UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	CV 16-5051-GW(AFMx)	Date	June 1, 2017
Title	*ALS Scan, Inc. v. Cloudflare, Inc., et al.*		

Present: The Honorable	GEORGE H. WU, UNITED STATES DISTRICT JUDGE	
Javier Gonzalez	Katie Thibodeaux	
Deputy Clerk	Court Reporter / Recorder	Tape No.

Attorneys Present for Plaintiffs:	Attorneys Present for Defendants:
Jay M. Spillane	Rachel H. Kassabian John L. Ambrogi by telephone Shahrokh Sheik by telephone

PROCEEDINGS: CLOUDFLARE, INC.'S MOTION FOR PARTIAL SUMMARY JUDGMENT REGARDING EXTRATERRITORIALITY [121]

Court hears further argument. The Court's Final Ruling is attached hereto. Based on the Court's Ruling, and for reasons stated on the record, Defendant's motion is GRANTED IN PART and DENIED IN PART. The Court DENIES Cloudflare's Motion as to the following thirteen sites: imgchili.com, slimpics.com, bestofsexpics.com, greenpics.com, imgspot.org, imgsen.se, imgspice.com, stooorage.com, img.yt, vipergirls.to, fboom.me, imgflash.net, and imgtrex.com. The Court GRANTS Defendant's Motion as to pornwire.net.

: 20

Initials of Preparer JG

ALS Scan, Inc. v. Cloudflare, Inc., et al., Case No. CV-16-5051-GW-AFM(x)
Final Ruling on Motion for Partial Summary Judgment Regarding Extraterritoriality

I. Background

ALS Scan, Inc. ("Plaintiff") sues Cloudflare, Inc. ("Cloudflare"); Dolphin Media Ltd. ("Dolphin"); Hivelocity Ventures Corporation ("Hivelocity"); and Steadfast Networks, LLC ("Steadfast") (collectively, "Defendants")[1] for various claims related to Defendants' alleged infringement of Plaintiff's copyrighted and trademarked works. *See generally* Third Am. Compl. ("TAC"), Docket No. 148.[2] The TAC asserts six causes of action: (1) direct copyright infringement, against Dolphin; (2) contributory copyright infringement, against all Defendants; (3) vicarious copyright infringement, against Dolphin, Hivelocity, and Steadfast; (4) direct trademark infringement, against Dolphin; (5) direct trademark counterfeiting, against Dolphin; and (6) contributory trademark infringement, against Dolphin, Hivelocity, and Steadfast. *Id.* Plaintiff owns a library of copyrighted and trademarked works of adult entertainment. *Id.* ¶ 3. Plaintiff alleges that its works are repeatedly infringed by pirate Internet sites, which display Plaintiff's works without Plaintiff's permission. *Id.* ¶ 4. These sites are allegedly supported by third-party service providers that continue doing business with the sites even after receiving actual notice of infringement from Plaintiff. *Id.* ¶ 6.

Cloudflare is a web performance and security company that offers a content delivery network ("CDN"), web content optimization, website security, denial of service protection, and a managed domain name system network ("DNS"). *Id.* ¶ 25. Cloudflare's website advertises that its CDN caches[3] clients' content and "automatically optimize[s] the delivery of your web pages so your visitors get the fastest page load times and best performance." *Id.* ¶ 26.

---

[1] The Court previously granted Defendant Tiger Media, Inc.'s ("Tiger") motion to dismiss the First Amended Complaint as to it. *See* Docket No. 53. Plaintiff did not seek to file an amended complaint against Tiger. In addition, on February 23, 2017, Plaintiff dismissed Defendants Hebergement OVH Inc. and OVH SAS from this action. *See* Docket No. 113.

[2] Plaintiff filed the Third Amended Complaint after the instant Motion was filed. However, the Third Amended Complaint did not change the allegations or the cause of action asserted against Cloudflare. Because the Third Amended Complaint is now the operative complaint in this action, the Court cites to this version rather than the Second Amended Complaint.

[3] "Generally, a 'cache' is a 'computer memory with very short access time used for storage of frequently or recently used instructions or data.'" *Perfect 10, Inc. v. Amazon.com, Inc.* 508 F.3d 1146, 1156 n.3 (9th Cir. 2007) (quoting *United States v. Ziegler*, 474 F.3d 1184, 1186 n.3 (9th Cir. 2007)).

The TAC alleges that the purpose of Cloudflare's CDN is to "speed a customer's access to the website of Cloudflare's client through a series of data centers maintained by Cloudflare that cache mirror copies of that site." *Id.* ¶ 28. According to Plaintiff, this service allows consumers seeking to access a Cloudflare client's website to retrieve the website's content from the closest Cloudflare data center, rather than accessing the content from the primary host. *Id.* This purportedly results in a client's website content loading twice as fast for website users, regardless of where the users are located. *Id.*

In addition, the TAC alleges that Cloudflare's DNS services "allow pirate sites and their hosts to conceal their identity from copyright owners. The domain registration information for some of the pirate sites . . . indicate that the sites reside on a Cloudflare server in Phoenix, Arizona. When presented with a notice of infringement, however, Cloudflare . . . refuses to disclose the identity of the primary host and site owner. In this fashion Cloudflare acts as a firewall protecting pirate sites and their hosts from legal recourse by copyright owners." *Id.* ¶ 29.

Plaintiff alleges that it sent numerous notices to Cloudflare regarding the infringement of its copyrighted works by Cloudflare's clients. *Id.* ¶ 34. However, Plaintiff alleges that Cloudflare has continued to offer its CDN and related services to these clients, despite the infringement notifications. *Id.* ¶ 37.

Plaintiff seeks actual damages, statutory damages, disgorgement of profits obtained from the infringing activity, trebling of damages, costs and attorney's fees, preliminary and permanent injunctive relief, and such other relief as the Court deems appropriate. *Id.* at 19:20-20:4.

On October 24, 2016, the Court granted-in-part and denied-in-part Cloudflare's Motion to Dismiss the First Amended Complaint. *See* Docket No. 60. The Court dismissed Plaintiff's claims for vicarious copyright infringement, contributory trademark infringement, and unfair competition on the grounds that the FAC failed to adequately plead these claims against Cloudflare. *Id.* However, the Court denied Cloudflare's motion to dismiss the contributory copyright claim, reasoning that Plaintiff had plausibly pled secondary liability based on a material contribution theory. *See id.* at pages 5-9. The Court reasoned that the FAC's allegations that Cloudflare's CDN services made it faster and easier for users to access infringing images, and that consumers seeking access to infringing images retrieved the images from the closest Cloudflare data center rather than the primary host, were sufficient to state a claim for

material contribution under Ninth Circuit precedent. *Id.* at page 7.

Now pending before the Court is Cloudflare's Motion for Partial Summary Judgment ("MSJ"). *See* Docket No. 122. Cloudflare contends it is entitled to judgment with respect to 14 of the 15 alleged direct infringer websites because those websites are not located in the United States, and thus the alleged infringements are extraterritorial and not actionable. *Id.* Plaintiff filed an Opposition to which Defendant filed a Reply. *See generally* Plaintiff's Opposition to Cloudflare's Motion for Summary Judgment ("Opp'n"), Docket No. 130; Reply to Plaintiff's Opposition ("Reply"), Docket No. 144.

On March 30, 2017 the Court issued a tentative ruling and heard oral argument but continued the hearing until April 13, 2017. *See* Court's Civil Minutes March 30, 2017 ("Ruling"), Docket No. 159. The Court's tentative ruling indicated it would grant Cloudflare's motion unless Plaintiff could provide evidence that its images were stored as cache copies on Cloudflare's CDN databases located within the United States. *Id.* at 16. The Court indicated that it would deny Defendant's motion upon a showing that cache copies of images from the at-issue websites were created and stored on Cloudflare's domestic servers. *Id.* The Court allowed Plaintiff to submit an offer of proof to present such evidence. *Id.* Plaintiff filed its Offer of Proof on April 20, 2017. *See* Plaintiff's Offer of Proof ("Offer"), Docket No. 169. Defendant then filed a Sur-Reply. *See* Reply to ALS Scan's Offer of Proof ("Sur-Reply"), Docket No. 174. Both parties then took it upon themselves to file additional documents without leave of the Court. *See* Plaintiff's Motion to Strike New Arguments in Cloudflare's Sur-Reply ("MTS"), Docket No. 178; Cloudflare's Opposition to ALS Scan's Motion to Strike ("Opp'n MTS"), Docket No. 179. The Court entertained additional oral argument on May 5, 2017 and again continued the motion. *See* Civil Minutes May 4, 2017, Docket No. 181.

