IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

IN RE: SUBPOENA OF INTERNET SUBSCRIBERS OF COX COMMUNICATIONS, LLC AND COXCOM LLC.	CIV. NO. 23-00426 JMS-WRP ORDER OVERRULING OBJECTIONS, ECF NO. 10, AND ADOPTING FINDINGS AND RECOMMENDATION TO QUASH 512(h) SUBPOENA, ECF NO. 8

ORDER OVERRULING OBJECTIONS, ECF NO. 10, AND ADOPTING FINDINGS AND RECOMMENDATION TO QUASH 512(h) SUBPOENA, ECF NO. 8

I. INTRODUCTION

Before the court are Objections filed by Petitioners Voltage Holdings, LLC; Millennium Funding, Inc.; and Capstone Studios Corp. (collectively "Petitioners") to a Magistrate Judge's Findings and Recommendation to Grant John Doe's Motion to Quash a Subpoena ("F&R") issued under 17 U.S.C. § 512(h), part of the Digital Millennium Copyright Act ("DMCA"). ECF No. 10. After the Objections were filed, to address Petitioners' Objections on a full record, the court ordered supplemental briefing from Cox Communications LLC and CoxCom LLC (collectively, "Cox"). ECF No. 26. Accordingly, Cox submitted a

declaration, ECF No. 29, and Petitioners submitted a response to the declaration, ECF No. 30.

Having considered the F&R and the supplemental briefing, Petitioners' Objections are OVERRULED, and the August 31, 2023 F&R is ADOPTED. The court determines that, because Cox acted as a conduit for the allegedly copyrighted material, Cox falls under the safe harbor in 17 U.S.C. § 512(a), and therefore § 512(h) does not authorize the subpoena issued here.[1] The subpoena is quashed.

II. STANDARD OF REVIEW

When a party objects to a magistrate judge's findings or recommendations, the district court must review de novo those portions to which the objections are made and "may accept, reject, or modify, in whole or in part, the findings or recommendations made by the magistrate judge." 28 U.S.C. § 636(b)(1); *see also United States v. Raddatz*, 447 U.S. 667, 673–74 (1980); *United States v. Reyna-Tapia*, 328 F.3d 1114, 1121 (9th Cir. 2003) (en banc) ("[T]he district judge must review the magistrate judge's findings and recommendations de novo if objection is made, but not otherwise.").

[1] The court rules on Petitioners' objections to the F&R and to the Hall Declaration without a hearing pursuant to Local Rule 7.1(c).

Under a de novo standard, this court reviews "the matter anew, the same as if it had not been heard before, and as if no decision previously had been rendered." *Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1004 (9th Cir. 2006); *United States v. Silverman*, 861 F.2d 571, 576 (9th Cir. 1988). Although the court need not hold a de novo hearing, the court must arrive at its own independent conclusion about those portions of the magistrate judge's findings or recommendation to which a party objects. *United States v. Remsing*, 874 F.2d 614, 618 (9th Cir. 1989).

III. BACKGROUND

A. Proceedings Before the Magistrate Judge

This case concerns a subpoena issued by Petitioners to Cox pursuant to 17 U.S.C. § 512(h) (the "Subpoena"). ECF No. 1. Petitioners identified the IP addresses of certain Cox subscribers who had allegedly distributed copies of Petitioners' copyrighted film using peer-to-peer ("P2P") filesharing. ECF No. 1 at PageID.2. By issuing the Subpoena to Cox, Petitioners sought to discover these subscribers' identities using the IP addresses that Cox had assigned to them. *Id.* at PageID.2; ECF No. 1-1 at PageID.7. Cox gave its subscribers an opportunity to object to the disclosure of their identities, and one subscriber ("John Doe") did so. ECF No. 4. The Magistrate Judge construed John Doe's letter of objection as a

motion to quash, ECF No. 5, and recommended that the Subpoena be quashed because it was invalid under 17 U.S.C. § 512(h). ECF No. 8 at PageID.54.

Petitioners objected under Local Rule 74.1(a), appealing to this court by making five specific Objections to the F&R. ECF No. 10 at PageID.62-63. But before reaching the specific issues on appeal, the court provides necessary context by setting forth the relevant technologies at issue and the DMCA's legal framework applicable to P2P filesharing.

B. The Technologies at Issue

Two technologies are at issue—the assignment of IP addresses by an internet service provider ("ISP"), and P2P file sharing.

