in infringing conduct on the school's network. To qualify for § 512(e) protection, the educational institution must first qualify for one of the four primary safe harbors, § 512(a)–(d). Subsection 512(e) also requires that the educational institution must not have received "more than two notifications described in subsection (c)(3)[(A)] of claimed infringement by such faculty member or graduate student" in the past three years. § 512(e)(1)(B). Capstone argues that if a § 512(e) institution can also be a § 512(a) service provider, then the requirement that the institution receive no more than two (c)(3)(A) notifications in the past three years makes no sense unless a § 512(a) service provider can receive (c)(3)(A) notifications. In a similar vein, § 512(m) states that eligibility for the first four safe harbors, § 512(a)–(d), does not require service providers to "gain[] access to, remov[e], or disabl[e] access to" the infringing content if doing so would violate another law. § 512(m)(2). In Capstone's view, § 512(m) assumes that all service providers eligible for the primary safe harbors—including § 512(a)—are capable of removing or disabling access to infringing material.

Capstone's argument improperly examines these provisions of § 512 in isolation. Reading the statute as a whole, § 512(e) sets forth the requirements for an educational institution to qualify for that safe harbor without regard to which of the four primary safe harbors the institution also qualifies. The requirement that the institution receive no more than two (c)(3)(A) notifications applies generally; the fact that a § 512(a) service provider cannot receive (c)(3)(A) notifications simply means that § 512(a) service providers automatically meet the

requirement of receiving two or fewer notifications. Subsection 512(m) merely states the DMCA should not be construed to require service providers to break the law to satisfy the notice and takedown requirement. It does not suggest that every service provider is necessarily capable of participating in the notice and takedown process. There are numerous indications within § 512 that § 512(a) service providers are incapable of removing or disabling access to infringing content, and those indications sufficiently outweigh the contrary implication Capstone reads within § 512(e) or § 512(m).

Capstone next argues that the notification provision in (c)(3)(A) can be satisfied in two ways, only one of which requires the copyright holder to remove or disable access to the infringing material. The (c)(3)(A) notification provision requires that a copyright holder provide:

> Identification 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.

§ 512(c)(3)(A)(iii) (emphasis added). Capstone argues that the first "or" creates two options for a copyright holder to give notice: the copyright holder can either (1) identify the material that is claimed to be infringing; *or* (2) identify the material that is the subject of infringing activity and that is to be removed or access to which is to be disabled. But reading the requirement that an ISP "remove" or "disable access" to apply only to "material [that is] the subject of infringing activity" and not apply to "material that is claimed

to be infringing" violates fundamental principles of statutory interpretation. *See* Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 147 (2012) ("When there is a straightforward, parallel construction that involves all nouns or verbs in a series, a prepositive or postpositive modifier normally applies to the entire series."). Capstone's reading would also lead to absurd results contrary to the purpose of the statute. In creating § 512, Congress sought to offer service providers safe harbor in exchange for their cooperation in expeditiously removing infringing material from their systems and networks. Capstone does not explain why Congress would require takedown for only "material that is subject to infringing activity" but not "material that is claimed to be infringing." *See* § 512(c)(3)(A)(iii).

Finally, Capstone argues that the alternative to a § 512(h) subpoena—filing John Doe lawsuits against thousands of subscribers—is an unworkable means of policing P2P infringers. We are sympathetic to this argument, but whether the DMCA provides a sufficient remedy for copyright holders to vindicate their rights against infringers using P2P networking is ultimately a question for Congress, not the courts.

The matter before us is a discrete question of statutory interpretation. Because § 512(a) service providers, by definition, are not entities that store infringing material or link users to a location where infringing material is stored, copyright holders cannot give § 512(a) service providers effective (c)(3)(A) notifications. And without an effective (c)(3)(A) notification, a copyright holder cannot obtain a valid § 512(h) subpoena. We conclude as a matter of law that the DMCA does not permit a § 512(h) subpoena to issue to a § 512(a) service provider.

B.

Having resolved the legal question, we turn next to the factual question: whether the district court clearly erred when it found that Cox acted only as a § 512(a) service provider with respect to the alleged infringement undertaken via BitTorrent by Cox's 29 subscribers.

The plain text of § 512 indicates that the safe harbor for which a service provider qualifies depends on the function the service provider performed with respect to the infringement at issue. For example, § 512(a) states: "[a] service provider shall not be liable . . . for infringement of copyright *by reason of* the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider . . . ." § 512(a) (emphasis added). Subsections 512(b), (c), and (d) contain similar language. *See* § 512(b)(1), (c)(1), (d). In this way, the safe harbors are not status-based and it would be incorrect to say that a service provider "is" a § 512(a) service provider. What matters is the function performed with respect to the alleged infringement at issue. *See Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1116–17 (9th Cir. 2007) (rejecting a service provider's argument that its provision of a hyperlink qualified it as a § 512(d) service provider because the copyright holder did not allege that the service provider infringed its copyrights by providing a hyperlink).