II. Legal Standard

Summary judgment is proper when the pleadings, the discovery and disclosed materials on file, including any affidavits/declarations, show that "there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law."[4] Fed. R. Civ. P. 56; *see also Miranda v. City of Cornelius*, 429 F.3d 858, 860 n.1 (9th Cir. 2005). To satisfy its

[4] Under Federal Rule of Civil Procedure 56, the same legal standard applies to motions for partial summary judgment and ordinary motions for summary judgment. *See* Fed. R. Civ. P. 56(a): *see also California v. Campbell*, 138 F.3d 772, 780 (9th Cir. 1998); *Barnes v. Cnty. of Placer*, 654 F.Supp.2d 1066, 1070 (E.D. Cal. 2009), *aff'd*, 386 F.App'x 633 (9th Cir. 2010) ("A motion for partial summary judgment is resolved under the same standard as a motion for summary judgment.").

burden at summary judgment, a moving party *with* the burden of persuasion must establish "beyond controversy every essential element of its [claim or defense]." *S. Cal. Gas Co. v. City of Santa Ana*, 336 F.3d 885, 888 (9th Cir. 2003); William W. Schwarzer, et al., Cal. Prac. Guide Fed. Civ. Proc. Before Trial (The Rutter Group 2016) § 14:126 at 14-45. By contrast, a moving party *without* the burden of persuasion "must either produce evidence negating an essential element of the nonmoving party's claim or defense or show that the nonmoving party does not have enough evidence of an essential element to carry its ultimate burden of persuasion at trial." *Nissan Fire & Marine Ins. Co., Ltd. v. Fritz Cos., Inc.*, 210 F.3d 1099, 1102 (9th Cir. 2000).

> If the party moving for summary judgment meets its initial burden of identifying for the court the portions of the materials on file that it believes demonstrate the absence of any genuine issue of material fact, the nonmoving party may not rely on the mere allegations in the pleadings in order to preclude summary judgment[, but instead] must set forth, by affidavit or as otherwise provided in Rule 56, *specific facts* showing that there is a genuine issue for trial.

T.W. Elec. Serv., Inc., v. Pac. Elec. Contractors Ass'n, 809 F.2d 626, 630 (9th Cir. 1987) (internal citations and quotation marks omitted, emphasis in original) (citing, among other cases, *Celotex Corp. v. Catrett*, 477 U.S. 317 (1986)).

"A non-movant's bald assertions or a mere scintilla of evidence in his favor are both insufficient to withstand summary judgment." *FTC v. Stefanchik*, 559 F.3d 924, 929 (9th Cir. 2009). In addition, the evidence presented by the parties must be admissible. *See* Fed. R. Civ. P. 56(e); *see also Pelletier v. Fed. Home Loan Bank of S.F.*, 968 F.2d 865, 872 (9th Cir. 1992) (to survive summary judgment, the non-movant party "ordinarily must furnish affidavits containing admissible evidence tending to show the existence of a genuine dispute of material fact"). Conclusory, speculative testimony in affidavits and moving papers is insufficient to raise genuine issues of fact and defeat summary judgment. *See Thornhill Publ'g Co., Inc. v. GTE Corp.*, 594 F.2d 730, 738 (9th Cir. 1979). With that said, courts do not make credibility determinations or weigh conflicting evidence at the summary judgment stage, and must view all evidence and draw all inferences in the light most favorable to the non-moving party. *See T.W. Elec.*, 809 F.2d at 630-31 (citing *Matsushita Elec. Indus. Co., Ltd. v. Zenith Radio Corp.*, 475 U.S. 574 (1986)); *see also Motley v. Parks*, 432 F.3d 1072, 1075, n.1 (9th Cir. 2005) (en banc).

III. Analysis

A. Undisputed Facts

Cloudflare provides internet services to optimize and protect websites, including by improving transmission of website content and website security for its clients. *See* Cloudflare's Response to Plaintiff's Statement of Additional Genuine Disputes ("PGSD"), Docket No. 176 at ¶ 1. Cloudflare's clients maintain complete existing websites independent of Cloudflare's services, including hosting facilities, internet connectivity, and technical applications required to operate their websites. *Id.* Cloudflare does not own or operate the physical "host"[5] computers that store the permanent copies of its clients' website content, and its services have no impact on the location or substance of those permanent copies. *Id.* ¶¶ 4-5. Indeed, Cloudflare's Terms of Service specify that its services are "offered as a platform to cache and serve web pages and websites and is not offered for other purposes, such as remote storage. *Id.* ¶ 2. Accordingly, [clients] understand and agree to use the [s]ervice solely for the purpose of hosting and serving web pages as viewed through a web browser or other application." *Id.*; Decl. of Trey Guinn ("Guinn Decl.") Ex. A, Docket No. 128 at page 11.

In order to improve transmission of website content, Cloudflare operates a content delivery network ("CDN"), which "takes [clients'] static content and stores a copy closer to [clients'] visitors." PGSD ¶ 17; Decl. of Jay Spillane ("Spillane Decl.") Ex. F, Docket No. 133-6. Cloudflare's CDN is comprised of 102 data centers located throughout the world, including 19 within the United States. PGSD ¶ 16; Spillane Decl. Ex. E, Docket No. 133-5. Cloudflare's Terms of Service state the following with respect to its CDN services:

> To speed up response time for a request that goes to one of our frontline servers, Cloudflare caches parts of websites that are static in these servers. For example, we cache things like images, CSS, and Javascript. We are very conservative with our caching because we never want to mess up dynamic content. So, for example, as a general rule we do not cache HTML. We also refresh the cache relatively frequently, so files are never more than a few hours old. Even being conservative, however, typically 50% of the resources on any given web page are cacheable.

See Spillane Decl. Ex. A at CLOUDFLARE00000131, Docket No. 133-1.

When an end user chooses to visit a Cloudflare client's website, the user is routed through the Cloudflare data server closest to the end user's computer. PGSD ¶ 18. Cloudflare's

[5] The parties use the term "host" in various inconsistent contexts. For example, Cloudflare's Terms of Service state that the primary purpose of Cloudflare's services is the "hosting and serving" of web pages. *See* Guinn Decl. Ex. A ¶ 10. However, the parties agree that Cloudflare is not the host of its clients' websites, in that it does not provide *permanent* storage for its clients' website content. *See* PGSD ¶ 5. For purposes of the instant Motion, the Court uses the term "host" to designate the primary server that stores the permanent content of each client's website.

content caching is dependent on two independent factors: (1) where the end user is located; and (2) how many times the website content is requested at a given data server. *Id.*; *see also* Spillane Decl. Ex. J at CLOUDFLARE00000144, Docket No. 133-10. Because each data server's cached content depends on how many times the website content is requested from that server, Cloudflare does not cache the same resources for a client's website at each data server location. *Id.* As a result, some files are served from Cloudflare's CDN cache, which occurs when the file is available at a particular data center, while other files are served from the origin host server of the client's website, which occurs when the file is not available at a particular data center.[6] *Id.* Cloudflare offers its clients "caching levels: basic, simple, and aggressive." *Id.* ¶ 23. The "aggressive" level is the default setting and unless a client changes its account settings Cloudflare caches all static content with certain file extensions. *Id.* ¶ 21. Twelve of the fifteen sites in question elected to keep the default setting of "aggressive" caching, while two others elected for "basic" caching. *Id.* ¶ 23.

A user can determine whether it is viewing a cache copy of an image sent directly from a Cloudflare data server, as opposed to a copy sent from the host server, based on information contained in the header of the page. *Id.* ¶ 24. For example, Cloudflare's website explains to users that they can determine whether "Cloudflare is caching [a client's] site or a specific file by checking the responses shown in the 'CF-Cache-Status' header," and states that within the CF-Cache-Status header, "HIT" means "resource in cache, served from CDN Cache"; "MISS" means "resource not in cache, served from origin server"; and "EXPIRED" means "resource in cache but has since expired, served from origin server." *Id.*; *see also* Spillane Decl. Ex. J at CLOUDFLARE00000144, Docket No. 133-10. The absence of a "CF-Cache-Status" header, or a "cache control" header value of "private" or "no-cache" also means the image was not served from a CDN server. *Id.* ¶ 38. A user can also determine the location of the CDN database that either supplied a cache copy of the image or transmitted a copy directly from the host server by viewing the three letter airport code in the "CF-RAY" header. *Id.* ¶ 39.

As part of Cloudflare's provision of security services, clients must designate "two Cloudflare nameservers as the authoritative nameservers for the [client's] domain (*e.g.*

[6] The parties have not clarified whether multiple data centers are searched before the content is retrieved from the host server – that is, if the data center nearest to the end user does not have the requested content, are other nearby data centers searched for the content, or is the search automatically routed back to the host server?

bob.ns.cloudflare.com and sara.ns.cloudflare.com)." PGSD ¶ 10; *see also* Spillane Decl. Ex. A at CLOUDFLARE00000131. Cloudflare emphasizes that "[d]esignating Cloudflare as your authoritative nameservers doesn't change anything about your website. Your registrar remains your registrar, and your hosting provider remains your hosting provider, and so on." *Id.* Because Cloudflare is designated as the nameserver, an IP address lookup for a Cloudflare client's website traces to Cloudflare's nameserver address in San Francisco, California, rather than the origin host server address. PGSD ¶ 12. Cloudflare advertises that this service "will mask [client's] IP [address]," which helps protect client's host server from cyber-attacks, and also speeds up client's websites. *Id.* ¶ 13; Spillane Decl. Ex. C at CLOUDFLARE00000142, Docket No. 133-5.