An IP address is a unique identifier assigned by an ISP to every computer having access to the internet, including computer servers that host websites. *United States v. Werdene*, 883 F.3d 204, 207 (3d Cir. 2018). Thus, each user of an ISP, and each computer hosting websites, has a unique IP address. "Many IP addresses are dynamic, meaning that they are assigned when a user connects to the internet, and they change from time to time." *Hard Drive Prods., Inc. v. Does 1-90*, 2012 WL 1094653, at *1 n.2 (N.D. Cal. Mar. 30, 2012).

P2P filesharing systems allow users to disseminate files stored on their computers to other internet users, or "peers." *In re Charter Commc'ns, Inc., Subpoena Enf't Matter*, 393 F.3d 771, 773 (8th Cir. 2005). "By utilizing [P2P]

technology, an internet user can directly search the MP3 file libraries of other users, with no web site being involved because the transferred files are not stored on the computers of the ISP providing the P2P users with internet access." *Id.* In the context of P2P filesharing, individual internet subscribers (each with a unique IP address assigned by their ISP) share files among themselves through the aid of a P2P system that helps each user locate other users seeking to distribute or receive the file in question. *See id.* In other words, P2P acts as a decentralized platform permitting individuals to share files without a third party acting as an intermediary.

C. The DMCA and P2P Filesharing

The DMCA authorizes copyright owners to seek a subpoena from the clerk of any United States District Court for identification of an alleged infringer. 17 U.S.C. § 512(h).[2] Section 512(h)(2)(A) requires a request for subpoena to

[2] 17 U.S.C. § 512(h) reads in relevant part:

> **(h) Subpoena to identify infringer.—**
>
> **(1) Request.**—A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.
>
> **(2) Contents of request.**—The request may be made by filing with the clerk—
>
> **(A)** *a copy of a notification described in subsection (c)(3)(A)*;
>
> **(B)** a proposed subpoena; and
>
> **(C)** a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.
>
> **(3) Contents of subpoena.**—
>
> The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorized by the copyright owner information sufficient to identify the

(continued . . .)

contain "a copy of a notification described in subsection (c)(3)(A)." 17 U.S.C. § 512(h)(2)(A). In turn, subsection (c)(3)(A) of § 512 ("Subsection (c)(3)(A)") requires the notification to contain an "[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 . . . ." 17 U.S.C. § 512(c)(3)(A).[3]

---

alleged infringer of the material described in the notification to the extent such information is available to the service provider.

(4) Basis for granting subpoena.—*If the notification filed satisfies the provisions of subsection (c)(3)(A)*, the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider.

(Emphases added.)

[3] Subsection (c)(3)(a) reads:

(c) Information residing on systems or networks at direction of users.—

. . . .

(3) Elements of notification.—

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) *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.*

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(continued . . .)

And § 512(h)(4) states that notice satisfying each part of Subsection (c)(3)(A) is a condition precedent to issuing a subpoena. 17 U.S.C. § 512(h)(4) ("Basis for granting subpoena."). In other words, if a copyright holder does not or cannot fulfill the notice provision in Subsection (c)(3)(A), it cannot obtain a subpoena under § 512(h).

The DMCA creates four safe harbors for ISPs to avoid liability for infringing activity. Under the reasoning of the Eighth and District of Colombia Circuits (and many district courts), these safe harbor provisions demonstrate that a § 512(h) subpoena may not be used to obtain the identities of P2P infringers from an ISP falling within safe harbor provision § 512(a). *See Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc.*, 351 F.3d 1229, 1234 (D.C. Cir. 2003); *In re Charter*, 393 F.3d at 776; *see, e.g.*, *In re Subpoena issued to Birch Commc'ns, Inc.*, 2015 WL 2091735, at *5 (N.D. Ga. May 5, 2015); *In re Subpoena to Univ. of N.C. at Chapel Hill*, 367 F.Supp.2d 945, 951–956 (M.D.N.C. 2005).

> **(v)** A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
>
> **(vi)** A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(Emphasis added.)