A service provider can simultaneously qualify for more than one safe harbor, § 512(n), and while the parties appear to agree that Cox acted as a § 512(a) service provider, Capstone argues that Cox *also* acted as a § 512(d) service provider with respect to the infringement at issue. There is

no dispute that a § 512(h) subpoena may issue to a § 512(d) service provider.

Subsection 512(d), titled "Information location tools," provides a safe harbor when an alleged infringement takes place "by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link." § 512(d). Capstone argues that Cox acted as a § 512(d) service provider because it assigned IP addresses to its subscribers and, by connecting those IP addresses to the Internet, it referred or linked those users to online locations that contained infringing material or material subject to infringing activity. Capstone contends that an IP address is the same as a hypertext link, reference, or pointer because an IP address can function just like a hypertext link that directs a user to a website or other destination.

Capstone cites to no case or other authority that outlines the types of service providers that "refer or link" users to infringing material within the meaning of § 512(d), but a basic understanding of IP addresses and P2P networking defeats Capstone's argument. Connecting a user to the Internet and assigning the user an IP address does not "link" or "refer" the user anywhere, much less to a particular location containing infringing material. Following Capstone's logic, an ISP's assignment of an IP address to a user would also "link" or "refer" that user to all locations on the Internet, including all those containing illicit and illegal content. If every ISP "links" or "refers" its users to infringing material merely by assigning an IP address and providing Internet service, then the § 512(d) safe harbor would completely swallow the § 512(a) safe harbor. We reject Capstone's argument that Cox also served as a

§ 512(d) service provider with respect to the alleged infringement.

Capstone separately challenges certain evidence the district court relied upon when it found that Cox acted only as a § 512(a) service provider—and not a § 512(d) service provider—with respect to the 29 IP addresses that Capstone suspects shared *Fall*. Upon receipt of the magistrate judge's F&R, Capstone's objections, and Cox's response, the district court issued an order requesting supplemental evidence. The court agreed that a § 512(a) service provider cannot be subject to a § 512(h) subpoena but requested that Cox "file with the court appropriate evidentiary proof that it is—or is not—an internet service provider under 17 U.S.C. § 512(a) for purposes of the subpoena issued in this matter." Cox submitted the declaration of Amber Hall, Cox's Chief Compliance and Privacy Officer. Hall explained that Cox engages in transmitting, routing, or providing connections for its users. The declaration said nothing about the 29 IP addresses, BitTorrent, or the specific infringement of *Fall*. Capstone moved to strike Hall's declaration, provided a side-by-side comparison of the declaration and the DMCA, and argued that the declaration was devoid of facts and merely parroted the language of § 512(a). Capstone maintains on appeal that Hall's declaration was wholly conclusory and that the district court clearly erred when it relied on the declaration to find that Cox acted only as a § 512(a) service provider.

A declaration is conclusory if it "do[es] not affirmatively show personal knowledge of specific facts," *Shakur v. Schriro*, 514 F.3d 878, 890 (9th Cir. 2008) (citation omitted), or if it "state[s] only conclusions, and not such facts as would be admissible in evidence," *United States v. Shumway*, 199 F.3d 1093, 1104 (9th Cir. 1999) (citation modified). We

agree that Hall's declaration is conclusory because it is devoid of factual assertions that would help determine the technical role Cox played in the alleged infringement. But we do not conclude that the district court clearly erred when it found that Cox acted as a § 512(a) service provider because the parties did not meaningfully dispute the role Cox played with respect to the alleged infringement.

Below and on appeal, the parties agreed that Cox did nothing more than assign IP addresses and provide an Internet connection to its 29 subscribers who allegedly engaged in copyright infringement.[6] The parties have only ever disputed whether those services qualify as transmission services described in § 512(a), or qualify as information location tool services described in § 512(d). The court clearly understood, and Capstone did not dispute, that the infringement took place via P2P networking and the extent of an ISP's technical involvement in P2P networking. Thus, the district court did not need any additional evidence to find that Cox acted only as a § 512(a) service provider.

Because Cox's role in the alleged infringement was limited to that of a § 512(a) ISP, and because a § 512(h) subpoena cannot issue as a matter of law to a § 512(a)

[6] Capstone directs the panel to Cox's website, which advertises its cloud storage services, and argues that these advertisements contradict the district court's conclusion that Cox does not store content. As we have already explained, § 512(a) does not require that the service provider act merely as a transmitter in all respects—only with respect to its role in the alleged infringement. *See Perfect 10*, 488 F.3d at 1116–17. Accordingly, whether Cox has the ability to provide storage is only pertinent if Capstone alleged that Cox stored the infringing material at issue. As long as Cox did nothing more than transmit, route, or provide connections for the subscribers who infringed Capstone's copyright, Cox qualifies for only the § 512(a) safe harbor.

service provider, Capstone's subpoena was invalid and the district court did not abuse its discretion when it quashed the subpoena.

IV.

We affirm the district court's orders quashing the subpoena and denying Capstone's motion for reconsideration.

AFFIRMED.