Plaintiff alleges a claim for contributory copyright infringement against Cloudflare based on Cloudflare's provision of services to the following 15 alleged direct infringer websites:

- Bestofsexpics.com
- Cumonmy.com
- Fboom.me
- Greenpiccs.com
- Img.yt
- Imgchili.net
- Imgflash.net
- Imgsen.se
- Imgspice.com
- Imgspot.org
- Imgtrex.com
- Pornwire.net
- Slimpics.com
- Stoorage.com
- Vipergirls.com

PGSD ¶ 3. Although each IP address is masked for these websites, Cloudflare's client records contain the actual IP address for each website, which can be used to trace the country in which the host server for each website is located. *Id.* ¶¶ 4, 14. The IP addresses for 14 of the 15 websites (every website except cumonmy.com) trace to host servers located in foreign countries. *Id.* ¶ 8; *see also* Guinn Decl. ¶ 15, Exs. G-U.[7]

[7] Each exhibit uses basic IP address lookup tools to confirm the location of each at-issue website. *See* Guinn Decl. ¶ 14. The first five pages of each exhibit contain information regarding the respective website from Cloudflare's records; the sixth page contains the IP address lookup results for that website, including the host server location. *See, e.g.* Ex. G at page 6, Docket No. 128 at page 44 (providing lookup results for imgchili.net and listing France as

B. Whether the Underlying Acts of Direct Infringement are Extraterritorial

The only remaining claim against Cloudflare is a claim for contributory copyright infringement. In order to establish a claim for contributory copyright infringement, Plaintiff must first establish the underlying acts of direct infringement by third parties that give rise to the contributory infringement claim. *See, e.g., Perfect 10, Inc. v. Amazon.com, Inc.* ("*Amazon*"), 508 F.3d 1146, 1169 (9th Cir. 2007) ("Secondary liability for copyright infringement does not exist in the absence of direct infringement by a third party." (internal quotation marks and citation omitted)).

Cloudflare contends that it is entitled to summary judgment with respect to 14 of the 15 direct infringer websites because each of those websites are hosted on foreign servers, and therefore Plaintiff's direct infringement claims against those websites consist of wholly extraterritorial acts that are not actionable. *See* MSJ at 3:18-4:1. Plaintiff responds, in part, that the infringement is not wholly extraterritorial because the cache copies created on Cloudflare's CDN within the United States are acts of infringement by the host websites. Opp'n at 9:21-12:25. Cloudflare responds that (1) Plaintiff fails to show cache copies of Plaintiff's images were ever created on Cloudflare's servers within the United States and (2) even if Plaintiff shows cache copies were created domestically, Cloudflare is still entitled to summary judgment based on the affirmative defense of fair use. *See* Reply at 9:4-10:4.

The Ninth Circuit has made clear that "the United States copyright laws do not reach acts of infringement that take place entirely abroad." *See Subafilms, Ltd. v. MGM-Pathe Comm'cns Co.*, 24 F.3d 1088, 1098 (9th Cir.) (en banc), *cert. denied*, 513 U.S. 1001 (1994); *see also Perfect 10, Inc. v. Yandex N.V.*, 962 F.Supp.2d 1146, 1152 (N.D. Cal. 2013) ("It is a well-established principle that, as a general rule, the Copyright Act has no extraterritorial application." (citations omitted)); *Aurora World, Inc. v. Ty Inc.*, 719 F.Supp.2d 1115, 1131 (C.D. Cal. 2009) ("The Ninth Circuit has spoken clearly on the extraterritoriality of the Copyright Act. As [plaintiff] has adduced no evidence of domestic infringement of [two of] its copyrights . . . the court declines to consider these copyrights."); *Danjaq S.A. v. MGM/UA Comm'cns, Co.*, 773 F.Supp. 194, 203

---

the host server location). Plaintiff does not dispute the accuracy of these results, which were also included in Cloudflare's document production; rather, Plaintiff appears to dispute this fact based on its assertion that Cloudflare's services mask the IP address for each website, so the average user is unable to identify the site owner and origin host servers on their own – rather, an IP address lookup by the average user traces to Cloudflare's headquarters in San Francisco, California. *See* PGSD ¶¶ 8, 12. While relevant to the types of services Cloudflare provides to its clients, Plaintiff's contention fails to controvert the fact that 14 of the at-issue websites are in fact located outside of the United States.

(C.D. Cal. 1991) (holding that unauthorized performance of U.S. copyrighted movie in Europe was not actionable under U.S. copyright laws because infringing performance took place entirely abroad). As such, a defendant is not liable for contributory copyright infringement where the underlying acts of direct infringement occur entirely abroad. *Subafilms*, 24 F.3d at 1094-95 (dismissing claim for contributory infringement where direct infringement took place entirely abroad and was therefore not actionable).

Cloudflare contends that there are no actionable acts of direct infringement against the at-issue websites because those websites are hosted on foreign servers. *See* MSJ at 6:26-7:10; *see also* PGSD ¶ 8; Guinn Decl. ¶ 15, Exs. G-U. For purposes of determining the location of an infringing act, Cloudflare asserts that under Ninth Circuit law, an infringing act occurring over the Internet "'takes place'" at the location of the computer responsible for "hosting" the allegedly infringing content.[8] *See* MSJ at 6:10-23. Because the websites are "hosted" on foreign servers, Cloudflare contends that the infringing acts took place entirely abroad, and therefore are not actionable. *Id.*

In support, Cloudflare relies on *Amazon*, 508 F.3d at 1159-62. However, *Amazon* is not directly on point with the instant case. *Amazon* did not involve extraterritoriality, but rather revolved around whether Google could be liable for direct infringement (and separately,

---

[8] Cloudflare correctly refers to this as the "server test," however, Cloudflare's characterization of the test is not entirely correct. In *Amazon*, the Ninth Circuit affirmed the following standard for direct copyright infringement under the "server test" applied by the district court:

> [A] computer owner that stores an image as electronic information and serves that electronic information directly to the user . . . is displaying the electronic information in violation of a copyright holder's exclusive display right. Conversely, the owner of a computer that does not store and serve the electronic information to a user is not displaying that information, even if such owner in-line links to or frames the electronic information. The district court referred to this test as the "server test" . . . . As explained below, because this analysis comports with the language of the Copyright Act, we agree with the district court's resolution . . . .

See 508 F.3d at 1159.

Under the server test, courts have not limited liability for copyright infringement to the permanent copies of infringing images that are stored on the primary "host" computer, as that term has been used by the parties in this matter – *e.g.*, the origin server where the original copy is stored. Rather, the Ninth Circuit has made clear that liability for infringement exists where a copy of an infringing image is stored on a computer server, regardless of whether that computer is the primary "host" of the infringing website's content. *See Amazon*, 508 F.3d at 1160 (holding that Google could be held directly liable for thumbnail copies of images derived from infringing websites, even though Google was not primary host of those websites, because the thumbnail copies were stored on Google's computer servers).

contributory infringement) based on its practice of linking users to websites that displayed infringing images, and also its practice of indexing and storing thumbnail copies of infringing images on its servers. *Id.* The Ninth Circuit held that Google could not be liable for linking users to infringing images, because Google did not store actual copies of the infringing images – rather, Google used "HTML instructions that direct a user's browsers to the website publisher's computer that store the full-size photographic image." *Id.* at 1161. It was explained that "Google's cache merely stores the text of webpages," and "[p]roviding these HTML instructions is not equivalent to showing a copy." *Id.* The Ninth Circuit thus held that "[b]ecause Google's computers do not store the photographic images, Google does not have a copy of the images for purposes of the Copyright Act. In other words, Google does not have any 'material objects . . . in which a work is fixed . . . and from which the work can be perceived, reproduced, or otherwise communicated' and thus cannot communicate a copy." *Id.* at 1160-61 (quoting 17 U.S.C. § 101). Thus, Google's practice of linking users to infringing websites was not an infringing act under the server test. *See id.* at 1159.