The safe harbor in § 512(a) protects ISPs from liability for "transmitting, routing, or providing connections for" material through a system or network.[4] 17 U.S.C. § 512(a); *see also In re Charter*, 393 F.3d at 775 (observing that § 512(a) limits liability for ISPs that serve as a "mere conduit"). The safe harbors in § 512(b), (c), and (d) protect ISPs from liability for infringing material that users temporarily store in caches (§ 512(b)), on systems or networks (§ 512(c)), or at links (§ 512(d)) provided by the ISP.[5] 17 U.S.C. § 512(b)–(d).

---

[4] 17 U.S.C. § 512(a) reads:

> **(a) Transitory digital network communications.**—A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, 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, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if—
>
> **(1)** the transmission of the material was initiated by or at the direction of a person other than the service provider;
>
> **(2)** the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;
>
> **(3)** the service provider does not select the recipients of the material except as an automatic response to the request of another person;
>
> **(4)** no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and
>
> **(5)** the material is transmitted through the system or network without modification of its content.

(Emphasis added.)

[5] The relevant portions of 17 U.S.C. § 512(b), (c), and (d) read:

> **(b) System caching**.—

(continued . . .)

The safe harbor in § 512(a) does not require ISPs to take down material upon receiving notice from a copyright owner—if an ISP is a "mere conduit," nothing is stored, and there is nothing to take down. *Cf. In re Charter*, 393 F.3d at 775. Conversely, though their wording differs, each of the safe harbors in § 512(b), (c), and (d) requires that, when notified of alleged infringement by a copyright owner, an ISP "respond[] expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement." *Compare* 17 U.S.C. § 512(b)(2)(E), *with* 17 U.S.C. § 512(c)(1)(C) *and* 17 U.S.C. § 512(d)(3). These provisions within § 512 (b), (c), and (d) (called "notice and take down" provisions) all require that the notice from the copyright owner first meet the requirements of Subsection (c)(3)(A). In contrast, the "mere

---

> **(1) Limitation on liability.**—A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of *the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider* . . . .

> **(c) Information residing on systems or networks at direction of users.**—
>
> **(1) In general.**—A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of *the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider* . . . .

> **(d) Information location tools.—**A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright 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* . . . .

(Emphases added.)

conduit" safe harbor in § 512(a) does not contain any notice and take down provision referring to Subsection (c)(3)(A)—because there is no material to take down.

In considering whether a copyright owner can obtain the IP addresses of P2P infringers by subpoenaing an ISP under § 512(h), the Eighth Circuit and D.C. Circuit both reasoned that if the ISP acts as a "mere conduit" in cases of P2P filesharing, it is not possible for a copyright owner to satisfy the notice requirement in Subsection (c)(3)(A). *Verizon*, 351 F.3d at 1233 ("We conclude from both the terms of § 512(h) and the overall structure of § 512 that, . . . a [512(h)] subpoena may be issued only to an ISP engaged in storing on its servers material that is infringing or the subject of infringing activity."); *In re Charter*, 393 F.3d at 777 ("[B]ecause the parties do not dispute that [the ISP's] function was limited to acting as a conduit for the allegedly copyright protected material, we agree § 512(h) does not authorize the subpoenas issued here."). The Eighth Circuit explained that

> [t]he absence of the remove-or-disable-access provision (and the concomitant notification provision) [in § 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.

In re Charter, 393 F.3d at 776.

On this basis, both courts ruled that the ISP fell within the safe harbor in § 512(a) and the subpoenas over P2P filesharing were improper. *Verizon*, 351 F.3d at 1233; *In re Charter*, 393 F.3d at 777. In short, a § 512(h) subpoena cannot issue if the ISP is unable to locate and remove the infringing material, and an ISP acting as a mere conduit for allegedly infringing activity cannot do so. This court agrees with the reasoning of the Eighth and D.C. Circuits.

With this background, the court now turns to Petitioners' specific objections.

D. Petitioners' Objections to the F&R

Petitioners appealed the Magistrate Judge's F&R to this court, making five Objections. ECF No. 10 at PageID.62–63. Cox submitted a Response to the Objections, ECF No.18, and Petitioners submitted a Reply, ECF No. 24.

Petitioners' Objections (1), (2) and (3) all address the Magistrate Judge's determination that the Subpoena was invalid under the DMCA. Along with their request for subpoena, Petitioners had submitted a list of IP addresses of Cox subscribers that allegedly participated in infringing activity, which Petitioners argued constituted adequate notice to Cox of the infringing activity under § 512(h) and Subsection (c)(3)(A). ECF No. 1-2 at PageID.9–16; ECF No. 10-1 at PageID.69. Relying on *Verizon* and *In re Charter*, the F&R found the notice was

inadequate, and recommended the subpoena be quashed. ECF No. 8 at PageID.44–56.

