

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
MIAMI DIVISION**

CASE NO.: 1:21-cv-20862-BB

MILLENNIUM FUNDING, INC., et al.,

Plaintiffs,

v.

1701 MANAGEMENT, LLC DBA
LIQUIDVPN, et al.,

Defendants.

**PLAINTIFFS' OPPOSITION TO DEFENDANT VPNETWORKS, LLC D/B/A
TORGUARD'S MOTION TO DISMISS
PLAINTIFFS' SECOND AMENDED COMPLAINT**

JOEL B. ROTHMAN
Florida Bar No. 98220
joel.rothman@sriplaw.com
CRAIG A. WIRTH
Florida Bar Number: 125322
craig.wirth@sriplaw.com
SRIPLAW
21301 Powerline Road, Suite 100
Boca Raton, FL 33433
561.404.4350 – Telephone
561.404.4353 – Facsimile

and

Kerry S. Culpepper
Admitted pro hac vice
CULPEPPER IP, LLLC
75-170 Hualalai Road, Suite B204
Kailua-Kona, HI 96740
808.464.4047 – Telephone
kculpepper@culpepperip.com
Attorney for Plaintiffs

SRIPLAW

CALIFORNIA ♦ GEORGIA ♦ FLORIDA ♦ TENNESSEE ♦ NEW YORK

Plaintiffs MILLENNIUM FUNDING, INC.; VOLTAGE HOLDINGS, LLC; AMBI DISTRIBUTION CORP.; AFTER II MOVIE, LLC; MORGAN CREEK PRODUCTIONS, INC.; MILLENNIUM FUNDING, INC.; BEDEVILED LLC; MILLENNIUM MEDIA, INC.; COLOSSAL MOVIE PRODUCTIONS, LLC; YAR PRODUCTIONS, INC.; FSMQ FILM, LLC; FW PRODUCTIONS, LLC; MILLENNIUM IP, INC.; I AM WRATH PRODUCTION, INC.; KILLING LINK DISTRIBUTION, LLC; BADHOUSE STUDIOS, LLC; LF2 PRODUCTIONS, INC.; LHF PRODUCTIONS, INC.; VENICE PI, LLC; RAMBO V PRODUCTIONS, INC.; RUPTURE CAL, INC.; MON, LLC; SPEED KILLS PRODUCTIONS, INC.; MILLENNIUM IP, INC.; NIKOLA PRODUCTIONS, INC.; WONDER ONE, LLC; BODYGUARD PRODUCTIONS, INC.; OUTPOST PRODUCTIONS, INC.; GLACIER FILMS 1, LLC; DEFINITION DELAWARE LLC; HANNIBAL CLASSICS INC.; JUSTICE EVERYWHERE PRODUCTIONS LLC; PARADOX STUDIOS, LLC; DALLAS BUYERS CLUB, LLC and SCREEN MEDIA VENTURES, LLC (“Plaintiffs”), by and through their counsel, file this opposition to the Motion to Dismiss [Doc. #14] the Second Amended Complaint (“SAC”) of Defendant VPNetworks, LLC d/b/a TorGuard (“Defendant”). For the reasons discussed below, Defendant’s Motion should be denied.

I. INTRODUCTION

Although sometimes couched in terms of privacy, Defendant promotes its Virtual Private Network (“VPN”) service for piracy, instructs its customers to use its VPN service for piracy, and heavily advertises that it destroys all evidence of its customer’s piracy¹. Defendant’s customers use its VPN service for piracy and Defendant destroys all evidence of its customer’s piracy just as promised.² And Defendant profits from its customer’s piracy³ without even bothering to conceal its piracy business plan – it even chose as its company name “TorGuard”, and states that the name refers to “...guarding one’s privacy when using [*sic*] bitorrent” – a protocol so overwhelmingly

1 “If you don’t have protective measures in place to secure your connection to the torrent cloud...The worst case scenario is...receive a subpoena from an attorney requesting your identity for a potential lawsuit...TorGuard offers...VPN service...protecting you from these risks. Our private VPN...can keep you completely safe when you use a BitTorrent client...[W]e don’t keep any logs...so there’s no trail leading back to you....” Exhibit “8”

2 Defendant’s affiliate, end user and avid defender “Travis” promotes Defendant’s service as an alternative to paying for streaming service from Disney and states he uses the website YTS frequently. *See* Decl. of Culpepper at ¶¶55-56.

3 Defendant boasted that its Canadian sales went up 100 percent after Canada implemented a rule requiring mandatory piracy notifications. *See* Decl. of Culpepper at ¶¶60-61.

used for piracy that a study showed that 96.28% of BitTorrent users sought infringing content. Defendant's advertisements are so over the top that legitimate companies such as PayPal and even other BitTorrent Client application providers want no part of doing business with it.⁴

Defendant attempts to portray its TorGuard as innocuous by comparing itself to the VPN definition in *VirnetX Inc. v. Mitel Networks Corp.*, No. 6:11-CV-18, 2012 U.S. Dist. LEXIS 107280 (E.D. Tex. Aug. 1, 2012) and inaccurately quoting the SAC⁵. However, encrypting customer communication as defined in *VirnetX* is starkly different from actively deleting customer log records to keep the end user's identity from being determined by "IP monitoring firms", "lawsuit happy lawyers" and the "ISP from sending [the end user] a harrowing letter" and promoting the service for breaking the geographic restrictions of legal platforms such as Hulu as done by Defendant.

In addition to destroying its end user log records, Defendant chooses host providers such as Digital Ocean and QuadraNet that do not publish reassigned Internet Protocol ("IP") addresses so it can conceal the IP addresses it uses and rightsholders cannot directly send it Notices of infringement.

But even if a rightsholder somehow identifies Defendant as the relevant party for an IP address where infringement has occurred, Defendant makes clear that it has specifically set up its network so that there is nothing it can do.⁶

Defendant's defense amounts to this –we know our end users pirate and that we are helping them do it but we cannot do anything about it and you cannot hold us liable because we have purposely set up our network to conceal and destroy the evidence.

II. BRIEF FACTUAL ALLEGATIONS

Plaintiffs own the copyrights for motion pictures ("Works") listed in Exhibit "1" to the SAC. *See* Exhibit "1" [Doc. #104-1] (errata). These Works are currently available for sale online and in brick-and-mortar retail stores. *See* SAC [Doc. #96] at ¶54.

⁴ PayPal stopped accepting payments from Defendant in 2019. BitTorrent, Inc. refused to allow Defendant to advertise in its client app unless Defendant changed its name and stopped promoting its service for piracy. *See* Decl. of Culpepper at ¶¶80-82.

⁵ Defendant inaccurately cites paragraphs 102-103 of the SAC for support for its assertion that "**Most** VPN providers...provided "anonymous" usage by...not logging subscriber access...". The relevant portion says "...**many** VPN providers..."

⁶ "Due to our no-log policy and shared IP network, we are unable to forward any [DMCA takedown notice] requests to a single user..." Decl. of Culpepper at ¶63.

To deal with massive piracy of their Works, Plaintiffs engaged Maverickeye UG (haftungsbeschränkt) (“MEU”) to monitor P2P/BitTorrent networks, capture evidence of acts of distribution of Plaintiffs’ Works, and generate infringement notices (“Notices”) to be sent to the service provider assigned the IP addresses where infringements of the Works was confirmed. *See Id.* at ¶¶201. Each Notice included at least the name of the copyright owner, the title of the Work, the manner by which it was infringed, the infringing file name which includes the altered copyright management information, the IP address and port number at where infringement was confirmed and the time of infringement down to the second. *See Id.* at ¶202.

MEU determines the proper abuse contact email address for the service provider assigned the IP addresses at issue from WHOis records of the American Registry for Internet Numbers Ltd (“ARIN”). QuadraNet failed to update the ARIN records to identify Defendant having been reassigned IP addresses. *See Id.* at ¶¶203 and 209. In comparison, other host providers such as CenturyLink require their subscribers to submit the proper documentation so that it can update the ARIN WHOis records to reflect proper identification. *See Decl. of Culpepper* at ¶8; www.centurylinkservices.net/faq.php [Doc. #117-7 at pg. 3].

Plaintiffs’ agent sent hundreds of Notices to QuadraNet concerning infringements of Plaintiffs’ Works at IP addresses QuadraNet reassigned to Defendant. For example, Plaintiffs’ agent sent over 50 Notices to QuadraNet concerning infringement of motion pictures such as *A Family Man*, *Hitman’s Bodyguard*, *Bedeviled*, *Hellboy* and *Angel Has Fallen* at IP address 96.44.142.226 reassigned by QuadraNet to Defendant. SAC at ¶¶208, 212.

QuadraNet’s CEO Ilan Mishan stated in his declaration that “Quadranet Enterprises, LLC’s system is semi-automated and forwards the abuse notification to the relevant customer.” Decl. of Mishan [Doc. #108-1] at ¶30; SAC at ¶464.

David Cox, the former owner of LiquidVPN, stated in his declaration that he received abuse notices from rightsholders that were forwarded to him by QuadraNet. *See Decl. of Cox* [Doc. #96-9] at ¶¶3-4; SAC at ¶290.

Upon information and belief, QuadraNet forwarded Plaintiffs’ Notices to TorGuard and other rightsholders had similar Notices sent to QuadraNet concerning infringing activity at IP addresses controlled by TorGuard that QuadraNet forwarded to TorGuard. *See Id.* at ¶¶208-209 and 212-214.

Defendant continued to provide the VPN service to its end users despite knowledge that its end users were using the service to pirate copyright protected Works including Plaintiffs' exactly as promoted, encouraged and instructed by Defendant. SAC at ¶223.

Defendant promotes its VPN service for piracy. Defendant operates its VPN service under the name "TorGuard" and advertises the service to "Torrent the Way You Want" and "...lets you use P2P activity the way you want to..." and tells its end users to "...plug VPN credentials into your favorite BitTorrent app to secure the app's outgoing traffic by hiding and replacing your IP..." SAC at ¶108.

BitTorrent is overwhelmingly used for piracy. *See* David Price, "NetNames Piracy Analysis: Sizing the Piracy Universe", September 2013, pg. 18, http://creativefuture.org/wp-content/uploads/2016/01/netnames-sizing_piracy_universe-FULLreport-sept2013.pdf [last accessed on Oct. 1, 2021] ("Of all unique visitors to bittorrent portals in January 2013, it is estimated that 96.28% sought infringing content during the month...")