However, the *Amazon* court separately held that Google *could* be liable for direct infringement based on its practice of indexing and storing thumbnail copies of infringing images, because those thumbnail copies were actually stored on Google's servers. *Id.* at 1160 (emphasizing that "[t]here is no dispute that Google's computers store thumbnail versions of [plaintiff's] copyrighted images and communicate copies of those thumbnails to Google's users"); *see also MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 517-18 (9th Cir. 1993) (holding that a computer makes a "copy" of a software program for purposes of copyright infringement liability when it transfers the program from a third party computer into its own memory). The *Amazon* court ultimately held that Google's indexing and storing of thumbnails was not actionable because it constituted fair use. *See Amazon*, 508 F.3d at 1163-68 (holding Google's use of thumbnail images constitutes fair use under requisite four-factor common law test codified in the Copyright Act). The Ninth Circuit also upheld the district court's ruling that end users who clicked on the in-links and then viewed the offending sites did not commit acts of direct infringement. *Id.* at 1169-70. Specifically, the court found that the cache copies automatically created by an end user's computer upon viewing a website were fair use and thus could not be the basis for contributory liability for Google. *Id.*

Cloudflare also relies on *Yandex*, which held that a defendant could not be liable under

U.S. copyright laws for user-uploaded infringing images hosted on servers located in Russia. 962 F. Supp. 2d at 1153. In *Yandex*, the court emphasized that the mere fact that copyrighted images could be downloaded from the foreign servers to computers in the United States did not establish that infringing acts had taken place in the United States. *Id.* However, the court also held that the plaintiff's alternative theory that infringing acts could have taken place in the United States because the defendant previously operated data servers located in the United States, which could have stored infringing images, was a "more plausible" variation of liability, but ultimately rejected it for lack of proof. *Id.* (emphasizing that the plaintiff failed to "demonstrate that [defendant] in fact stored or displayed full-sized copies of the [plaintiff's] images on [defendant's] United States servers").

Here, it is undisputed that cache copies of Cloudflare clients' files are stored on Cloudflare's data servers; it is also undisputed that some of those data servers are located in the United States. *See* PGSD ¶¶ 16-22; Spillane Decl. Ex. F. It is also undisputed that those cache copies are the product of third parties' decision to register and pay for Cloudflare's caching service. *Id.* Thus, to the extent cache copies of Plaintiff's images have been stored on Cloudflare's U.S. servers, the creation of those copies would be an act of direct infringement by a given host website within the United States.

Indeed, Plaintiff provides several cases that support this conclusion. For example, Plaintiff cites *L.A. News Serv. v. Reuters Television Int'l., Ltd.*, 149 F.3d 987, 991-92 (9th Cir. 1998), in which the Ninth Circuit held that a defendant can be liable for direct infringement under U.S. copyright laws where at least one infringing act occurs within the United States. The Ninth Circuit distinguished *Subafilms*, explaining that in *Subafilms*, no infringing act had taken place within the United States – the only action that took place within the United States was the authorization of foreign distribution of the infringing material. *Id.* at 992. In contrast, in *Reuters*, the defendant had made copies of the infringing material in the United States, had transmitted the copies to a third party, which also made copies in the United States and then transmitted those copies to a foreign agency, which in turn distributed copies in a foreign country. *Id.* at 991. The court held that the defendant could be liable under U.S. copyright law for the foreign copies that were distributed, emphasizing that "[e]ach act of copying constituted a completed act of infringement," and since some of the acts took place in the United States the infringing acts were not wholly extraterritorial. *Id.*

Plaintiff also relies on *Shropshire v. Canning*, 809 F.Supp.2d 1139, 1146 (N.D. Cal. 2011), in which a Canadian defendant uploaded an infringing video from Canada to YouTube, which caused copies of the video to be made on YouTube's servers in California. The court held that the defendant's actions were not wholly extraterritorial even though the original infringing copy was made in Canada because the defendant's "direct action led to the creation of a copy of the [infringing video] on YouTube's servers in California, and to the subsequent viewing of the video by potentially thousands in the United States." *Id.* The court further emphasized that notwithstanding the defendant's protests that it had only uploaded the video to YouTube's Canadian web address, the fact that copies ended up on YouTube's California servers rendered the defendant liable under U.S. copyright laws because "[d]irect infringement does not require intent or any particular state of mind." *Id.*

Similarly, in *L.A. News Serv. v. Conus Comm'cn Co. Ltd.*, 969 F.Supp. 579 (C.D. Cal. 1997), the court held that U.S. copyright laws applied to a Canadian broadcaster that broadcasted infringing material from Canada to Canadian residents, because the material was picked up by United States networks and viewed in the United States. *See* 969 F. Supp. at 583-84 (emphasizing that it did not matter whether the primary infringer (the broadcaster) intended for the infringing material to reach audiences in the United States).

In response, Cloudflare contends that the location of Cloudflare's data servers is irrelevant, because it is only the location of the underlying direct infringement that matters for purposes of contributory copyright liability. *See* MSJ at 8:8-22. Cloudflare points out that Plaintiff has not attempted to state a claim for direct infringement against Cloudflare. *Id.*

However, Plaintiff is not attempting to argue that Cloudflare is directly liable for the infringing content potentially stored on Cloudflare's U.S. servers – rather, Plaintiff's contention is that the third-party websites themselves are directly liable for the copies purportedly stored on Cloudflare's U.S. servers, and thus the underlying direct infringement is not wholly extraterritorial. *See* Opp'n at 14:9-14 ("Even accepting that the first infringing copy was made and stored on a foreign origin server, the site owners took action that caused reproduction, display and distribution of infringing works on Cloudflare's domestic servers."). Cloudflare fails to explain why the infringing websites do not commit actionable direct infringement, within the U.S., when they cause the creation of "[copies]…closer to the [sites'] visitors" on Cloudflare's domestic servers. *See* PGSD ¶ 17.

Cloudflare also argues that computer caching itself is an automatic, non-volitional process for which a defendant cannot be liable. *See* Reply at 6:21-9:3. However, the cases on which Cloudflare relies involve situations where the caching service (such as Cloudflare) itself is sued for direct infringement; they do not address whether the third party responsible for the infringing material can be liable for such copies. *See Perfect 10, Inc. v. Giganews, Inc.*, 847 F.3d 657, 666 (9th Cir. 2017). Moreover, no court has actually held that cache copies that are transmitted and displayed to users are not infringing material; rather, the relevant case law holds that a caching service cannot be directly liable if it takes no volitional act to cause the copies to be made. For example, in *Giganews*, which Cloudflare heavily relies on, the Ninth Circuit held that to establish direct infringement, a plaintiff must "show causation (also referred to as 'volitional conduct') by the defendant." *Id.* at 666. The court explained that this term "does not really mean an 'act of willing or choosing' or an 'act of deciding,'" but rather "'simply stands for the unremarkable proposition that proximate causation historically underlines copyright infringement liability no less than other torts.'" *Id.* (citations omitted). Put simply, the court explained that this requires that a "defendant cause the copying." *Id.* (citation omitted). Thus, the *Giganews* court held that the plaintiff had failed to establish a direct infringement claim against an internet service provider that supplied server storage to clients because the evidence only showed that the provider was a passive host pursuant to which users could post infringing images, which "does not demonstrate that [defendant] – as opposed to the user who called up the images – caused the [infringing] images to be displayed." *Id.* at 668. It was emphasized that there was "no evidence showing [defendant] exercised control (other than by general operation of [its] service); selected any material for upload, download, transmission, or storage; or instigated any copying, storage, or distribution." *Id.* at 670. Moreover, the Ninth Circuit distinguished *Amazon*, explaining that in *Amazon*, Google could be liable for storing thumbnail versions of infringing images on its servers because Google engaged in volitional conduct by initiating the indexing and organization of those images, and thus was more than a passive host. *Id.*; *see also Costar v. LoopNet, Inc.*, 373 F.3d 544, 555 (4th Cir. 2004) (holding that "automatic copying, storage, and transmission of copyrighted materials, *when instigated by others*, does not render an ISP strictly liable for copyright infringement . . . . An ISP, however, can become liable indirectly upon a showing of additional involvement sufficient to establish a contributory or vicarious violation of the [Copyright] Act." (emphasis added)).

Here, in contrast, the at-issue websites are not merely passive hosts. Rather, as in *Reuters*, *Shropshire*, and *Canning*, the at-issue websites created the copies of the infringing images, uploaded them to their websites, and elected to use Cloudflare's services thereby purportedly creating additional copies in the United States.[9] *See Reuters*, 149 F.3d at 990-92 (holding news agency liable under U.S. copyright laws for making infringing copy in the United States and transmitting it to foreign news agency, which proceeded to make copies of the infringing copy and distribute them in foreign country); *Shropshire*, 809 F.Supp.2d at 1146 (Canadian citizen liable under U.S. copyright laws for uploading infringing video in Canada because copies were then made on servers in United States); *Conus*, 969 F.Supp. at 583 (Canadian broadcaster liable under U.S. copyright laws for infringing broadcast picked up and displayed on U.S. television sets, regardless of fact that broadcast was intended to only reach television sets in Canada). In other words, the infringing sites took the volitional step to pay for, and utilize, Cloudflare's CDN servers.[10] As such, the at-issue websites could be liable under U.S. copyright laws provided cache copies of their images were created and stored on Cloudflare's domestic CDN servers. Cloudflare also relies on *Giganews* and *Amazon* in its Sur-Reply to argue that the infringing websites themselves cannot be liable for cache copies because they do not engage in volitional conduct each time a cache copy is made. Sur-Reply at 21:6-16. However, as explained above, neither case addressed the potential liability of the users who initially uploaded the infringing images onto the networks.