First, Petitioners object to the F&R's conclusion that "Cox's role in disseminating the allegedly copyrighted material is confined to acting as a mere 'conduit' in the transfer of files through its network including the files at issue in this case." ECF No. 10 at PageID.62. They argue that in assigning IP addresses to the alleged P2P infringers, Cox was also referring or linking material under § 512(d), making their list of IP addresses valid notice of infringement. ECF No. 10-1 at PageID.68–70.

Second, Petitioners object to the F&R's conclusion that the subpoena was not valid because "subpart 512(c)(3)(A)(iii) required Petitioners to identify in their 512(c)(3)(A) notice to Cox the infringing material that could be removed or access to which could be disabled, which Petitioners could not do because Cox's role in the alleged infringement was limited to providing the internet service that connected P2P subscribers . . . ." ECF No. 10 at PageID.62. This argument is essentially coterminous with Petitioners' Objection (1).

Third, Petitioners object to the F&R's conclusion that "when the infringement complained of is done through P2P file sharing such as through a BitTorrent protocol, the ISP can neither 'remove' nor 'disable access to' the

infringing material because that material is not stored on the ISP's servers." *Id.* at PageID.62–63.

Fourth, Petitioners object to "the F&R's factual conclusions that were not based upon any briefings of Doe or Petitioners," namely, the F&R's determination, based on an "appear[ance] from other cases and the circumstances of this case," that Cox acted as a "mere 'conduit' in the transfer of files through its network." ECF No. 8 at PageID.45; ECF No. 10 at PageID.63; ECF No. 10-1 at PageID. 74. Petitioners initially argued that the parties should have had the ability to submit briefing on the statutory interpretation issue. ECF No. 10-1 at PageID.74. In response, this court requested that Cox submit appropriate evidentiary proof that it falls (or does not fall) under 17 U.S.C. § 512(a), noting that a declaration by an appropriate corporate representative with personal knowledge of the relevant statutory factors would appear to be sufficient. ECF No. 26. Cox responded by filing a declaration by one of its officers stating that it was an internet service provider under 17 U.S.C. § 512(a) (the "Hall Declaration"). ECF No. 29. Petitioners objected to the declaration. ECF No. 30.

Finally, Petitioners object to the F&R's conclusion "that Petitioners be ordered to return and/or destroy any information obtained from the Subpoena, to maintain no further record of the information from the Subpoena, and to make no further use of the subscriber data obtained from the Subpoena." ECF No. 10 at

PageID.63. They ask that any remedy apply only to the information of John Doe. ECF No. 10-1 at PageID.74–75.

The court now turns to each of these points on appeal.

IV. DISCUSSION

A. Petitioners' Objections (1), (2), and (3)

Reading all the statutory provisions in concert and applying them to the alleged P2P infringement at issue, this court reaches the same conclusion as the F&R: The 17 U.S.C. § 512(h) subpoena is invalid because the notice provisions of 17 U.S.C. § 512(c)(3)(A) are not satisfied.

The F&R reasoned, following *Verizon* and *In re Charter*, that the structure of the DMCA precludes a copyright owner from requesting a § 512(h) subpoena for an ISP acting as a conduit for filesharing. ECF No.8 at PageID.52–54. Having determined that Cox—like the ISPs in *Verizon* and *In re Charter*—was a "mere conduit" for infringing material under § 512(a), the F&R decided that no proper notice could be issued, because there is no notice and take down provision in § 512(a). ECF No. 8 at PageID.57. Therefore, the Subpoena was invalid. *Id.*