Defendant warns its end users that when they use BitTorrent to pirate content that their IP addresses will be visible, and third parties can monitor their activity. Defendant tells its users that if they use its VPN service, their traffic will be tunneled through another server "so your ISP will not have any cause to send you a harrowing letter." SAC at ¶109.

Defendant recognizes that its end users are afraid to use BitTorrent to pirate Works due to the legal risks, but tells them that, "TorGuard shields all of your activities, including torrenting, from absolutely everyone. If no one can see what you're doing, you're free to do whatever you want. Stay safe and secure while torrenting by using TorGuard." *Id.* at ¶246.

Defendant knows and encourages its end users to use its VPN service to access notorious piracy torrent sites such as the "The Pirate Bay" to pirate content and provides technical help when its end users encounter difficulty pirating from torrent sites. *See Id.* at ¶¶152-154.

Defendant emphasizes that its VPN service is compatible with popular BitTorrent client apps so end users can "Stream your favorite content and download anonymously." *Id.* at ¶¶243-245.

Defendant instructs its end users how to setup their BitTorrent client with a special proxy link it provides to efficiently pirate content. *See Id.* at ¶262.

Defendant pays affiliates commissions for referring new customers and to promote its VPN service. *See Id.* at ¶¶247-250, 263.

Some of Defendant's affiliates promote TorGuard as "The Best VPN for Popcorn Time". Exhibit "3" and "4"⁷.

Defendant's end users install BitTorrent Client such as "Popcorn Time" onto their respective computer. See SAC at ¶139; see also Decl. of Culpepper at ¶64 (Defendant advising end user to help setup a script to "kill" Popcorn Time when the VPN goes down); see Id. at ¶54 (Defendant's affiliate Travis suggest Popcorn Time should be released with a built in VPN).

Defendant interferes with standard technical measures used by copyright holders to identify or protect copyright works by destroying the log data for their end users to conceal their piracy. See SAC at ¶¶257, 326. Defendant advertises its service as permitting its end users to "torrent as much as you want" because "No Logs Means No Records". See Id. at ¶257.

Defendant is motivated to become a subscriber of QuadraNet since it knows that QuadraNet will not make Defendant publish its own contact information in the Whois records for the IP addresses allocated to it. See Id. at ¶348.

MEU confirmed that Defendant used certain IP addresses reassigned to it from QuadraNet to distribute copies of the Works *I.T.*, *A Family Man*, *The Hitman's Bodyguard*, *Bedeviled*, *The Mechanic: Resurrection*, *The Humbling*, *211*, *I Feel Pretty*, *Hunter Killer*, *Hellboy*, *Angel Has Fallen*, *Rambo V: Last Blood*, *Boyka: Undisputed IV*, *Vengeance: A Love Story*, *Criminal*, *Once Upon a Time in Venice*, *I Am Wrath*, *London Has Fallen*, *Black Butterfly*, *Rupture*, *Day of the Dead*, *Extremely Wicked*, *Shockingly Evil and Vile*, and *Automata*. See Id. at ¶181.

III. BRIEF PROCEDURAL HISTORY

On Aug. 17, 2021, Plaintiffs filed the SAC [Doc. #96] seeking damages and injunctive relief against Defendant, among others, based upon claims for Direct Copyright Infringement (FIRST CLAIM), Contributory Copyright Infringement by Intentional Inducement (SECOND CLAIM), Contributory Copyright by Material Contribution Infringement (THIRD CLAIM) and vicarious infringement (FOURTH CLAIM).

On Sept. 24, 2021, Plaintiffs served a First Request for Production of Documents ("RPOD") on QuadraNet requesting identification information of the 245,706 IP addresses where

⁷ This Court can take judicial notice of this website and the other websites cited in this Motion as well as the screenshots in the declaration of Culpepper because they are publicly available documents. "The Court may take judicial notice of any fact that is not subject to reasonable dispute because it 'can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned.'" *Schink v. Comm'r of Soc. Sec.*, 935 F.3d 1245, 1258 (11th Cir. 2019) (quoting Fed. R. Evid. 201(b)(2)).

their Works were pirated. QuadraNet has objected and refused to disclose the identification information. *See* Decl. of Culpepper at ¶¶14-15.

On Oct. 8, 2021, Plaintiffs served a subpoena on non-party Digital Ocean requesting, *inter alia*, the IP addresses that Digital Ocean reassigned to Defendant. *See* Exhibit “1” [Doc. #143-1] to Defendant’s Notice of Hearing [Doc. #143].

On Oct. 18, 2021, Plaintiffs cross-noticed a hearing based upon Defendant’s refusal to preserve end user customer records and to provide initial disclosures. *See* Cross-Notice of Hearing [Doc. #146].

On Oct. 18, 2021, Defendant filed the present Motion.

IV. APPLICABLE LEGAL STANDARD

A pleading in a civil action must contain “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2). Although a complaint “does not need detailed factual allegations,” it must provide “more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555, 127 S. Ct. 1955, 167 L. Ed. 2d 929 (2007); *see Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S. Ct. 1937, 173 L. Ed. 2d 868 (2009). “To survive a motion to dismiss a complaint must contain sufficient factual matter, accepted as true, to ‘state a claim to relief that is plausible on its face.’” *Id.* (quoting *Twombly*, 550 U.S. at 570). A complaint should not be dismissed simply because the court is doubtful that the plaintiff will be able to prove all of the necessary factual allegations. *See Twombly*, 550 U.S. at 555. Accordingly, a well pleaded complaint will survive a motion to dismiss “even if it appears that a recovery is very remote and unlikely.” *Id.* at 556

When reviewing a motion under Rule 12(b)(6), a court, as a general rule, must accept the plaintiff’s allegations as true and evaluate all plausible inferences derived from those facts in favor of the plaintiff. *See Miccosukee Tribe of Indians of Fla. v. S. Everglades Restoration Alliance*, 304 F.3d 1076, 1084 (11th Cir. 2002); *AXA Equitable Life Ins. Co. v. Infinity Fin. Grp., LLC*, 608 F. Supp. 2d 1349, 1353 (S.D. Fla. 2009). Pleadings that “are no more than conclusions, are not entitled to the assumption of truth. While legal conclusions can provide the framework of a complaint, they must be supported by factual allegations.” *Iqbal*, 556 U.S. at 679. A Court considering a Rule 12(b)(6) motion is generally limited to the facts contained in the complaint and attached exhibits, including documents referred to in the complaint that are central to the claim. *See Wilchombe v. TeeVee Toons, Inc.*, 555 F.3d 949, 959 (11th Cir. 2009).

V. ARGUMENT - VENUE

A. Defendant has waived any arguments against venue in this District.

Defendant has waived arguments of improper venue by simultaneously making a motion to dismiss the SAC with prejudice unconditionally. *See Boulger v. Woods*, 306 F. Supp. 3d 985, 996 (S.D. Ohio 2018) (a Defendant that made motions to dismiss for lack of personal jurisdiction and service of process and then made a motion for judgment on the pleadings waived jurisdictional arguments because “by asking the Court to pass on the merits, [the defendant] voluntarily submitted to the jurisdiction of the Court”). Defendant first requests that this Court consider its Motion to dismiss the SAC as a “shotgun pleading”, then as a second alternative requests that the Court dismiss the SAC for failing to plead a claim for failure to claim, and then, as a third alternative requests a more definite statement, and finally as a fourth alternative (after the first three alternatives are considered) requests dismissal or transfer for improper venue. Thus, Defendant requests this Court fully consider the allegations of the SAC, and then consider venue only if this Court concludes that the SAC should fail. Defendant did not condition its first three request on whether this Court considered venue proper.

Moreover, Defendant has constructively consented to personal jurisdiction and thus venue in this Court by its extensive participation in these proceedings without any condition. “[T]he voluntary use of certain [district] court procedures” serve as “constructive consent to the personal jurisdiction of the [district] court.” *Ins. Corp. of Ireland, LTD v. Compagnie des Bauxite de Guinea*, 456 U.S. 694, 704 (1982). Besides filing the Motion to dismiss the SAC on its merits, Defendant has gone further in its case participation by agreeing to a mediation schedule (*see* Doc. #114) and filing a Motion to Quash [Doc. #141] a subpoena Plaintiff made to a third party without any condition on its appearance in any of these filings. Defendant’s actions demonstrate that it has sought to have this Court use its power to reach a decision on the merits, and requires the court to expend significant efforts in doing so. Accordingly, Defendant has participated in these proceedings to the extent that it has waived any arguments against venue.

B. Venue is appropriate because this Court has personal jurisdiction over Defendant.

28 U.S.C. §1400(a) provides that civil action relating to copyrights “may be instituted in the district in which the defendant or his agent resides or may be found.” §1391(b) provides that venue is appropriate in “a judicial district in which any defendant resides, if all defendants are residents of the State in which the district is located”. § 1391(c)(2) provides that “an entity...shall

be deemed to reside...in any judicial district in which such defendant is subject to the court's personal jurisdiction...".

Accordingly, based upon the definition of "reside" provided in § 1391(c)(2), under either §1391(b) or §1400(a) venue is appropriate where Defendant is subject to the court's personal jurisdiction. Defendant is a Florida limited liability company, and thus subject to personal jurisdiction in Florida. By the plain language of either venue statute, venue is appropriate in this District despite Defendant having its principal address in Orlando since this District is in Florida. Defendant cites *David Byrne & Index Music v. Crist*, No. 8:10-cv-1187-T-26MAP, 2010 U.S. Dist. LEXIS 162786, at *6 (M.D. Fla. Aug. 4, 2010) for the proposition that venue is only appropriate in the specific district where it could be served. However, *Byrne* and the Eleventh Circuit decision of *Palmer v. Braun*, 376 F.3d 1254, 1259 (11th Cir. 2004) on which *Byrne* relies both concerned the residence of *natural persons* such as Charlie Crist and Eldon Braun. Neither of these cases dealt with the explicit definition of "reside" for entities provided in § 1391(c)(2) in comparison to the definition of residence of a natural person in §1391(c)(1) which is limited to his/her domicile.

Nonetheless, venue is also appropriate in this District because Plaintiffs have pled that Defendant conducts business and has committed the tortious act of copyright infringement in this district. *See* SAC at ¶10. Defendant's CEO attempts to rebut this allegation by stating in his declaration that "TorGuard does not operate or conduct business in... Miami-Dade... (the "Southern District of Florida")". Decl. of Van Pelt [Doc. #145-3]. Mr. Van Pelt's declaration is contradicted by Defendant's multiple advertisements on its website that it maintains servers in Miami-Dade county (Miami) and has a location in Miami. *See* Decl. of Culpepper at ¶¶43-48. Because Plaintiffs have set forth evidence conclusively contradicting Mr. Van Pelt's declaration, the Court should credit Plaintiffs' evidence and construe all reasonable inferences in favor of Plaintiffs. *See Madara v. Hall*, 916 F.2d 1510, 1514 (11th Cir. 1990).