C. Whether Plaintiff Provides Sufficient Evidence of Domestic Caching

Plaintiff submits evidence it contends proves its copyrighted images were copied and stored temporarily on Cloudflare's CDN servers in the United States. *See* Proof at 6:22-9:12, 11:16-13:14. Plaintiff's evidence consists of screenshots from URL "lookups" generated by "response header sites" Redbot.org and Hurl.it ("Redbot Reports" and "Hurlit Reports") as well

[9] For the first time in its Reply, Cloudflare asserts that "infrastructure-level caching" is a fair use. *See* Reply at 9:5-11:12. The Court addresses this argument in full below.

[10] Defense counsel repeated this line of argument at the May 25, 2017 hearing and directed the Court to consider the undisputed fact that the third party sites do not affirmatively decide whether a given image is cached by a given server at a given time. *See* Reporter's Transcript of May 25, 2017 hearing at 20:13-21:2. This analysis fails to address the volitional act that occurred here: Cloudflare's clients sign up, pay for, and utilize Cloudflare's caching services. Such conduct is sufficient to show the third party infringers caused the copies to be created. *See Giganews*, 847 F.3d at 666 (explaining that the causation requirement "does not really mean an 'act of willing or choosing' or an 'act of deciding,'" but rather "'simply stands for the unremarkable proposition that proximate causation historically underlines copyright infringement liability no less than other torts'").

as a Google Chrome application "HTTP Header" ("HTTP Reports") that performs a similar function. PGSD ¶ 42; *see, e.g.*, Penn Decl. Ex. 6 at page 5; Supplemental Declaration of Eric Penn ("Penn Supp. Decl.") Exs. 1-21, Docket No. 170. Each report contains a series of headers, including a "CF-Cache-Status" header and a "CF-Ray" header. PGSD ¶¶ 38-39. The CF-Cache-Status header shows whether or not a cache copy of a given image was sent from one of Cloudflare's CDN servers. *Id.* ¶ 38. Alternatively, the "CF-Ray" header contains a three letter airport code that corresponds to the location of the Cloudflare server that either provided a cache copy of the image, or served the image directly from the host's server. PGSD ¶ 39; Declaration of Kenneth Carter ("Carter Decl.") ¶ 7, Docket No. 144-2. The absence of a CF-Cache-Status header, or a Cache-Control header value of "private" or "no-cache" also means that the image was not cached. PGSD ¶ 38.

In Plaintiff's initial opposition filed in March, it argued that a series of Redbot Reports prove that cache copies of images from ten of the offending sites were created on Cloudflare's domestic servers. PGSD ¶ 25; *see also* Penn Decl. ¶ 10. As pointed out in the Court's first tentative ruling, this evidence is deficient for numerous reasons. Ruling at 13-14. First, as Cloudflare points out, Plaintiff submits Redbot Reports for only seven of the 14 at-issue websites. *See* Reply at 11:15-12:18 (providing chart of images provided for each website, with respective citations). Second, with respect to the seven websites for which Plaintiff does provide Redbot Reports, the header reading "CF-Cache-Status: HIT" does not establish that the image was copied on a Cloudflare server located *in the United States*. Rather, the reports show that cache copies of the images were sent from a Cloudflare server in Sydney, Australia. *See* PGSD ¶¶ 20, 39; Reply at 12:19-24; Carter Decl. ¶ 7. Thus, the Redbot Reports *alone* do not provide sufficient evidence of domestic caching to survive summary judgment.

Plaintiff's Offer of Proof, filed April 20, 2017 relies on additional screen shots of Hurl.it Reports and HTML Reports. Proof at 6:22-9:13. Plaintiff purportedly switched from Redbot.org to Hurl.it after discovering that Redbot.org's servers are located in Hong Kong, a fact Plaintiff contends explains why all of the Redbot Reports on the record contain a CF:RAY header corresponding to Cloudflare's Sydney, Australia server, as opposed to a domestic one. Offer at 6:22-7:1; Supp. Penn Decl. ¶¶ 3-4. Hurlit.com's servers are purportedly located in Virginia. Supp. Penn. Decl. ¶ 7. The results of the Hurl.it Reports vary from site to site but do show the creation and storage of images from three of the infringing sites: imgchili.com, slimpics.com,

and bestofsexpics.com on Cloudflare servers within the United States. *See* Offer at 7:2-9:13, 11:16-21; Supp. Penn Decl. Exs. 1-3. Plaintiff also submits reports using HTTP Header. Supp. Penn Decl. ¶ 9; Supplemental Declaration of Jay Spillane ("Supp. Spillane Decl.") Exs. 1-10, Docket No. 171. The HTTP Reports also demonstrate domestic caching of images from imgchili.com, slimpics.com, and bestofsexpics.com, and show domestic caching from a fourth site, greenpiccs.com. Supp. Penn Decl. Ex. 14; Supp. Spillane Decl. ¶ 4. Specifically, for imgchili.com, slimpics.com, and bestofsexpics.com, both the Hurlit Reports and the HTTP Reports contain the header "CF-Cache-Status: HIT" and one of the two location headers, "CF-RAY: 33c08af3bd0d96581-DFW" or "CF-RAY: 33c08af3bd0d96581-IAD".[11] Supp. Penn Decl. Exs. 1-3. The same result appeared for an image from greenpics.com, but only on the HTTP Report. Supp. Penn Decl. Ex. 14; Supp. Spillane Decl. ¶ 4. This evidence shows that cache copies of images from these four websites were created and stored on domestic servers. Therefore, the Court would find that Plaintiff has created a triable issue of fact as to whether the primary infringement by these four sites was not entirely extraterritorial.

Cloudflare argues Plaintiff's Offer of Proof fails to establish any domestic infringement of the images at issue in this case for two reasons. First, Cloudflare contends the Hurl.it Reports and HTTP Reports relate to images that are not at-issue in this case. *See* Sur-Reply at 9:12-10:13. Cloudflare bases this contention on what it claims was Plaintiff's failure to produce, or disclose these images during discovery. *Id.* Cloudflare further argues that, even if the four images submitted with Plaintiff's Offer of Proof are at issue in this case, it is still entitled to summary judgment as to every other image in this litigation. *Id.*

The Court would agree that Plaintiff has only submitted direct evidence of domestic caching of the four images provided in its Offer of Proof. First, it is undisputed that Cloudflare's CDN servers only create cache copies of images in response to multiple requests. PGSD ¶ 35. Second, with the exception of the specific images submitted with its Offer of Proof, Plaintiff fails to present any evidence that any end users made requests for these images. Plaintiff thus fails to demonstrate actionable direct infringement through direct evidence for the remaining images. *See Amazon*, 487 F.3d at 726 (plaintiff failed to show direct infringement by end users because it presented no evidence that users ever stored infringing images on their computers); *see also*

[11] DFW and IAD are domestic airport codes that indicate the cached images came from Cloudflare servers in these two domestic locations.

Yandex, 962 F.Supp.2d at 156 (granting summary judgment in favor of defendant on contributory infringement claim because plaintiff failed to adduce evidence that end users in the U.S. actually downloaded the offending images.) Here, like the plaintiffs in *Amazon* and *Yandex*, Plaintiff seeks to ground a contributory infringement claim in acts of direct infringement but presents no evidence that such acts ever occurred. Instead, Plaintiff asks the Court to assume end users in the U.S. requested access to the copyrighted images, requests, which in turn, caused cache copies of those images to be created on CDN servers. As in, *Yandex*, while such requests, and corresponding cache copies could have been made, Plaintiff fails to directly show they were, at least on an image-by-image basis. *See Yandex*, 962 F. Supp. 2d at 1153 ("[Plaintiff's] speculation that full-size image storage may have occurred in the United States is insufficient at the summary judgment stage, which is the point in litigation to stand and deliver on admissible evidence."). However, unlike in *Yandex* and *Amazon*, Plaintiff has presented direct evidence of specific acts of infringement from each site as well as significant circumstantial evidence of Cloudflare's processes. Further, the question of image-by-image summary adjudication was not fully briefed by either side. As a result, and given the complicated and evolving nature of both parties' claims and defenses, the Court would not grant summary adjudication on any specific images from cumonmy.com, imgchili.com, slimpics.com, bestofsexpics.com, and greenpics.com at this time.[12]

The Court is also not convinced that Plaintiff's discovery responses preclude it from trying its contributory infringement claims based on images from these four sites. As Plaintiff points out, it retains the right to supplement its discovery responses and disclosures where new information or evidence comes into its possession. *See* MTS at 1; *see also generally* Fed. R. Civ. Proc. § 26(e)(1))(A). Defendant also does not show, or even argue it has been prejudiced by Plaintiff's alleged failure to produce or disclose these images so as to warrant excluding the material entirely.