On appeal, Petitioners concede that Cox acted as a "conduit" for P2P infringement under the safe harbor in § 512(a), but argue that Cox is not a "*mere* conduit" because it *also* falls under § 512(d). Petitioners claim that, in assigning IP addresses to P2P infringers, Cox "refer[s] or link[s]" users to infringing material

using "information location tool[s]." ECF No.10-1 at PageID.68. They argue that the IP addresses Cox assigns to users like John Doe are *both* "information location tool[s]" *and* "online location[s] containing infringing material" for the purposes of § 512(d). ECF No. 24 at PageID.125–126. As explained, the § 512(d) safe harbor does have a notice and take down provision, though the § 512(a) safe harbor does not. If the ISP falls under § 512(a) *and* § 512(d), Petitioners argue, the list of IP addresses that Petitioners attached to their request for subpoena could constitute adequate notice under Subsection (c)(3)(A) for infringement under § 512(d). In other words, the list of IP addresses of alleged infringers *is* the "infringing material" or "material that is . . . the subject of infringing activity" that Petitioners wanted Cox to take down under § 512(d), because users' IP addresses "link" them to each other within the P2P system. ECF No. 10-1 at PageID.72. Petitioners further contend that *Verizon* and *In re Charter* never addressed the question of whether P2P infringement fell under § 512(d) because the argument was never raised. ECF No. 10-1 at PageID.70.

In support of this argument, Petitioners claim that simply by typing a website's IP address into an internet search bar, a user can connect to that website. ECF No. 24 at PageID.128. Under this argument, the IP address therefore functions as a link or reference of a user to a website. Therefore, Petitioners also claim that it is possible for Cox to stop its users' infringing activity by disabling

infringers' IP addresses, for example, through null routing. ECF No. 10-1 at PageID.70 n.5, 73.

Petitioners are incorrect. Simply because users can use an IP address to access a website does not mean that IP addresses necessarily function as links or references in P2P filesharing.[6] In typical P2P filesharing, individual internet subscribers share files among themselves through the aid of a P2P system, "with no website being involved." *In re Charter*, 393 F.3d at 773. Although each internet user sharing files over P2P has an IP address, it is the P2P system that enables users to locate peers who are also seeking to distribute or receive files.[7]

---

[6] Although the DMCA does not define "referring or linking," § 512(d) (which gives a safe harbor to ISPs that "refer[] or link[]" users to infringing material) has been described as "cover[ing] *active assistance* to users." *A&M Recs., Inc. v. Napster, Inc.*, 2000 WL 573136, at *5 (N.D. Cal. May 12, 2000) (emphasis added). Thus, "referring or linking" requires more than just the assignment of an IP address to a user through automatic operations—it requires providing some degree of "active assistance" to users in locating online resources. *Cf. id.* The legislative history of the DMCA supports this position. The Committee Reports describe information location tools as being created, not by automatic processes occurring below the user level, but by "online editors and catalogers." H.R. Rep No. 105-551, pt. 2, at 58 (1998) ("Information location tools are essential to the operation of the internet . . . Directories such as Yahoo!'s usually *are created by people visiting sites to categorize them*. It is precisely the *human judgment and editorial discretion* exercised by these cataloguers which makes directories valuable.") (emphases added); S. Rep No. 105-190, at 49 (1998) (same).

[7] The P2P system that John Doe and others allegedly used is BitTorrent. ECF No. 1-3 at PageID.18. The Ninth Circuit explained the operation of BitTorrent in detail in *Columbia Pictures Indus., Inc. v. Fung*, 710 F.3d 1020, 1026–28 (9th Cir. 2013). Importantly, "[t]here is no central repository of torrent files . . . ." *Id.* at 1028. In order to enable users to locate files, BitTorrent employs both client software on a user's computer and "trackers," servers run by various independent operators that help users seeking to download particular files locate peers who have those files available to distribute. *Id.* These trackers "serve many of the functions of an indexing server" for torrents. *Id.* at 1027. Thus, while one BitTorrent user may download files from other users, all of whom happen to have IP addresses, the trackers and the client

(continued . . .)

The most fitting description of what Cox did in assigning John Doe an IP address is that Cox "provid[ed] connections for" the alleged infringement under § 512(a). Cox assigned Doe an IP address, and routed traffic that allegedly contained a copyrighted file to that IP address using "automatic technical processes." 17 U.S.C. § 512(a). If an ISP assigning an IP address is both "providing connections for" infringement under (a) and "referring or linking" to infringing material under (d)—as Petitioners contend—Congress would not have created two separate safe harbors. *See GCIU-Emp. Ret. Fund v. MNG Enterprises, Inc.*, 51 F.4th 1092, 1097 (9th Cir. 2022) (Courts "presume that Congress did not intend any part of [a] statute to be "superfluous, void, or insignificant") (internal quotations omitted); *cf. Verizon*, 351 F.3d at 1234 ("Section 512 creates four safe harbors, *each of which* immunizes ISPs from liability for copyright infringement *under certain highly specialized conditions*.") (emphases added).