The Plaintiffs cannot determine the extent of the piracy of their Works at Defendant's servers in Miami because Defendant conceals from public records the IP addresses that are assigned to it. Indeed, concealing the IP addresses Defendant uses is a portion of its business strategy to prevent legal content streaming services such as Hulu and Netflix from blacklisting its IP addresses. *See* Decl. of Culpepper at ¶¶29-36, 40-42. The Defendant has even filed a motion to quash a subpoena Plaintiffs issued to one of its host providers requesting the IP addresses assigned to it by arguing that disclosure of the requested information may divulge its trade secrets.

See Notice [Doc. ##143, 147]. Nonetheless, Plaintiffs have alleged that Defendant solicits, transacts, or is doing business within this jurisdiction, and has committed unlawful and tortious acts both within and outside this jurisdiction with the full knowledge that its acts would cause injury in this jurisdiction. See SAC at ¶10. Thus, personal jurisdiction in this District is appropriate per Fla. Stat. § 48.193(1)(a)(1) and (2), and thus venue in this District is proper. Should this Court not be persuaded by Plaintiffs' allegations, Plaintiffs respectfully request the Court permit it to continue with discovery to ascertain Defendant's contacts with this District such as the IP addresses it uses in Miami and identification information of its end users.

VI. ARGUMENT – THE CLAIMS AGAINST DEFENDANT IN THE SAC ARE ADEQUATELY PLED

A. The SAC is not an impermissible “Shotgun Pleading”.

Defendant criticizes the SAC for being “almost 100 pages in length with more than 200 pages of exhibits...”, “vague and immaterial facts” and “a ramshackle compilation”. Mot. at pg. 3. However, in actuality what displeases Defendant is the inclusion of screenshots from its website showing exactly how it advertises its service for piracy and deletes end user's logs so they won't get caught. See e.g., SAC at ¶257. But despite Defendant's criticisms about the length, it turns around and argues that this Circuit's pleading standards require Plaintiffs to include even *more*. For example, Defendant argues that Plaintiffs need to allege “which specific Defendant infringed which specific Work” or “which Plaintiff holds rights to the allegedly infringed Work.” Mot. at pg. 4. However, Plaintiffs already allege in, for example, Count 1, that they “are the copyright owners of the Works which each contains an original work of authorship” and that Defendant “distributed and reproduced...Plaintiffs' copyright protected Works via networks under their control without authorization in violation... 17 U.S.C. §§ 106(1), 106(3) and 501” in paragraphs 373 and 378. Moreover, Exhibit “1” [Doc. #104-1] to the SAC sets forth specifically the entity that owns the Works and the relevant copyright registration number. In a case such as this where Plaintiffs' Works have been pirated on *hundreds of thousands* of IP addresses, it would require *volumes* to lay out the specific IP addresses and times where the Works were pirated. This is made even more difficult by Defendant's practice of concealing from the public which IP addresses have been reassigned to it from QuadraNet and other host providers. But this Court need not delve into this issue because this is not the level of pleading that is required. Rather, Rule 8 merely requires

“a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a)(2).

Defendant also argues that a separate count should be set forth for each Defendant by each Plaintiff even when Plaintiffs are asserting the same basis for relief against the Defendants. Mot. at pg. 4. Defendant’s ridiculous demand for a 144 count complaint (36 Plaintiffs x 4 Counts) is not required by Rule 8. Rule 8 merely requires that Plaintiffs provide Defendants fair notice of the claims against them. *See Exist, Inc. v. E.S.Y., Inc.*, No. 14-62429-CIV-BLOOM/VALLE, 2015 U.S. Dist. LEXIS 181144, at 12 (S.D. Fla. May 20, 2015) (finding that allegations that Defendant, an officer of the Defendant corporations, along with the Doe Defendants, contributed to a single category of unauthorized use of Plaintiff’s copyright and trademark provided Defendants with fair notice of the claims against them). Defendant has fair notice that Plaintiffs allege that it infringes their exclusive rights.

B. The SAC adequately pleads a claim for direct copyright infringement against Defendant.

Plaintiffs assert that they “are the copyright owners of the Works which each contains an original work of authorship”, that Defendant “distributed and reproduced...Plaintiffs’ copyright protected Works via networks under their control without authorization in violation of 17 U.S.C. §§ 106(1), 106(3) and 501, “encourage[s] end users to use the network to distribute and reproduce copies of Plaintiffs’ Works” and “interfere[s] with standard technical measures used by copyright holders to identify or protect copyright works by purposefully deleting...end users’ log information.” SAC at ¶¶373, 376-379

Defendant does not contest Plaintiffs’ allegation that it transmits, routes or provides connection for transmitting copies of Plaintiffs’ Works. Further, Defendant does not appear to dispute Plaintiffs’ allegation that it violates their exclusive right of distribution. Rather, Defendant incorrectly argues that Plaintiffs have failed to allege that “TorGuard **copied** original elements of the Works”. Mot. at pg. 6. However, Plaintiffs explicitly allege, for example, that Defendant “TorGuard...made **copies** of copyright protected Works to others on said network...” SAC at ¶376 (emphasis added).

Defendant further argues that “there is no volitional conduct by TorGuard related to the alleged infringement of the Works.” Mot. at pg. 6. However, Plaintiffs’ plausible allegations of Defendant’s involvement with its end users’ piracy amount to significantly greater than “merely

passively providing the means to transmit, route or provide connections for the piracy.”⁸ Mot. at pg. 7. First, Plaintiffs allege that Defendant deletes its end users’ log information so that they cannot be tied to the piracy in violation of the prohibition against interference with standard technical measures provided by 17 U.S.C. § 512(i)(1)(B). Second, Plaintiffs allege that Defendant provides a special proxy link and instructs its end users how to set up their BitTorrent client to include the special proxy link to efficiently pirate content. *See* SAC at ¶262. Third, Plaintiffs allege that Defendant helps its end users access pirated content from notorious piracy sources such as The Pirate Bay. *Id.* at ¶154.

In the context of the public performance right, the Supreme Court’s decision in *ABC, Inc. v. Aereo, Inc.*, 573 U.S. 431, 134 S. Ct. 2498 (2014) is instructive of the very limited amount of “volition or causation” necessary for direct infringement. The Defendant in *Aereo* sold a service that allowed its subscribers to watch television programs over the Internet at about the same time as the programs were broadcast over the air. *See Id.* at 431. The Supreme Court concluded that “when Aereo merely supplies equipment that allows others [to transmit copyright works,] the Act is unmistakable: An entity that engages in activities like Aereo’s performs.” *Id.* at 438-439. In grappling with a similar issue, the DC Circuit similarly concluded that *Aereo* “forecloses [Defendant’s] argument that the automated nature of its video-on-demand system or the end users’ role in selecting which content to access insulates it from Copyright Act liability.” *Spanski Enterprises v. Telewizja Polska*, 883 F.3d 904, 911 (D.C. Cir. 2018).

The facts alleged against Defendant in the SAC are even worse than in *Aereo* and *Spanski* because Defendant: (1) deletes log records so its end users can pirate without fear (*see* SAC at ¶¶257, 326); (2) instructs their end users exactly how to set up their BitTorrent client to efficiently pirate content using a specially provided proxy link (*see Id.* at ¶262); and (3) helps their customers access notorious torrent websites such as The Pirate Bay to pirate content [*see Id.* at ¶¶153-154 (Defendant’s administrator advises end user trying to access piracy website that is blocked by a Court order to try using TorGuard’s alternative DNS)]. Defendant tries to brush its atrocious behavior aside by stating “it is not in the business of online censorship” and arguing that “the asker did not state their purpose for accessing [The Pirate Bay] or identify the specific materials they sought

⁸ Defendant’s assertion that Plaintiffs are trying to claim that TorGuard copies the Works...to Does 1-100 is nonsensical. DOES 1-100 are alleged to be subscribers of QuadraNet and likely other service providers rather than end users of TorGuard. *See* SAC at ¶101.

access”. Mot. at pgs. 16 and 21. However, Defendant does not even bother concealing that their motive for deleting end users’ logs is to defeat standard measures used by rightsholders to track infringements. *See Id.* at ¶¶109, 226, 244, 246, 257; Decl. of Culpepper at ¶¶68-69 (Defendant states, “If no one can see what you’re doing, you’re free to do whatever you want” and promotes it service for preventing receiving “a subpoena from an attorney requesting your identify for a potential lawsuit”).

Simply put, Defendant tells its end users how to pirate with its service, assists them in pirating, and destroys the evidence. Solely Defendant’s action of destroying the end user’s log records so that its end users cannot be tied to the piracy is sufficient volitional conduct. Defendant cannot now argue that there is no evidence of its volitional conduct because it destroyed the evidence.

Defendant incorrectly argues Plaintiff is alleging that the same conduct is evidence of both direct and secondary liability and – without citation to any legal precedent – state that “it is axiomatic that what is contributory or vicarious infringement cannot also be direct infringement.” Mot. at pg. 6. 17 U.S.C. § 106 grants Plaintiffs exclusive rights besides reproduction such as the distribution and public performance. Defendant is secondarily liable for its end users’ violations of Plaintiffs’ exclusive right to publicly perform (stream) or distribute Plaintiffs’ works because, for example, it provides its end users IP addresses at servers outside of their geographic region and explicitly encourages them to use them to access Netflix, Amazon Prime and Hulu for streaming or downloading Plaintiffs’ Works in violation of the geographical restrictions. Defendant is secondarily liable for its end users’ violation of Plaintiffs’ exclusive right of distribution by, for example, connecting its end users to sources (such as the BitTorrent swarm) to obtain an infringing copy of their Works and deletes log records. Defendant directly infringes Plaintiffs’ exclusive rights of distribution and reproduction when, for example, it distributes copies of their Works (to the BitTorrent swarm) after the copy is obtained and deletes log records.