Plaintiff also submits Hurl.it Reports and HTTP Header Reports for five other sites,

[12] It is also unclear Plaintiff is required to present direct evidence of copying for each image at issue to survive summary judgment. *See Three Boys Music Corp. v. Bolton*, 212 F.3d 477, 481 (9th Cir. 2000) (noting copying may be shown through circumstantial evidence and often is); *Columbia Pictures Indus. v. Gary Fung*, 710 F.3d 1020 (9th Cir. 2013) (same); *see also Capitol Records, Inc. v. Thomas*, 579 F. Supp. 2d 1210, 1225 (D. Minn. 2008) ("[D]irect proof of actual dissemination is not required by the Copyright Act. Plaintiffs are free to employ circumstantial evidence to attempt to prove [a violation]."); *see also BMG Rights Mgmt. (US) LLC v. Cox Communs.*, 149 F.Supp.3d 634, 663 (E.D. Va. 2015). Moreover, if Defendant believes it is entitled to summary judgment on an image-by-image basis it must move on such grounds.

stooorage.com, imgsen.se, imgspot.org, img.yt, and imgflash.net that do not contain CF-Cache-Status and CF-RAY headers that indicate cache copies of images from those sites were created on Cloudfare's domestic servers. *See* Proof at 7:2-9:13 (table showing results of Redbot, Hurl.it and HTTP Header reports). The reports for these sites contained no "CF-Cache Status" header at all. *Id.* While these reports do contain CF-RAY headings bearing domestic location codes the absence of a CF-Cache-Status header indicates that cache copies of the images were not created on Cloudfare's server. PGSD ¶ 38. In this scenario, the airport code contained in the CF-RAY header merely corresponds to the Cloudflare CDN server that transmits the image - without creating a cache copy - directly from the host server. *Id.* In the case of imflash.com, the site has gone offline sometime after Plaintiff's Redbot Reports were generated. Proof at 7:24-28.

As discussed above, Plaintiff did receive Redbot Reports that show cache copies of images from these five sites were created on a Cloudflare CDN server in Sydney, Australia. *See* PGSD ¶¶ 20, 39; Reply at 12:19-24; Carter Decl. ¶ 7. Thus, as it relates to these five sites, Plaintiff's evidence only shows (1) cache copies of images from these sites were at one time located on one of Cloudflare's foreign CDN servers and (2) images from these sites (with the exception of the offline imgflash.com) are currently transmitted through Cloudflare's domestic CDN servers, but are not currently being cached on Cloudflare's domestic servers.

Plaintiff contends, this is enough circumstantial evidence to create a triable issue of fact as to whether images from these five sites were ever stored on domestic servers. Offer at 12:16-13:14. However, absent any direct evidence of a single instance of domestic caching of images from these sites, the Court would find that Plaintiff fails to create a triable issue of fact as to whether any images from these five sites were cached domestically. The same is true of the three remaining sites, Imgspice.com, fboom.me and imgretx.xom sites, none of which brought back direct evidence of domestic, or any type of caching. *Id.* at 7:9-9:13 (table showing results of Redbot, Hurl.it and HTTP Header reports). Plaintiff's only circumstantial evidence as to these sites is that each Hurl.it Report shows a domestic server location. But such results only show that a Cloudflare server transmitted an image directly from the host server, an act that, pursuant to the Ninth Circuit's server test, takes place at the location of that server and is thus extraterritorial. *Amazon*, 508 F.3d at 1159. Because Plaintiff has failed to establish that any of its images were actually stored on Cloudflare's U.S. data servers by 10 of the 15 at-issue websites, the underlying infringement by those sites of Plaintiff's right of duplication is not

actionable under U.S. copyright laws and therefore cannot give rise to contributory infringement claims against Cloudflare.[13] However, because Plaintiff has shown at least four acts of domestic copying the Court would deny the motion in part, unless the fair use doctrine applies.[14]

D. Whether the Cache Copies are "Fair Use"

For the first time in its Reply, Cloudflare asserts that "infrastructure-level caching" is a fair use. *See* Reply at 9:5-11:12. Defendant reiterates this argument in its Sur-Reply to argue that the cache copies created on Cloudflare's CDN, even if they would otherwise be domestic infringement, are not actionable under the fair use defense. Sur-Reply at 19:1-23. While the Court did not fully address this issue in its prior tentative, it did indicate its reluctance to conclude that the *third party infringers'* utilization of Cloudflare's caching technology is a fair use. Ruling at 13. Upon further review, the Court remains unconvinced.

The doctrine of fair use is a common law doctrine of judicial creation later codified in Section 107 of the Copyright Act. Section 107 states:

> In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include—
>
> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
> (2) the nature of the copyrighted work;
> (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole;
> (4) and the effect of the use upon the potential market for or value of the copyrighted work.

17 U.S.C. § 107.

"[Since] the [fair use] doctrine is an equitable rule of reason, no generally applicable

[13] Plaintiff repeatedly raises what appears to be an alternative theory of extraterritoriality based on the fact that Cloudflare masks its customers' actual IP addresses, which Plaintiff contends deprives copyright owners of contact information for site owners and origins servers. *See, e.g.*, Opp'n at 8:18-9:20. Plaintiff contends that this conduct has "domestic impact" that renders the 14 at-issue websites within the purview of U.S. copyright laws. *Id.* Plaintiff cites to no authority in support of this theory and, in any event, this theory was expressly rejected in *Subafilms. See Subfilms*, 24 F.3d at 1095 (holding that U.S. copyright laws do not extend to extraterritorial acts of infringement even "where such acts result in adverse effects within the United States").

[14] Cloudflare also argues, in its Sur-Reply that Plaintiff failed to plead a theory based on the creation and storage of cache copies by the third party infringers. Sur-Reply at 20:6-21:14. The Court rejects this argument because nothing in the TAC indicates Plaintiff limited its infringement theory to the copies of Plaintiff's images stored on the host sites' own servers. To the contrary, Plaintiff alleges that the infringing sites utilized Cloudflare's services, services it alleges create and store cache copies of copyrighted materials on Cloudflare's CDN. *See* TAC ¶¶ 5, 28, 30, 34-35.

definition is possible, and each case raising the question must be decided on its own facts." *Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 560 (1985). Courts "must balance these factors in light of the objectives of copyright law, rather than view them as definitive or determinative tests." *Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 818 (9th Cir. 2002); *see also Campbell v. Acuff–Rose Music, Inc.*, 510 U.S. 569, 578 (1994) ("All [the factors] are to be explored, and the results weighed together, in light of the purposes of copyright."). As an affirmative defense, the burden is on Defendant to prove fair use. *See Amazon*, 508 F.3d at 1158; *see also Sega Enters. v. Sabella*, No. C 93-04260 CW, 1996 WL 780560, *9, (N.D. Cal. Dec. 18, 1996) ("It is [defendant's] burden to show that the fair use doctrine applies.").

As an initial matter, the Court notes that Plaintiff has not brought a direct infringement claim against Cloudflare. *See* MSJ at 2:25-3:14. Therefore, to escape liability for contributory infringement based on a fair use defense, Cloudflare must demonstrate the primary infringers' unauthorized copying of Plaintiff's images is fair use. *See Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 447-55 (applying fair use factors to the acts of direct infringers not the acts of the related defendant asserting the defense); *see also* 3 Nimmer on Copyright § 12.04 (2017) ("The Supreme Court gauged the fair use of the contested Betamax recorder against the circumstances of the primary infringers, not the related defendant who happened to be present in court.") In other words, the proper inquiry is whether the cache copies that the third party sites created are a fair use.

This distinction is somewhat lost on Cloudflare who contends "because the fair use factors look at the nature of the use, not the identity of the user" it makes no difference who engages in the alleged fair use. Sur-Reply at 19:1-20:5. This position is at odds with the Ninth Circuit case law on which Cloudflare relies. *See Amazon*, 508 F.3d at 1165 ("A use is considered transformative only where a *defendant* changes a plaintiff's copyrighted work or uses the plaintiff's copyrighted work in a different context such that the plaintiff's work is transformed into a new creation."). Cloudflare cites *Amazon*, as well *as Rosen v. eBay, Inc.*, No. CV 13-6801 MWF-EX, 2015 WL 1600081 (C.D. Cal. Jan. 16, 2015) for the proposition that fair use analysis is the same regardless of the identity of the direct infringer. Sur-Reply at 19:1-23. However, the *Amazon* court did not address fair use in the context of a website that uploads copyrighted images to the web. 508 F.3d at 1169. In fact, in asserting its fair use defense in that case, Google did not even contest that certain third party websites had directly infringed on the

plaintiff's copyrights. *Id.* at 1165.