Furthermore, IP addresses do not fit comfortably within § 512(d)'s description of an "information location tool." Section 512(d) describes an "information location tool" as "including a directory, index, reference, pointer, or hypertext link" that is used to "refer[] or link[] users to an online location containing infringing material or infringing activity." 17 U.S.C. § 512(d). The

---

software accomplish the indexing, referencing, and linking functions necessary to locate and distribute files—the ISP is not involved. *Cf. id.* at 1026–1028; *see also, e.g., HB Prods., Inc. v. Faizan*, 603 F. Supp. 3d 910, 917–19 (D. Haw. 2022) (describing how BitTorrent operates).

prototypical "information location tool" is a search engine. *See, e.g.*, *Capitol Recs., Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627, 639 (S.D.N.Y. 2011) ("Subsection 512(d) governs information location tools, e.g., search engines."). An IP address does not, in itself, constitute a "directory, index, reference, pointer, or hypertext link."

Petitioners' argument that Cox may "remove or disable access to" the infringing material, for example, by using null routing, also fails. ECF No. 10-1 at PageID.73. The F&R correctly reasons, following *Verizon*, that in the text of the DMCA, Congress considered disabling access to infringing material and disabling access to a subscriber's account to be distinct remedies. *Verizon*, 351 F.3d at 1235 (comparing 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 terminating a subscriber's account)). As Petitioners acknowledge, null routing effectively terminates a network connection. ECF No. 10-1 at PageID.70. So, Cox has no meaningful ability to satisfy the remedial requirements of the § 512(d) safe harbor short of terminating the user's connection, which is a harsher remedy than the DMCA authorizes. If the assignment of IP addresses to P2P infringers falls under § 512(d), Cox would have no ability to avoid liability for monetary relief for P2P infringement in suits like Petitioners'

because although "notice" by copyright holders would be possible, "take down" by Cox would not. Petitioners' construction of the statute is therefore implausible.

The F&R suggests that Petitioners can seek Doe's identity through other avenues including a John Doe lawsuit. ECF No. 8 at PageID.56. Petitioners respond that it may be prohibitively difficult for them to file a John Doe lawsuit after the Ninth Circuit's decision in *Cobbler Nev., LLC v. Gonzales*, 901 F.3d 1142, 1145 (9th Cir. 2018). ECF No. 24 at PageID.129–130. But even assuming for the sake of argument that Petitioners are correct, it is simply not relevant to the court's interpretation of the DMCA. *Cf. Verizon*, 351 F.3d at 1238 ("It is not the province of the courts . . . to rewrite the DMCA in order to make it fit a new and unforeseen internet architecture [P2P filesharing], no matter how damaging that development has been to [copyright holders].").

B. Petitioners' Objections (4) and (5)

Petitioners' Fourth Objection is that the F&R should not have determined that Cox acted as a "mere conduit" without evidence from the parties. ECF No. 10 at PageID.73–74. In response to the court's request (*see, e.g.*, Federal Rule of Civil Procedure 72(b)(3), which allows this court to "receive further evidence"), Cox has supplemented the record with a declaration by its Chief

Compliance and Privacy Officer, Amber Hall.[8] ECF No. 29. Hall attests that Cox "is engaged in transmitting, routing, or providing connections for" material only as described in § 512(a). ECF No. 29 at PageID.141. Petitioners argue that Hall does not have the requisite technical expertise to attest to the facts in the declaration, that her statements are not credible because they conflict with other public statements by Cox, and that her statements are impermissible legal conclusions. ECF No. 30 at PageID.144–146.

Petitioners' challenge to Hall's credibility based on her job title, Chief Compliance and Privacy Officer, is unpersuasive. ECF No. 30 at PageID.147. Hall attests that as Chief Compliance and Privacy Officer, she is "responsible for understanding how Cox's Internet service product operates in connection with the [functionality at issue]." ECF No. 29 at PageID.140. Further, "personal knowledge of the business entity's activities may be inferred to corporate officers." *Envy Hawaii LLC v. Volvo Car USA LLC*, 2019 WL 5865912, at *6 (D. Haw. Nov. 8, 2019); *see also Siebert v. Gene Sec. Network, Inc.*, 75 F. Supp. 3d 1108, 1115 (N.D. Cal. 2014) (holding that an employee may testify about information she is