C. The SAC adequately pleads a claim for contributory infringement based upon intentional inducement against Defendant.

As stated by the Supreme Court, “one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties.” *MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 936-37, 125 S. Ct. 2764, 2780 (2005). The intentional inducement

standard of *Grokster* has been extended from products to services. See *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1037; *Disney Enters. v. Hotfile Corp.*, No. 11-20427-CIV-WILLIAMS, 2013 U.S. Dist. LEXIS 172339, at *113 (S.D. Fla. Aug. 28, 2013) (“a defendant will be liable for actually expressing an intention to foster infringement...”).

Defendant argues that it cannot be held liable for inducement because Plaintiffs did not send the Notices to its registered DMCA agent. Mot. at pg. 9. However, specific knowledge is not an element of intentional inducement. As explained by the Ninth Circuit in *Fung*, “...if one provides a service that could be used to infringe copyrights, with the manifest intent that the service actually be used in that manner, that person is liable for the infringement that occurs through the use of the service.” *Id.* at 1037. The Ninth Circuit went on to point out the potential devastating consequences to those liable for inducement.

We are mindful, however, of the potential severity of a loose causation theory for inducement liability. Under this theory of liability, the only causation requirement is that the product or service at issue was used to infringe the plaintiff's copyrights. The possible reach of liability is enormous, particularly in the digital age.

Id.

To deal with this “potential severity”, *Fung* discussed how an entity could “rehabilitate” itself so as not to “infinitely expand its liability in either temporal direction” by methods such as “actions actively discouraging the infringing use of their product...” *Id.* at 1038.

Plaintiffs have sufficiently alleged Defendant’s culpable expression and conduct by providing screenshots of Defendant’s advertisement of its service as “lets you use P2P activity the way you want”, “stream content and download anonymously”, “your ISP will not have any cause to send you a harrowing letter,” and pointing out how its affiliates promote TorGuard for piracy. SAC at ¶¶107-109, 247-250; see also Exhibits “3” and “4” (affiliates promoting TorGuard for using PopcornTime). Defendant’s argument that “there is no evidence that TorGuard...endorsed or approved the statements...” on pg. 12 is unavailing because Plaintiffs allege that Defendant pays the affiliates for referrals. Defendant cannot disavow the promotions of its service for piracy by the affiliates that it considers as “the backbone of [it’s] marketing team” and pays a bounty of “30% recurring lifetime commission for any and all sales”. Exhibit “7”. Defendant’s assertion that “it explicitly directs its affiliates not to promote piracy and has a strict termination policy for affiliates who violate its requirements” on pg. 18 is also unavailing because Defendant has failed

to provide *any* evidentiary support (not even a declaration) let alone publicly available documents in support of this assertion. Defendant's assertion is also contradicted by its affiliates' promotion of TorGuard as the Best VPN for Popcorn Time and Defendant's statement that "TorGuard cannot remove or censor our affiliate's YouTube videos or blogs under any circumstance." Decl. of Culpepper at ¶37; *see* Exhibits "3" and "4". Because the SAC includes sufficient supported allegations of culpable expression and conduct that are "plausible on its face", Plaintiffs should be permitted to proceed to discovery to obtain further evidence of Defendant's culpable expression and conduct and agency relationship between Defendant and its affiliates.

Assuming *arguendo* that intentional inducement requires specific knowledge, Defendant's argument still fails. First, this assertion relies on the declaration of Mr. Losey that he did not receive the notices, and thus non-public information outside of the pleadings that should not be considered. Moreover, if Defendant agreed to receive the notices from QuadraNet at a different contact from that of Losey PLLC, it cannot now turn around and argue that it does not have knowledge if the Notices were sent by QuadraNet to the very email address Defendant explicitly agreed to receive them. For example, §8(h) of QuadraNet's publicly available terms of service states that "It is client's responsibility to promptly notify...of any change in email address or contact person(s)" and the data breach policy states that it "...commits to a notification via email to...the primary business contact registered upon contract signing." Decl. of Culpepper at ¶¶25-27; <https://www.quadranet.com/terms-of-service> [last accessed on 10/26/2021].

Further, the declaration of Mr. Losey states that Losey PLLC has been TorGuard's DMCA agent "since at least 2018" and that Defendant has had a DMCA policy since sometime in "2018". Decl. of Losey [Doc. #145-1] at ¶¶8-9. However, the DMCA records show that Defendant *did not even have a registered DMCA agent* prior to Nov. 23, 2018. *See* Decl. of Culpepper at ¶¶23-24; Exhibit "1". The effective date of the SAC is March 3, 2018. *See* Fed. R. Civ. Pro 15(c). Plaintiffs should be able proceed to discovery to obtain evidence on the important issue of whether Defendant had a policy prior to Nov. 23, 2018 because, according to QuadraNet, Defendant "has been Quadranet's client since June 28, 2012". *See* Exhibit "3". It should be noted that the discovery rule permits Plaintiffs to proceed against Defendant for infringements prior to the three year statute of limitations of 17 U.S.C. § 507(b). *See Petrella v. Metro-Goldwyn-Mayer, Inc.*, 572 U.S. 663, 670 n.4, 134 S. Ct. 1962, 188 L. Ed. 2d 979 (2014); *see also Media Rights Techs., Inc. v. Microsoft Corp.*, 922 F.3d 1014, 1022-24 (9th Cir. 2019).

Second, Plaintiffs allege that they cannot send the Notices directly to Defendant because QuadraNet does not update the ARIN WHOis records to identify Defendant for the IP addresses QuadraNet reassigned to Defendant. QuadraNet’s CEO has stated in a declaration that QuadraNet forwards the Notices to its subscribers. Plaintiffs were only able to link certain IP addresses of QuadraNet to Defendant because QuadraNet provided that information in response to a subpoena. *See Decl. of Culpepper at ¶¶ 11-12, 20; Exhibits “3” and “9”.*

Third, Defendant arguments concerning Notices pertain to whether it has a safe harbor from financial liability, not whether it is liable. Particularly, 17 U.S.C. §512(c)(3)(B)(i) states that “a notification from a copyright owner...that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (I)(A).” However, §512(c)(1)(A) provides:

A...provider shall not be liable for monetary relief, or, *except as provided in subsection (j)*...for infringement of copyright by reason of the storage at the direction of a user of material that resides on a...network controlled...by the service provider, if the service provider (i) does not have actual knowledge that the material ...on the...network is infringing...

Even if Defendant established a safe harbor based upon defective notices, it can still be liable for the injunctive relief provided in §512(j)(1)(B)(ii) and ordered to block access to notorious foreign piracy websites such as The Pirate Bay that Defendant steadfastly refuses to do. Moreover, because Defendant asserts that it is a registered *transitory* digital network communications service provider, §512(c) is not applicable. Mot. at pg. 2 (“TorGuard is also a registered transitory digital network communications service provider...”).

Fourth, Plaintiffs also allege that Defendant distributes and contributes to distribution and public performance of unauthorized copies of Plaintiffs’ Works. *See SAC at ¶¶384, 418.* However, the provision of §512(c)(3)(B)(i) pertain to “storage of material”, not distribution and public performance.

Fifth, Defendant is incorrect in its assertion that Notices would need to be sent to its DMCA agent for it to need to terminate “subscribers and account holders of the service provider’s system or network who are repeat infringers” as called for §512(i)(1)(A). Defendant conflates the requirements for the §512(c)(3)(B)(i) notice scheme with the §512(i) requirements for eligibility of any of the safe harbors. Moreover, Defendant fails to address the fact that it interferes with standard technical measures in violation of §512(i)(1)(B) by destroying its customer’s log records.

D. The SAC adequately pleads a claim for contributory infringement based upon material contribution against Defendant.

Contributory copyright infringement occurs where a party with knowledge of infringing activity materially contributes to the infringing conduct of another. *See Cable/Home Commc'n Corp. v. Network Prods., Inc.*, 902 F.2d 829, 845 (11th Cir. 1990); *Casella v. Morris*, 820 F.2d 362, 365 (11th Cir. 1987); *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971).

Defendant materially contributes to infringement of Plaintiffs' Works by providing the VPN service its end users use to infringe Plaintiffs' exclusive rights of their Works despite having actual knowledge of their end users' piracy from the notices forwarded to it from QuadraNet and its other host providers. *See* SAC at ¶¶213, 396. "[A]ctual knowledge is not required. All that must be shown [for contributory infringement] is that [defendant] had reason to know" of the infringing activity. *See Cable/Home*, 902 F.2d at 846 (citing *Casella v. Morris*, 820 F.2d 362, 365 (11th Cir. 1987)).

Defendant asserts that Plaintiffs' claim based upon material contribution must fail because its service is capable of a substantial non-infringing use. Mot. at pg. 13. However, BitTorrent, from which Defendant's service TorGuard gets its name, is overwhelmingly (by some measures 96.28% percent of its traffic) used for piracy. *See* David Price, "NetNames Piracy Analysis: Sizing the Piracy Universe", September 2013, pg. 18. Moreover, Defendant's assertion (without any citation) that its VPN service "is also predominantly used and marketed for such noninfringing use..." improperly relies on non-public documents outside of the pleadings. Mot. at pg. 14. In the contrary, Defendant publicly states that its service can be used to avoid lawsuits, letters from an ISP and to break geographic restrictions of Hulu, Netflix and Amazon Prime. *See* Decl. of Culpepper at ¶¶29-34 and 41-42; Exhibits "5"- "6"

Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984) does not absolve Defendant from liability because Defendant has knowledge that its end users are using TorGuard to pirate copyright protected content via BitTorrent and, even now, steadfastly fails to take even the simplest measures to stop further piracy. In *Sony*, the Defendant sold a *product* (the VCR) to customers without specific notice that its customer was going to use the *product* to pirate content. Sony could not take any simple measures to stop piracy once the customer had purchased the product. In comparison, Defendant sells an ongoing *service* to its end users and has *specific notice*

that these end users are using the services to distribute copies of Plaintiffs' Works without authorization yet purposely chooses to do absolutely nothing while continuing to provide the service. Even worse, Defendant continues to delete the log records which provide evidence of the piracy even after being served with this lawsuit. In instances such as here where Defendant has knowledge of the specific infringing activity yet fails to take simple measures stop it, traditional common law principles permit a court to impute intent so that defendant may be liable, by operation of law just as if it had actually intended to infringe. *See Disney Enters. v. Hotfile Corp.*, No. 11-20427-CIV-WILLIAMS, 2013 U.S. Dist. LEXIS 172339, at 113 (S.D. Fla. Aug. 28, 2013).