Similarly, *Rosen* applied the fair use doctrine to two types of alleged infringement by E-Bay. First, it ruled that E-Bay's automatic creation of cache copies of copyrighted images was fair use. *Rosen*, 2015 WL 1600081, *20-21. The court also ruled that E-Bay's decision to upload pictures taken by a user of magazines containing copyrighted images was fair use by both E-Bay and the original uploader. *Id.* at 19-20. In doing so, the court applied a separate fair use analysis, unrelated to infrastructure level caching to hold "copies made of a magazine containing depictions of a copyrighted work, for the purpose of selling that magazine under the first sale doctrine, do not violate the Copyright Act under the fair use doctrine as codified in 17 U.S.C. § 107." *Id.* at 20. The *Rosen* court did not address whether or not the identity of a given infringer affects the fair use analysis generally, it simply held that E-Bay's posting of the images, and the E-Bay user who submitted the images, were both entitled to the defense. *Id.* In other words, the specific facts in *Rosen* meant the identity of the alleged infringer did not change the outcome of the court's fair use analysis because both E-Bay and the seller used the photos for the same purpose: to sell the magazines under the first sale doctrine. *Id.*

Further, the Ninth Circuit rejected a similar version of Cloudflare's argument in *Reuters*. The defendant there argued that its sale of copyrighted footage to news services must be fair use because the news services' ensuing use of the footage would be fair use. *See Reuters*, 149 F.3d at 994. The Ninth Circuit rejected this argument because "the question of whether defendants' copying and transmission of the works constitutes fair use is distinct from whether their subscribers' broadcasts of the works are fair use." *Id.* The same principal applies here: the question of whether the infringing sites' creation of cache copies constitutes fair use is distinct from whether *Cloudflare's* maintenance of its CDN would constitute fair use. *Id.*

1. Purpose and Character of Use

The Ninth Circuit has adopted a two-step analysis for this factor. *Kelly*, 336 F.3d at 818-19. First, a court determines whether the use is commercial in nature, and second, the court asks whether such use, even if it is commercial, is transformative. *Id.* While not determinative, "the more transformative the new work, the less important the other factors, including commercialism, become." *Id.* at 818; *see also Campbell*, 510 U.S. at 579 ("Although … transformative use is not absolutely necessary for a finding of fair use, the goal of copyright protection … is generally furthered by the creation of transformative works.").

Here, the third party websites are undoubtedly using Plaintiff's images for commercial gain. Further, in electing to utilize Cloudflare's CDN to store copies of the infringing images closer to their customers, the sites do not change the function of the images. Rather, the cache copies of the images, like those stored on the sites' foreign servers, are exact replicas of Plaintiff's images, used for the same purpose, enjoyment of the images by the sites' visitors. At least as it pertains to the infringing sites, the cache copies serve no other purpose than to supplant Plaintiff's original use of the works. Courts have found such use to be, at best minimally transformative. *See Wall Data Inc. v. L.A. County Sheriff's Dep't*, 447 F.3d 769, 778 (9th Cir. 2006) ("The Sheriff's Department created exact copies of RUMBA's software. It then put those copies to the identical purpose as the original software. Such a use cannot be considered transformative."); *Designer Skin, LLC v. S & L Vitamins, Inc.*, 560 F. Supp. 2d 811, 823-24 (D. Ariz. 2008) (images were minimally transformative when used for the same purpose as the original images).

Cloudflare argues that categorically "infrastructure-level caching" is a fair use and is essential to the functioning of the modern internet. *See* Reply at 9:5-11:12. In support, Cloudflare relies on *Amazon*, which is distinguishable from the instant case. In *Amazon*, the Ninth Circuit held that where an individual user links to an infringing site, and the user's computer automatically makes a cache copy of the infringing images, those copies are transformative because the copy is "designed to enhance an individual's use, not to supersede the copyright holders' exploitation of their works." *See* 508 F.3d at 1169. Here, in contrast, the cache copies are not copies made as part of an individual user's interaction with the internet generally, but rather copies of the infringing images created at the direction of the third party websites to expedite its ability to send those images to its end users. Unlike in *Amazon*, the cache copies here are the intended consequence of the third party infringers' utilization of Cloudflare's CDN. *See* PGSD ¶ 17 ("A content delivery network (CDN) takes your static content and stores a copy closer to your visitors."). Moreover, as discussed above, the question of whether an end user's actions constitute fair use, is different than the question of whether the party that provides the copyrighted materials to the end user engages in fair use. *Reuters*, 149 F.3d at 994.

The other cases relied on by Cloudflare all hold that an internet search engine/service provider – *not the third party responsible for distribution of the infringing images* – cannot be

liable for direct infringement based on cache copies automatically made on its servers. Cloudflare provides no case holding that the third party infringer that *causes* the infringing copies to be made and distributed is entitled to the fair use defense. *See, e.g.*, *Rosen*, 2015 WL 1600081, *21. (holding that eBay's creation of CDN cache copies in connection with eBay users' sales of goods was a fair use because it was "designed to enhance a user's use, not to supersede the copyright holders' exploitation of their works"). Indeed, Cloudflare's entire argument with respect to this defense appears to be asserting that Cloudflare is entitled to a fair use defense. *See, e.g.*, Reply at 10:5-11:2 (discussing why Cloudflare's services enhance an individual user's use and therefore constitute a fair use). But Cloudflare's fair use defense is of limited relevance to the direct infringers' defense. *See Reuters*, 149 F.3d at 994; *see also Religious Tech. Ctr.* v. *Netcom*, 907 F. Supp. 1361, 1378 (N.D. Cal. 1995) ("The proper focus here is on whether [the defendant's] actions qualify as fair use, not on whether [the infringing third party content poster] himself engaged in fair use."); *Sega Enters. v. MAPHIA*, 948 F. Supp. 923, 933-34 (applying fair use factors to the primary infringers' actions not the defendant raising the fair use defense to evade secondary liability); *Sabella*, 1996 WL 780560, *9-11 (finding Defendant accused of contributory infringement failed to establish fair use defense because the acts of direct infringers did not support the defense).

ii. Nature of the Copyrighted Work

When the copyrighted work is creative in nature, such as photographs meant to be viewed for aesthetic purposes, this factor weighs against a finding of fair use. *Kelly*, 336 F.3d at 820; *MAPHIA*, 948 F. Supp. at 934; *see also Wall Data*, 447 F.3d at 780 ("In analyzing the second fair use factor, we look at the nature of the copyrighted work, creative works being closer to the core of intended copyright protection than informational and functional works." (internal quotations omitted)). Here, the material at issue is photographs created for aesthetic value. However, this factor will not count against fair use if the "secondary user only copies as much as is necessary for his or her intended use." *Kelly*, 336 F.3d at 820-21. The second factor thus weighs against fair use.

iii. Amount and Substantiality of the Portion Used

"While wholesale copying does not preclude fair use per se, copying an entire work militates against a finding of fair use." *Kelly*, 336 F.3d at 820; *but see Amazon*, 508 F.3d at 1165 ("The fact that Google incorporates the entire Perfect 10 image into the search engine results

does not diminish the transformative nature of Google's use . . . . even making an exact copy of a work may be transformative so long as the copy serves a different function than the original work."). Here, the offending sites create cache copies of the entirety of Plaintiff's images in order to serve that image to their own end users. PGSD ¶¶ 17, 20, 22. However, this factor will not weigh against fair use if the "secondary user only copies as much as is necessary for his or her intended use." *Kelly*, 336 F.3d at 820-21. As a result, this factor does not weigh for, or against fair use given that the function to which the images were put required full replication.

iv. Effect of Use

This last factor requires the Court to consider not only the extent of market harm caused by the particular actions of the alleged infringer, but also whether unrestricted and wide-spread conduct of the sort engaged in by the alleged infringer would result in a substantially adverse impact on the potential market for the original. *Kelly*, 336 F.3d at 821. A transformative work is less likely to have an adverse impact on the market of the original than a work that merely supersedes the copyrighted work. *Id.* Here, as stated above, the third party websites do not transform the work of Plaintiff in any significant way. Rather, they seek to supplant the owner's use of the images by making them as available as possible to users within the United States. *See Rosen v. Masterpiece Mktg. Grp., LLC*, No. CV 15-06629 SJO, 2016 WL 7444688, *12-13 (no transformative use where display was inherently commercial). To allow the creation of cache copies on domestic servers would undoubtedly harm the market for Plaintiff's images because it would enhance the infringing sites' ability to reach users who would otherwise need to purchase access to the images from Plaintiff. Even absent evidence of a large scale market effect, this factor weighs against fair use because it would adversely impact the market for Plaintiff's images were it to be widespread. *Kelly*, 336 F.3d at 821; *see also MAPHIA*, 948 F. Supp. at 935-36 ("By downloading the games from the BBS, users avoid paying for the games…This conduct, if widespread, would adversely impact the market for Sega games.").