[8] Within their fourth objection, Petitioners also object to the F&R sua sponte analyzing whether the Subpoena was valid under 17 U.S.C. §512(h) without John Doe having raised that argument in his pro se motion. The Magistrate Judge was within his discretion to do so, and to the extent that objection was based on the lack of briefing, Petitioners have now had ample opportunity to submit briefing on these issues, which the court has reviewed de novo. *See* ECF Nos. 10 & 24; *see also United States v. Ochoa-Sanchez*, 676 F.2d 1283, 1288 (9th Cir. 1982) ("The trial court acts in its discretion in deciding whether to quash a subpoena.").

required to be aware of in the course of her employment); *In re Kaypro*, 218 F.3d 1070, 1075 (9th Cir. 2000) (holding that the declarant's five-year tenure as manager lent support to his claim of personal knowledge of industry practice). And it is insufficient for Petitioners to simply claim that Ms. Hall is not credible solely because of her job title (i.e., because she is not Chief Technology or Information Officer).

Petitioners' argument that Ms. Hall's declaration conflicts with public statements by Cox that Cox filters out spam email, viruses, botnets, and malware over its network also fails. ECF No. 30 at PageID.146–147. The fact that Cox refuses to transmit certain types of malicious files, or blocks certain ports, does not amount to an admission that Cox "modifi[es] the content" of transmissions through its network in a way that would remove Cox from the safe harbor in § 512(a). In other words, Cox's filtering or blocking certain transmissions does not mean Cox is not a "mere conduit" in the context of P2P filesharing.

Last, Petitioners' characterization of Ms. Hall's statements as "legal conclusions" is incorrect. Ms. Hall's use of the language of § 512(a) in her description of Cox's operations does not convert her factual statements into an impermissible legal conclusion.

Finally, turning to Petitioners' Fifth Objection, given that the Subpoena was inappropriately issued under § 512(h), it must be quashed as to all

Defendants.[9] As the F&R found, because there was no statutory basis for Petitioners to receive any of the information they requested, Petitioners must destroy and make no further use of all of the information they received. ECF No. 8 at PageID.57–58.

V. CONCLUSION

The court OVERRULES Petitioners' Objections, ECF No. 10, and ADOPTS the Magistrate Judge's August 31, 2023 Finding and Recommendation to quash Petitioners' Subpoena, ECF No. 8. Petitioners' 512(h) Subpoena is QUASHED. No later than one week after the date of this Order, Petitioners are ordered to return and/or destroy any information derived from the Subpoena, to maintain no further record of the information obtained the Subpoena, and to make no further use of the subscriber data obtained from the Subpoena.

[9] Finding that the Subpoena was not validly issued, the Court does not address John Doe's pro se arguments that (1) the infringer was someone using his family's unprotected Wi-Fi connection and that (2) John Doe does not have the ability or resources to travel to address this court (John Doe appears to be located in Las Vegas). ECF No. 4. Furthermore, as John Doe might be alluding to, the court need not decide whether the court has personal jurisdiction over John Doe (or whether he has waived it). In this regard, some courts have addressed the issue of personal jurisdiction and venue for recipients of a § 512(h) subpoena, with one court reasoning that "[although] Section 512(h) says that the copyright owner or agent can seek a subpoena from any district court, [it] does not say that every district court has [personal] jurisdiction to issue a subpoena compelling action from persons outside the district." *In re Subpoena to Univ. of N.C. at Chapel Hill*, 367 F.Supp.2d at 957 (quashing a subpoena seeking to compel discovery outside the court's district); *see also In re DMCA Section 512(h) Subpoena to Facebook, Inc.*, 2015 WL 12805630, at *8 (S.D. Tex. Nov. 18, 2015) (affirming Magistrate Judge's recommendation to deny a motion to compel for improper venue given Facebook's lack of nexus to the Southern District of Texas).

IT IS SO ORDERED.

/s/ J. Michael Seabright
J. Michael Seabright
United States District Judge

DATED: Honolulu, Hawaii, January 30, 2024.

In re: Subpoena of Internet Subscribers of Cox Communications, LLC and CoxCom, LLC, Civ. No. 23-00426 JMS-WRP, Order Overruling Objections, ECF No. 10, and Adopting Findings and Recommendation to Quash 512(h) Subpoena, ECF No. 8