Defendant's proposition that a service provider with knowledge of ongoing infringement by its subscribers can escape liability by merely asserting that its service has substantial non-infringing uses has been repeatedly rejected. The Fourth Circuit called this argument "meritless" when pointing out that the Supreme Court clarified in *Grokster* that "*Sony* barred secondary liability based on *presuming or imputing intent* to cause infringement solely from the design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement...the fact that a product is "capable of substantial lawful use" does not mean the "producer can never be held contributorily liable." *BMG Rights Mgmt. (US) LLC v. Cox Communs., Inc.*, 881 F.3d 293, 306 (4th Cir. 2018); *Umg Recordings, Inc. v. Grande Communs. Networks, LLC*, 384 F. Supp. 3d 743, 767 (W.D. Tex. 2019) ("liability may be imposed for intentionally encouraging infringement through specific acts...The specific act in question here is the continued provision of internet services to customers. Thus, this is not a case of mere refusal to act. Grande acted affirmatively by continuing to sell internet services and continuing to provide internet access to infringing customers."); *UMG Recordings, Inc. v. RCN Telecom Servs., LLC*, Civil Action No. 19-17272 (MAS) (ZQN), 2020 U.S. Dist. LEXIS 158269, at *31 (D.N.J. Aug. 31, 2020) (rejecting RCN's argument that material contribution to infringement is precluded by the *Sony* Rule because its internet service has substantial non-infringing uses). Courts have sustained pleadings of contributory infringement against residential service providers such as Cox, RCN and Charter that merely provide the Internet connection and a modem liable for contributory copyright infringement for their subscriber's piracy. *Supra*. While these residential providers had lax policies for terminating subscribers, Defendant goes further and deletes log records of its customer access. *See SAC* at ¶¶257, 326. Because Defendant deletes the log records, it is impossible for it to reasonably implement a policy for terminating its end users who use the service

for piracy as required. A defendant who disables itself from doing anything to prevent infringement does not reasonably implement a repeat infringer policy. *See In re Aimster Copyright Litig.*, 334 F.3d 643, 655 (7th Cir. 2003) (“Far from doing anything to discourage repeat infringers of the plaintiffs’ copyrights, Aimster invited them to do so, showed them how they could do so with ease using its system, and by teaching its users how to encrypt their unlawful distribution of copyrighted materials disabled itself from doing anything to prevent infringement”).

Defendant’s reliance on the unpublished decision of *Hydentra v. Luchian* to support its widely rejected proposition is misplaced because the Defendant in this case argued it never actually received the notices. *See Hydentra HLP Int. Ltd. v. Luchian*, No. 1:15-cv-22134-UU, 2016 U.S. Dist. LEXIS 193457, at *53 (S.D. Fla. June 2, 2016) (“SSM claims that it never received these takedown notices and was unaware of the allegedly infringing files until this lawsuit”). Here, Plaintiffs allege that QuadraNet and other host providers forwarded notices to Defendant. *See SAC* at ¶¶213, 396. Recognizing the weakness in its argument, Defendant attempts to improperly introduce evidence outside the pleadings that its DMCA agent never received the notices.⁹ *See Mot.* at pgs. 2. However, as discussed above, this argument fails. Moreover, as argued above, Plaintiffs should be permitted to proceed to discovery to determine if Defendant actually received the Notices.

E. The SAC Sufficiently Pleads a Claim for Vicarious Copyright Liability.

“One...infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it.” *MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. at 930. In order to state a claim for vicarious copyright infringement, a plaintiff must allege (1) “the right and ability to supervise,” and (2) “a direct financial interest” in the profits of the infringing activity. *See Affordable Aerial Photography, Inc. v. Modern Living Real Estate, LLC*, No. 19-cv-80488-BLOOM/Reinhart, 2019 U.S. Dist. LEXIS 132023, at *7-8 (S.D. Fla. Aug. 6, 2019) (citing *Klein & Heuchan, Inc. v. Costar Realty Info., Inc.*, 707 F. Supp. 2d 1287, 1297 (M.D. Fla. 2010)

Defendant contends that they do not have the right and ability to supervise the infringing activity or the obligation to terminate their user accounts “without specific knowledge and notice of infringement”. *Mot.* at pg. 16. Here, again Defendant does not argue that it did not receive

⁹ Plaintiffs reserve their right to move to disqualify Losey PLLC as counsel since according to the declaration of Mr. Losey, his firm is Defendant’s registered DMCA agent and receives notices of infringement on behalf of Defendant. Thus, Losey PLLC and Mr. Losey will be important witnesses in this action.

notices from QuadraNet, only that merely because QuadraNet did not forward the notices to its DMCA agent rather than to it, it does not have the requisite knowledge. As discussed above, this argument improperly relies on documents outside of the pleadings and is based on a conflation of the necessary elements of establishing a safe harbor defense from liability for infringing material residing on servers from actions of third parties. Defendant does not dispute Plaintiffs' allegation that it can control its users' alleged infringements by simple measures such as null-routing end users, logging their end users' access and blocking access to notorious piracy websites such as The Pirate Bay, it merely states that it does not want to do it. Mot. at pg. 16 ("...TorGuard is not in the business of online censorship...").

Plaintiffs also allege that Defendant at all relevant times have derived a direct financial benefit from the infringement of Plaintiffs' copyrights. Id at. ¶414. Defendant directly profit from its end users' reproduction, distribution and public performance of Plaintiffs' copyright protected Works without authorization because end users are motivated to become customers of Defendant so that they can use TorGuard to pirate without getting caught. Defendant argues that it "does not promote or endorse piracy". Mot. at pg. 17. However, Defendant clearly states its objective when it warns potential customers that they should use its service to keep their log information for illegal downloads from being released by the ISP in piracy lawsuits to lawsuit happy lawyers. See Exhibits "5" and "6". Moreover, Defendant explicitly promotes its service to end users that wish to break the geographic restrictions of legal platforms such as Netflix, Amazon Prime and Hulu to consume content from unauthorized regions. See Decl. of Culpepper at ¶¶29-34 and 41-42. Piracy is clearly the main draw of TorGuard.

F. Defendant's request for a more definite statement should be denied

The SAC clearly states that Defendant infringes and contributes to infringements in Plaintiffs' exclusive rights to their Works. Accordingly, no "more definite" statement is needed. Plaintiffs can provide Defendant with the "when" after obtaining from QuadraNet and Defendant's other host providers or from Defendant through discovery the IP addresses that were reassigned to it. See *Valentin v. J & T Management Inc.*, No. 14-cv-62087, 2014 U.S. Dist. LEXIS 163059, 2014 WL 6610941, at *2 (S.D. Fla. Nov. 20, 2014) (quoting *Hernandez v. Two Brothers Farm, LLC*, 579 F. Supp. 2d 1379, 1382 (S.D. Fla. 2008) ("Defendants may not use a motion for more definite statement as a means of discovery regarding those claims.")). It should be noted that Defendant is actively hindering Plaintiff from obtaining this information.

VII. CONCLUSION

Defendant's Motion should be denied because the SAC asserts ample facts supporting Plaintiffs' claims and venue in this district is proper. If the Defendant's 12(b)(6) Motion is granted, Plaintiff respectfully requests leave to amend the SAC. Further, should the Court be inclined to grant Defendant's 12(b)(2)(3) Motion, Plaintiffs respectfully request limited discovery to ascertain Defendant's contacts with the Southern District of Florida.

Dated: October 27, 2021

Respectfully submitted,

/s/ Joel B. Rothman

JOEL B. ROTHMAN

Florida Bar No. 98220

joel.rothman@sriplaw.com

CRAIG A. WIRTH

Florida Bar Number: 125322

craig.wirth@sriplaw.com

SRIPLAW

21301 Powerline Road, Suite 100

Boca Raton, FL 33433

561.404.4350 – Telephone

561.404.4353 – Facsimile

and

Kerry S. Culpepper

Admitted pro hac vice

CULPEPPER IP, LLC

75-170 Hualalai Road, Suite B204

Kailua-Kona, HI 96740

808.464.4047 – Telephone

kculpepper@culpepperip.com

Attorney for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on October 27, 2021, the foregoing document was electronically filed with the Clerk of the Court using CM/ECF. I also certify that the foregoing document is being served on this day on all those identified on the Service List, either via transmission of Notices of Electronic Filing generated by CM/ECF or in some other authorized manner for those parties who are not authorized to receive Notices of Electronic Filing.

s/ Joel B. Rothman
JOEL B. ROTHMAN
Florida Bar Number: 98220
joel.rothman@sriplaw.com

SERVICE LIST

Mr. Johnathan R. Woodard
Mr. John Cyril Malloy III
Mr. Oliver Alan Ruiz
Malloy & Malloy, PL
2800 SW 3rd Ave
Miami, FL 33129-2317
info@malloylaw.com
jwoodard@malloylaw.com
jcmalloy@malloylaw.com
oruiz@malloylaw.com
Attorneys for QuadraNet, Inc. and QuadraNet
Enterprises, LLC

Mr. Bobby A. Ghajar
Cooley LLP
1333 Second Street
Suite 400
Santa Monica, CA 90401
bghajar@cooley.com
Attorneys for QuadraNet, Inc. and QuadraNet
Enterprises, LLC

Mr. Adam Losey
Losey PLLC
1420 Edgewater Drive
Orlando, FL 32804
alosey@losey.law
Attorney for VPNetworks, LLC dba
TorGuard

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

Case No.: 21-cv-20862-BLOOM/Otazo-Reyes

MILLENNIUM FUNDING, INC. et al,

Plaintiffs,

vs.

1701 MANAGEMENT LLC et al,

Defendants.

DECLARATION OF KERRY S. CULPEPPER

KERRY S. CULPEPPER, hereby declares under penalty of law that the following is true and correct:

1. I am an attorney and represent the Plaintiffs, I have personal knowledge of the matters stated herein, and this declaration is given in support of Plaintiffs' Opposition to the Motion [Doc. #145] to Dismiss the Second Amended Complaint ("SAC") of Defendant VPNetworks, LLC d/b/a TorGuard ("Defendant").

2. I specialize in intellectual property, particularly electrical and computer software technology. I have a Bachelor of Civil Engineering degree from Georgia Institute of Technology and a Master of Science in Electrical Engineering degree from George Mason University.

**IP address reassignments/reallocations between host providers to subscribers and
publication of reassignments/reallocations.**

3. To receive Internet Protocol ("IP") addresses from the American Registry of Internet Numbers, Ltd ("ARIN"), host providers are required to agree to a registration Agreement and to be bound by ARIN's Number Resource Policy Manual ("Policy").