Further, the Supreme Court has made clear that the four factors discussed above are not meant to be exclusive. *Harper & Row*, 471 U.S. at 560; *see also Campbell*, 510 U.S. 577-78 ("The task is not to be simplified with bright-line rules, for the statute, like the doctrine it recognizes, calls for case-by-case analysis."). Here, additional facts, namely that the origin servers of the at-issue websites place them outside the reach of U.S. Copyright law should weigh against fair use. By signing up for Cloudflare, the third party infringers potentially cause copies

of their images to be created within the United States, in a manner not substantively different than if they were to rent domestic server space from which to deliver the images, conduct that would clearly be actionable domestic infringement. *See Amazon*, 508 F.3d at 1159 (discussing Ninth Circuit's server test); *see also Yandex*, 962 F. Supp. 2d at 1153 (finding Plaintiff's theory of liability based on presence of copyrighted images on defendant's U.S. servers plausible). While the caching technology employed by companies like Cloudflare may on the whole, be transforming the internet, the third party customers' use of such services to place copyrighted images closer to their own users appears to be nothing more than technological enhancement of their business of exploiting copyrighted images.

v. Balance of Factors

Because three of the four factors, as well as the additional consideration above weigh against fair use, the Court would find that the third parties' creation of cache copies using Cloudflare's CDN is not fair use.[15] As a result, Cloudflare may be secondarily liable for the infringement of the four third party sites identified above as well as a fifth site, cumonmy.com, whose host servers are located within the United States.

E. Whether Plaintiff's Display Rights Were Infringed Domestically

In moving for, and opposing summary judgment based on extraterritoriality neither party sufficiently differentiates between acts of duplication and display. For its part, Cloudflare argues that because the third party websites maintain foreign servers, that the *copying* (*i.e*. uploading of images to the host servers) occurred internationally. At the May 4, 2017 hearing the Court asked defense counsel if Plaintiff's display rights could potentially be violated - within the United States – when an end user in the U.S. accesses an image from a foreign server. *See* Transcript of May 4, 2017 Hearing at 4:6-5:15; 8:15-9:5. Defense counsel answered in the negative, claiming that because no copy is created or stored in the United States, no display occurs domestically either. *Id.* at 8:15-9:5. Upon review of the relevant Ninth Circuit authority the Court would disagree with Defendant's contention that the display right cannot be violated without a copy existing within the United States.

Amazon states the following in regards to display rights and online images:

> The computer owner shows a copy "by means of a . . . device or process" when the owner uses the computer to fill the computer screen with the

[15] The Court does not take a position on whether Cloudflare would be entitled to assert a fair use defense if Plaintiff were suing it here for direct infringement.

> photographic image stored on that computer, *or by communicating the stored image electronically to another person's computer*. In sum, based on the plain language of the statute, a person displays a photographic image by using a computer to fill a computer screen with a copy of the photographic image fixed in the computer's memory.

Amazon, 508 F.3d at 1160 (emphasis added). In so holding, the circuit court agreed with the district court that "a computer owner that stores an image as electronic information and serves that electronic information directly to the user…is displaying the electronic information in violation of a copyright holder's exclusive display right." *Id.* at 11-12.

Amazon is silent on the question of where, for extraterritoriality purposes, such display occurs. The only authority Cloudflare cites for its central proposition that infringing images on foreign servers cannot be actionable is *Yandex*, a district court case that read such a rule into the *Amazon* decision. Specifically, that court observed:

> The "server test" applied by our court of appeals makes the hosting website's computer, rather than the search engine's computer, the situs of direct copyright infringement liability. Therefore, [defendant] argues, these foreign-hosted images are extraterritorial and not actionable under the Act. This order agrees.

962 F.Supp.2d at 1153. Rather than grounding its holding in the language of *Amazon*, the *Yandex* court based its holding on: (1) its observation that the *Amazon* court did not address the issue of display of foreign images to U.S. viewers and (2) a general reference to the concept of territoriality:

> According to [plaintiff], when its images are hosted on servers located in Russia, [defendant] violates [plaintiff's] "exclusive display right" because users in the United States could download them….This theory of liability is rejected. Although [plaintiff] cites *Amazon* in support of its argument, nowhere in that decision did our court of appeals endorse the idea that display of a copyrighted image anywhere in the world creates direct copyright liability in the United States merely because the image could be downloaded from a server abroad by someone in the United States. Such a principle would destroy the concept of territoriality inherent in the Copyright Act for works on the internet.

Id. The *Yandex* court also noted that the plaintiff in that case failed to provide any evidence that any U.S. users actually viewed or downloaded the image in question. *Id.*

The Court disagrees with *Yandex's* application of *Amazon* to the display right in this manner. As stated above, and aptly noted by the *Yandex* court, *Amazon* does not address

extraterritoriality. *Id.* Further, *Amazon* plainly holds that the display right is infringed when "a computer owner shows a copy…by communicating the stored image electronically to another person's computer." *Amazon*, 508 F.3d at 1160. *Amazon* takes no position on the location of such a display for the purposes of extraterritoriality.[16] Finally, as discussed *supra*, several cases extend liability to acts of infringement that begin, or end in a foreign country that also take place, at least in part, in the United States. *See supra* at 11-14 (summarizing cases recognizing infringement for acts that do not occur entirely abroad, including *Reuters*, 149 F.3d 987; *Canning*, 809 F.Supp.2d 1139; and *Conus*, 969 F.Supp. 579). These cases, while factually distinct from both *Yandex* and the case at bar nonetheless appear at odds with the *Yandex* court's claim that recognizing liability for acts occurring on computer equipment on both sides of the border would destroy the concept of territoriality inherent in the Copyright Act.

Here, Plaintiff's images were displayed by the infringing websites to U.S. users. Plaintiff has arguably presented evidence that at least one image from 13 of the 14 sites at issue in the pending motion has been displayed on a computer within the United States. *See* Offer at 7:12-9:12 (showing chart containing results of Redbot.org, Hurl.it and HTML Header reports). As a result, the Court would deny without prejudice Defendant's Motion for Summary Judgment as to thirteen of the at-issue sites on the alternative grounds that it has failed to show, as a matter of settled law and undisputed fact that Plaintiff's display rights were not infringed within the United States. As stated above, the question of image-by-image summary adjudication was not fully briefed by either side and thus the Court would not grant summary adjudication on any specific images from these thirteen sites at this time.[17]

[16] At the May 25, 2017 hearing defense counsel directed the Court to footnote six in the *Amazon* decision. This note only makes clear that, in that case, the court was not addressing whether a passive bulletin board site violates display rights when copyrighted images are posted by users. *See Amazon*, 508 F.3d at 1117. Counsel then contended that two of the at-issue websites are only passive hosts of user generated images and thus do not display the images themselves. First, *Amazon* does not stand for this proposition directly, either in footnote six or elsewhere. Further, even if this were the law, the evidence Defendant cites consists solely of a declaration from the defense firm's paralegal who took screen shots of the infringing websites that show the sites allow for uploads by users. *See* Declaration of Nolan Schoichet ¶ 11, Docket No. 174-2. This, in and of itself, does not prove that any of the at-issues sites were only passive hosts of user-generated content. Finally, Defendant did not argue for summary judgment on the ground that the sites contain only user-generated images. Indeed, the evidence cited was not submitted until Defendant's Sur-Reply was filed. The Court will not choose to grant summary judgment on this theory, or any of the other alternative bases which Defendant has introduced after filing its opening brief.

[17] If Defendant believes it is entitled to summary judgment on an image-by-image basis it must move on such a ground.

IV. Conclusion

In sum, Cloudflare moved for summary judgment on the narrow theory that no direct infringement occurred within the United States. For the reasons stated above, it has failed to carry its burden to present settled law and undisputed facts proving as much. As a result, the Court would DENY Cloudflare's Motion as to the following thirteen sites: imgchili.com, slimpics.com, bestofsexpics.com, greenpics.com, imgspot.org, imgsen.se, imgspice.com, stooorage.com, img.yt, vipergirls.to, fboom.me, imgflash.net, and imgtrex.com. It would GRANT Defendant's Motion as to pornwire.net.[18]

V. Evidentiary Rulings

A. Cloudflare's Request for Evidentiary Rulings on Specified Objections − Docket No. 146

1. Sustained.
2. Sustained.
3. Sustained.
4. Overruled.
5. Sustained.
6. Sustained.
7. Sustained.
8. Sustained.

B. Cloudflare's Request for Evidentiary Ruling on Specified Objections − Docket No. 175

1. Sustained.
2. Overruled.
3. Overruled.
4. Overruled.
5. Overruled.

[18] Cumonmy.com has a domestic server and was thus not part of Cloudflare's Motion. Plaintiff's Offer of Proof indicates that it is not pursuing infringement claims based on pornwire.net. *See* Offer at 9.