4. Per paragraph 3(b) of the Registration Agreement, members such as host providers are responsible for updating the directory services data (Whois) to indicate who they have sub-delegated number resources.

5. ARIN provides two options for customer to report their reallocation/reassignment data: Referral Whois (RWhois) or the Shared Whois Project (SWIP). *See* <https://www.arin.net/resources/registry/reassignments/> [last accessed on 10/26/2021](partial screenshot below).

Options

ARIN customers have two options when it comes to reporting their reallocation/reassignment data. They can use Referral Whois (RWhois) or the Shared Whois Project (SWIP).

RWhois

RWhois is an extension of the original Whois protocol and service. It focuses on the distribution of data representing networks and POCs, and uses the inherently hierarchical nature of these network objects (domain names, IP networks, email addresses) to more accurately discover the requested information. RWhois allows organizations to advertise their reallocation/reassignment from an internal server, rather than actively sending it to ARIN. There are numerous requirements for using this sort of distribution server for reallocation/reassignment information, including 24 / 7 server functionality, response qualification, and continuity of data. For details, see [Section 3.2 of ARIN's Number Resource Policy Manual \(NRPM\)](#). More information about this method is available on the [Referral Whois \(RWhois\) page](#).

SWIP

SWIP is a process whereby ARIN customers report reallocation/reassignment data using one of the following methods:

- **ARIN Online:** ARIN Online provides a graphical user interface to ARIN's registration database.
- **Reg-RWS:** Registration Representational State Transfer (REST)ful Web Service (Reg-RWS) provides a secure and efficient method for interacting with ARIN's database. Reg-RWS is most handy for repetitive, mundane tasks done in high volume with no needed human communication, such as SWIP. In addition to being more secure than email templates, Reg-RWS allows for the retrieval of information about a record immediately before submitting changes to it. Reg-RWS also returns a predictable response that can be interpreted and reacted to by automation software.

6.

7. Some host providers such as Hurricane Electric provide a publicly accessible database to determine the identities of the subscribers to which it reassigned IP addresses. *See* <https://bgp.he.net/> [last accessed on 10/26/2021].

8. Some host providers such as Century Link require their subscribers to submit a SWIP documentation including their identification information so that they can update the ARIN Whois records to properly identify that subscriber as having been reassigned the IP addresses. *See* www.centurylinkservices.net/faq.php [Doc. #117-7 at pg. 3] (“CenturyLink will submit the proper Shared WhoIs Project (SWIP) documentation based on information provided by the IP Services subscriber...Once a SWIP registration is submitted the ORG ID becomes the responsibility of the IP Services subscriber...SWIP submissions can be viewed in ARIN’s WhoIs database.”)

9. For host providers such as QuadraNet that do not update the ARIN WHOis records to indicate the VPN providers to which they have reassigned IP addresses or provide a public directory, there is no practical way to determine all the IP addresses that are assigned to Defendant except from obtaining this information directly from the host provider.

10. Without citing to any publicly available document, Defendant states, “...the technical realities of the ARIN which make it impossible for TorGuard to be the abuse contact for the registered IP address...” Mot. at pg. 9. As shown in above screenshot, ARIN provides tools for reassignments to be updated and even helpful templates to use. *See, e.g.*, Template: ARIN-NET-MOD-5.2, <https://www.arin.net/resources/templates/netmod.txt> [last accessed on 10/26/2021]. Accordingly, Defendant’s bald assertion is untrue.

11. I represented the Plaintiffs in the Civil Action 1:19-cv-169-LEK-KJM in the District of Hawaii. Exhibit “2” is a true and accurate redacted response I received from QuadraNet in response to a subpoena for the subscriber identification records for certain IP addresses in which QuadraNet stated that these IP addresses were reassigned to Defendant. I was able to determine that Defendant was assigned these IP addresses from this response.

12. I represented the Plaintiffs in the Misc. Action 1:19-cv-257-LEK-KJM in the District of Hawaii. Exhibit “9” is a true and accurate redacted response I received from QuadraNet in response to a subpoena for the subscriber identification records for certain IP addresses in which QuadraNet stated that these IP addresses were reassigned to Noisebridge. I was able to determine that Noisebridge was assigned these IP addresses from this response.

13. Because Plaintiffs can only confirm that an IP address where their Works are being infringed is Defendant’s until after serving a subpoena on the host provider publicly tied to the IP address in the ARIN WhoIS records, Defendant’s assertion (Mot. at pg. 9) that Plaintiffs should have sent the DMCA notices directly to TorGuard is not grounded in practical reality.

14. On Sept. 24, 2021, I served a First Request for Production of Documents (“RPOD”) on QuadraNet on behalf of Plaintiffs requesting *inter alia* identification information of the 245,706 IP addresses where their Works were pirated.

15. On Oct. 25, 2021, I received objections from QuadraNet in which they refused to provide the identification information.

16. On Oct. 8, 2021, I served a third-party subpoena on Digital Ocean requesting records of the IP addresses that were assigned to Defendant and all communications with Defendant from 2016.

17. On Oct. 12, 2021, Defendant filed a motion to quash the third-party subpoena. Defendant's motion has been noticed for a hearing on Nov. 1, 2021. *See* Notice [Doc. #143].

18. On Oct. 21, 2021, I served an amended third-party subpoena on Digital Ocean requesting *inter alia* records of the IP addresses that were assigned to Defendant and communications concerning piracy. I amended the subpoena based upon a telephone conference with Digital Ocean. Counsel for Digital Ocean said he would respond to the amended third-party subpoena after the Court rules on Defendant's motion to quash.

19. On Oct. 26, 2021, Defendant filed an amended notice of hearing objecting to the amended subpoena in which it argues that disclosure would "potentially contain trade secret and confidential and proprietary information including, *inter alia*, pricing information and contracts between TorGuard and Digital Ocean LLC."

20. I cannot completely identify which IP addresses and the times where Defendant infringed Plaintiffs' Works without receiving the IP addresses reassigned to Defendant from its host providers such as QuadraNet and Digital Ocean or from Defendant.

21. Not only does Defendant use host providers that do not reveal the IP address reassignments, Defendant is actively hindering Plaintiff from obtaining this information in discovery.

22. As of today's date, Defendant has yet to provide even the initial disclosures required by Rule 26(a)(1)(D).

Defendant's DMCA agent/Notices

23. On Oct. 23, 2021, I searched the Copyright Office’s DMCA Designated Agent Directory for records for “VPNnetworks”. Exhibit “1” is a true and accurate printout of the records that show that Losey PLLC has been Defendant’s registered DMCA agent since Nov. 23, 2018.

24. On Oct. 23, 2021, I searched the Copyright Office’s “Old Directory of DMCA Designated Agents 1998-2016” [https://copyright.gov/onlinesp/list/t_agents.html] for records of a DMCA agent for Defendant under the name “VPNnetworks” or “TorGuard” and found none. Accordingly, it appears that Defendant did not have a DMCA agent prior to Nov. 23, 2018.

25. Below is a true and accurate copy of §8(h) and the notification section of QuadraNet’s publicly available terms of service and data breach policy viewable at <https://www.quadranet.com/terms-of-service> as it appeared on 10/26/2021. §8(h) states that “It is client’s responsibility to promptly notify...of any change in email address or contact person(s)” and the notification section states that it “...commits to a notification via email to...the primary business contact registered upon contract signing.”

8. Renewal and Billing Schedule

QuadraNet’s Billing and Renewal Schedules is subject to the following terms and conditions:

- a. All payments must be timely; that is, they must be received by QuadraNet on their due date. QuadraNet will send to client’s billing contact by email an invoice a minimum of ten (10) days prior to the date (unless specifically agreed otherwise in writing). All payment must be made in U.S. Dollars.
- b. If payment is not received when due, Client shall be in default and QuadraNet, will send notice of late payment to Client with ten (10) days to cure. If the account default is not cured within ten (10) days, Quadranet, at its sole discretion, may suspend or terminate services without further notice.
- c. All or any portion of monies owed to QuadraNet that are not received when due shall incur a late charge of 1.5% of the amount owing, per month, or the maximum permitted by law, whichever is less, until payment is made.
- d. If services are suspended, client shall pay a minimum reactivation fee of \$25.00.
- e. For clients on a month-to-month service, QuadraNet reserves the right to change pricing any time upon notice to client.
- f. If client’s account is paid by credit card, it is client’s responsibility to make sure the card is valid, so that QuadraNet can complete a charge. If the charge is not complete, QuadraNet is authorized to charge the account after the original processing date. It is client’s responsibility to notify QuadraNet of any change in credit card to be used for payment on client’s account.
- g. If client’s account is paid by check and the check is returned “Non-Sufficient Funds,” client shall be charged a \$35.00 process and handling fee.
- h. It is client’s responsibility to promptly notify QuadraNet of any change in email address or contact person(s).

26.

Notification

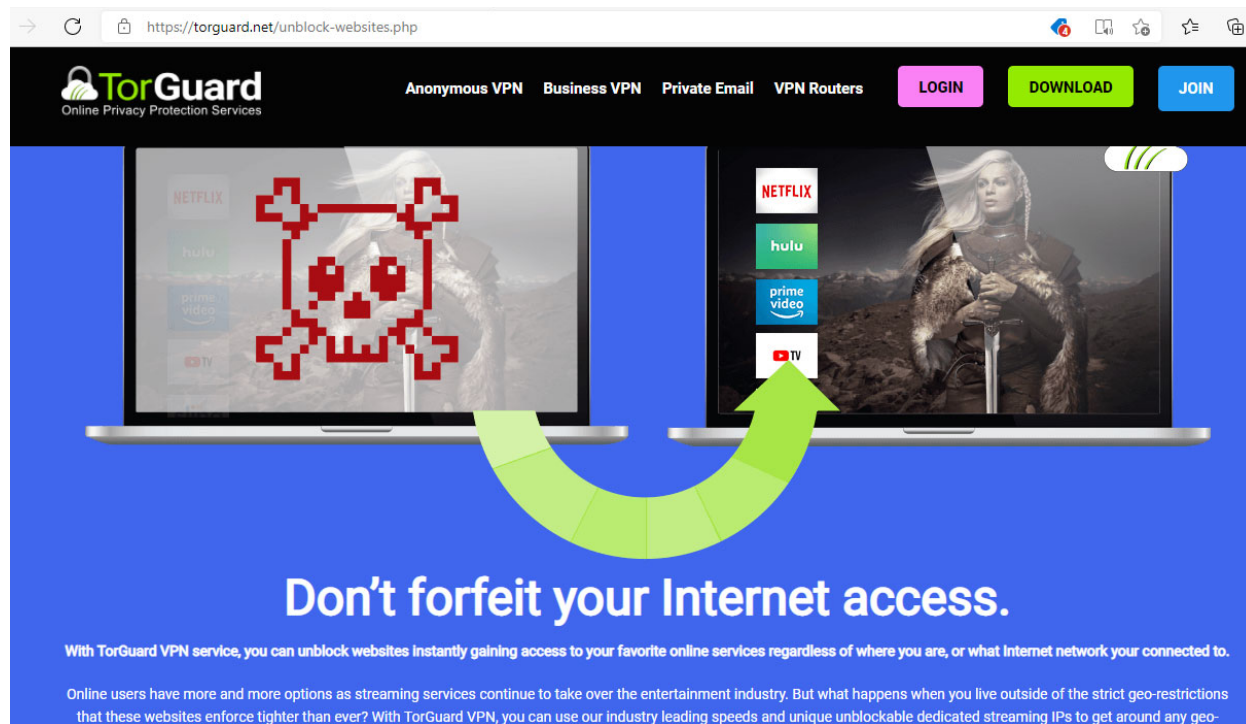
QuadraNet Enterprises LLC commits to a notification via email to affected data controllers -customers/partners-, specifically to the primary business contact registered upon contract signing, as soon as possible but no later than 72 hours of reasonable suspicion of a Data Breach. If there is an operational impact, an update can also be seen on status.quadranet.com.

27.

28. Plaintiffs' exclusive rights provided by US copyright law include the exclusive rights to publicly perform (stream) and distribute copies of their Works. Rightsholders will often negotiate licenses to different distributors in different geographic regions. Accordingly, a region outside of the US may have a different distributor from the US distributor or may not yet have a licensed distributor. For example, a legal platform such as Netflix or Hulu may have a license to distribute or stream a movie in the United States but not have a license to distribute or stream the same movie in a different region such as, for example, Singapore.

Defendant has an incentive to conceal its IP addresses so that it can continue to permit its subscribers to use the service for piracy.

29. Defendant promotes its VPN service for being used to overcome geographical restrictions of legal platforms such as Amazon Prime, Netflix or Hulu. Below is a true and accurate partial screenshot of Defendant's website <https://torguard.net/unblock-websites.php> as it appeared on 10/23/2021.



30.

31. Below is a true and accurate screenshot of Defendant's website

<https://torguard.net/blog/unblock-hulu-world/> as it appeared on 10/23/2021.

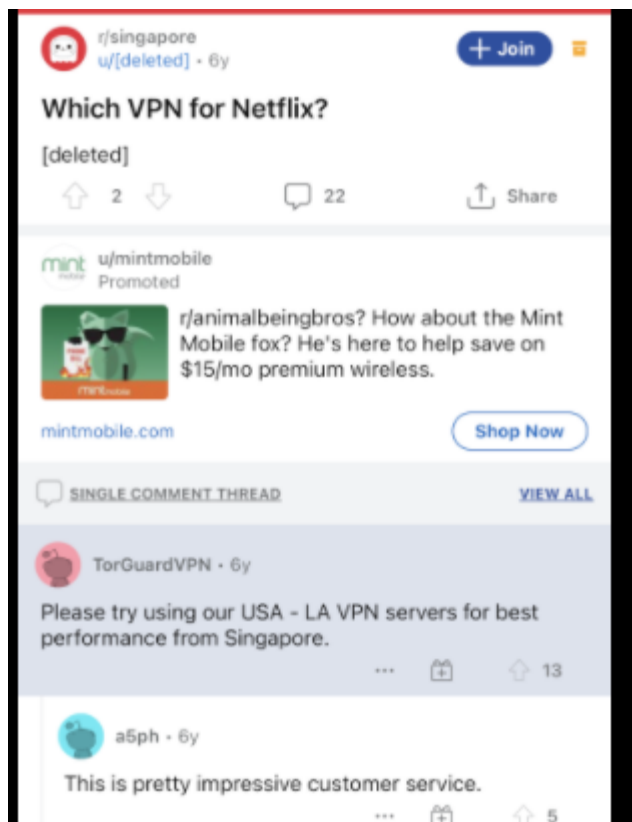
The screenshot shows a web browser window with the URL torguard.net/blog/unblock-hulu-world/. The page header features the TorGuard logo and navigation links for 'Anonymous VPN', 'Business VPN', 'Private Email', and 'VPN Routers'. The main content area displays a blog post with the following details:

- Post number: 23
- Month: July
- Author: admin
- Category: Countries
- Comments: 0

The post text reads: "Hulu is a great entertainment resource which provides an outstanding range of contents, such as TV shows, movies, clips, trailers, behind-the-scenes footage and a lot of other different media. But Hulu does have one major drawback. It's only available as long as you live in the United States and on its overseas territories. BUT! Why to miss all this fun if you are not in USA and why to think that living anywhere else is quite lack of luck? Well, do not worry, we are gonna give you some easy tips and tricks to watch Hulu outside US! You may do it thanks to our TorGuard VPN service. TorGuard VPN service is the best solution to bypass the site's blocking. Our software allows you to connect to a VPN server which provides you with a new US IP address and enables you to watch Hulu anytime you want it. How to get it? Order and pay for TorGuard VPN service; Download the application & connect to VPN; Simply watch Hulu!"


32.

33. Below is a true and accurate copy of a comment in the subreddit r/Singapore of the platform Reddit where Defendant encouraged an individual in Singapore to use its service, particularly Defendant's server in Los Angeles, to access Netflix and view content that is geographically restricted to the United States while the individual was in Singapore.



34.







35. I studied the comment history of the Reddit user TorGuardVPN. The comment history includes numerous comments promoting TorGuard with discount codes and responding to criticism of the service. Accordingly, I believe the Reddit user “TorGuardVPN” is an official account or authorized account of Defendant. Below are true and accurate screenshots of some of the comments by the user TorGuardVPN. Note that in the first comment Defendant states that they have removed their IP addresses from being publicly viewable.


 TorGuardVPN · 1y

Hi, nothing has changed. We removed the IP server list to prevent abuse and increase network performance.

Using load balancing provides you with a different IP more often which is better for privacy.







If you want to connect to a static socks5 proxy IP address you still can. Please contact our support desk and they will provide you some.

 7   Reply  Share  Report  Save

 gnomehole · 1y

How is this abused when we have a connection limit? This was poorly communicated, none of my proxies are working right now and it appears others are in the same boat.

I'm sure you have an explanation for current customers on the change, how to fix, and our options.. can you post a link or share this communication?

 5   Reply  Share  Report  Save

36.

movie_addict97 2 points · 2 years ago

Torguard should have handled it in a better way instead of filing a frivolous lawsuit.

TorGuardVPN 1 point · 2 years ago

TorGuard cannot remove or censor our affiliate's Youtube videos or blogs under any circumstance.

Our bug bounty program provides clear guidance on how to submit security concerns. Proper protocol was not followed. The evidence will speak for itself and we look forward to proving the truth of our allegations.


NordVPN's blog post claims the case was dismissed on June 19th but fails to mention the complaint was re-filed in the Middle District of Florida on 06/26/19:

<https://torguard.net/downloads/1.6-26-2019-Complaint.pdf>

Reply Share ...

37.

↑ 3
↓

 **r/torguard** · Posted by u/TorGuardVPN 3 years ago

Switch to TorGuard with our Fresh Start Promo and get 30 Days Free

torguard.net/blog/s...


0 Comments Share Save Hide Report

100% Upvoted

Log in or sign up to leave a comment


Log In Sign Up

Sort By: Best ▾



38.

↑ 2
↓

 **r/torguard** · Posted by u/TorGuardVPN 4 years ago

New Residential VPN IP's Now Available for US

torguard.net/blog/n...


5 Comments Share Save Hide Report

100% Upvoted

Log in or sign up to leave a comment

Log In Sign Up

Sort By: Best ▾

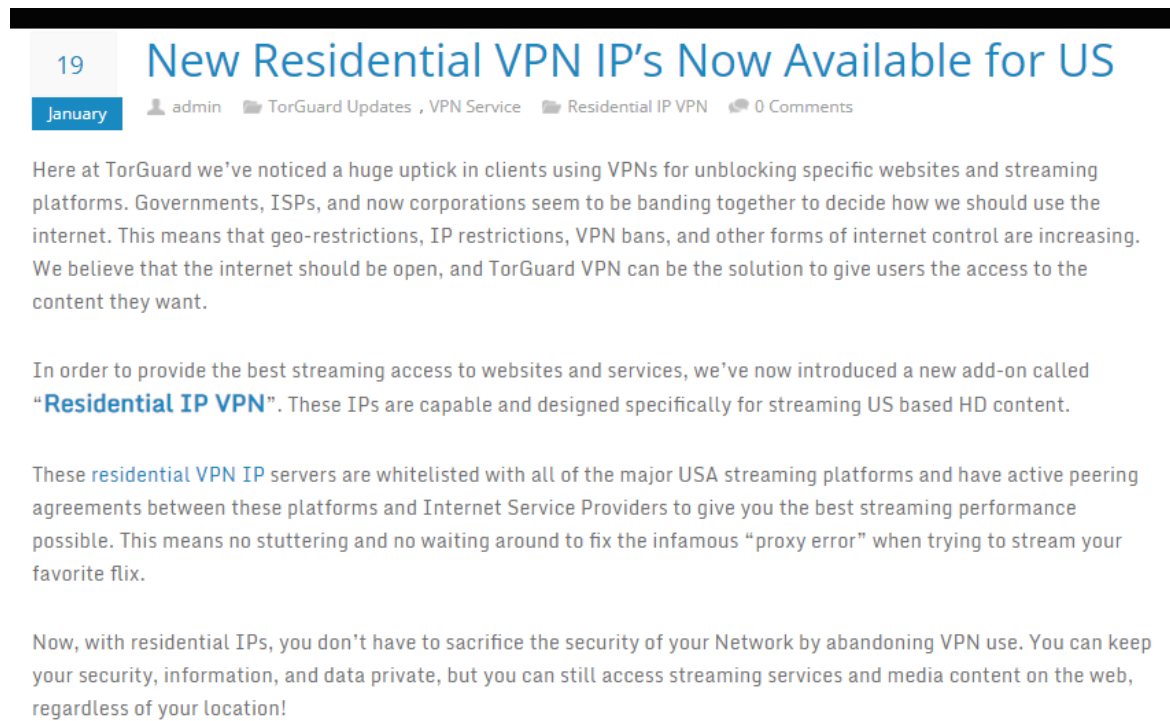


39.

40. Many legal platforms such as Netflix will “blacklist” IP addresses of known VPN providers to prevent violation of geographic restrictions. See Jacoby Parker, How does Netflix detect and block VPN use?, Aug. 16, 2021 <https://www.techradar.com/vpn/how-does-netflix-detect-and-block-vpn-use> [last accessed on 10/23/2021]. Accordingly, VPN providers such as Defendant have an incentive to not publicly reveal the IP addresses assigned to them so that they are not blacklisted to prevent their end users from streaming or distributing content from

unauthorized regions. As shown above, Reddit user TorGuardVPN states that Defendant removed its IP server list.

41. Defendant advertises a “Residential VPN” for the purpose of dealing with “geo-restrictions, IP restrictions, VPN bans” that includes “whitelisted” IP servers. Below is a true and accurate partial screenshot of the website <https://torguard.net/blog/new-residential-vpn-ips-now-available-for-us/> as it appeared on 10/24/2021.



42.

Defendant’s business activity in Miami.

43. Defendant advertises on its website that it has a server “us-fl.torguard.com” available in Miami for its customers to use. See <https://torguard.net/network/> [last accessed on 10/20/2021, relevant partial screenshot shown below].

Country	City	Endpoint	Status
Canada	Vancouver	cavan.torguard.com	✓
Mexico	Mexico City	mx.torguard.com	✓
USA	Atlanta	us-atl.torguard.com	✓
USA	LA	us-la.torguard.com	✓
USA	Miami	us-fl.torguard.com	✓

44.

45. On Defendant’s frequently asked question (“FAQ”) website

[https://torguard.net/faq.php], in response to the question “What locations do you offer?”

Defendant answers Miami, USA as one of its locations. Below is a true and accurate partial screenshot (highlight added) of how this portion appeared as of 10/25/2021.

46.

torguard.net/faq.php

TorGuard
Online Privacy Protection Services

Anonymous VPN Business VPN Private Email VPN Routers LOGIN DOWNLOAD JOIN

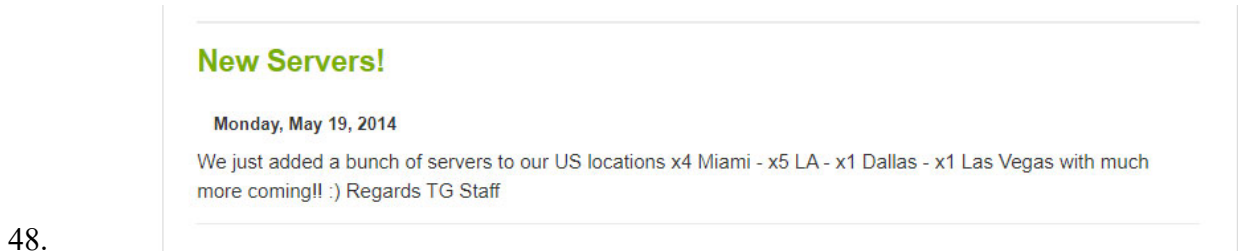
What forms of payment do you currently accept?

What locations do you offer?

Answer: We offer many locations around the world with multiple endpoints in each location, please see below:

Country-City AUS:Sydney AUT:Vienna BEL:Brussels BGR:Sofia BRA:Sao Paulo CAN:Toronto CAN:Vancouver CHE:Zurich CHL:Vina del Mar CZE:Prague DEU:Frankfurt DNK:Copenhagen EGY:Cairo (Virtual) ESP:Madrid FIN:Helsinki FRA:Paris GBR:London GRC:Athens HKG:HongKong HUN:Budapest IDN:Jakarta IND:Bangalore IRL:Dublin ISL:Reykjavik ISR:Tel Aviv ISR:Jerusalem ITA:Milan JPN:Tokyo KOR:Incheon (Virtual) LUX:Luxembourg MDA:Chisinau MEX:Mexico City (Virtual) NLD:Amsterdam NOR:Oslo NZL:Auckland POL:Warsaw PRT:Lisbon ROM:Bucharest SGP:Singapore SVK:Bratislava SWE:Stockholm THA:Bangkok UAE:Dubai UKR:Kremenchuk USA:Atlanta USA:Chicago USA:Dallas USA:Las Vegas USA:Los Angeles **USA:Miami** USA:New Jersey USA:New York USA:Seattle USA:Salt Lake City

47. On Oct. 25, 2021, I used the Internet Archive website “Wayback Machine” to look at previous versions of Defendant’s website. I have used the Internet Archive website numerous times and have found it to be reliable. Below is a true and accurate partial screenshot of a previous version of Defendant’s Announcement website at <http://torguard.net/announcements.php> where it announced it had added four servers in Miami.



Defendant’s Affiliate Program and its affiliates’ promotion of TorGuard for piracy.

49. Defendant promotes its affiliate program on its website <https://torguard.net/vpn-reseller-affiliate.php>. Exhibit “7” is a true and accurate printout of this website. Below is a true and accurate partial screenshot of how the website appeared on 10/24/2021. Here, Defendant states, “...we consider our affiliates the backbone of our marketing team.”

The Benefit of Becoming a TorGuard VPN Affiliate:

<ul style="list-style-type: none"> Commission Management Banners Payouts Support 		<p>30% Lifetime Recurring Commissions:</p> <p>At TorGuard, we consider our affiliates the backbone of our marketing team. To prove this, we are now offering 30% recurring lifetime commission for any and all sales referred to us. This includes commission payouts on all services like Proxy, VPN, Dedicated IPs and Email, but also includes any upsell features like dedicated IPs or other account add-ons. Because bonuses are recurring, you will continue to get paid for the life of your referrals subscription.</p> <p>Signing up for TorGuard’s VPN affiliate program is easy. All current members can activate their affiliate account within the online control panel, while prospective affiliates can fill out the form below to apply. After activating your VPN affiliate account please contact our support desk with any questions.</p>
---	--	--

50.

51. Exhibit “2” is a true and accurate response I received from QuadraNet in response to a subpoena for the subscriber identification records for certain IP addresses in the Hawaii action stating that these IP addresses were reassigned to TorGuard. MEU confirmed over 1000 instances of infringement at each of IP addresses 96.44.142.226 and 173.254.255.106.

52. The affiliate “Travis” referred to in paragraph 248 of the Second Amended Complaint posted comments in support of piracy and promoting TorGuard with a discount code from these IP addresses and others that are believed to be associated with Defendant.

53. For example, on 2019-03-30 17:29:41 UTC, Travis posted the following comment defending TorGuard:

But none of that changes the fact, that the whole basis of the argument was that Torguard claimed, that it would not be possible either "IF their servers was compromised", which is blatantly false [...] Understand now?" Yes, I understand that the scenario you imagine is one to which technical staff at TorGuard Head Quarters would not be able to notice the compromised server, would be unable to detect the sudden exportation and resource load of log activity, and would be unable to revoke that compromised servers access to the rest of the Torguard VPN network which would render any logged user usage activity moot since Torguard customers would no longer be able to log in to the compromised server, nor would that server be listed on the available server list. But realistically, none of that would ever happen so the statement in the OP is still True. Not some imaginary BS you come up with in your head.

54. Travis posted numerous comments supporting use of VPN for piracy. For example, on 2019-04-19 13:53:50 UTC, Travis posted the following comment:

Just imagine if PopcornTime would have been released with a built in VPN or some other way to obfuscate the traffic like Tribler. The reason for the sabotage, smearing, loss of popularity, and failure of the app should now be clearly apparent.

55. On 2019-08-01 05:33:18 UTC, Travis posted the following comment admitting to his use of a VPN to access the notorious piracy website YTS:

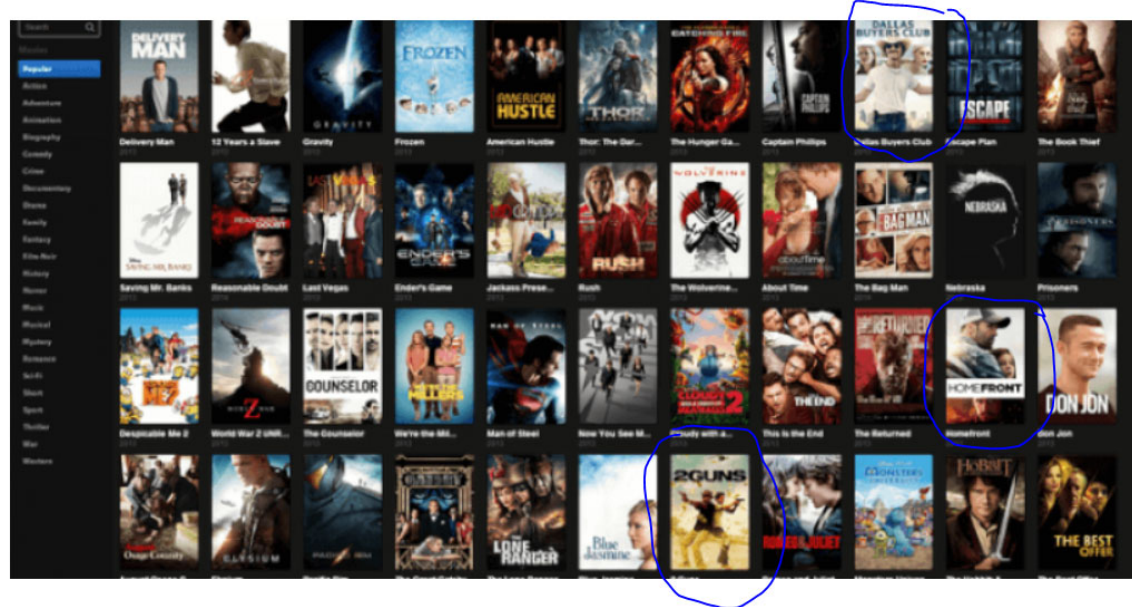
I use YTS quite frequently. The only users who are being pursued are those who don't download behind a log free VPN provider.

56. On 2019-08-17 14:05:18. UTC, Travis posted the following comment, “Forget the additional \$20 cost of some Disney streaming package, just teach your kids how to download their favorite Disney titles from TPB while using a VPN.” TPB refers to the notorious piracy website The Pirate Bay.

57. Exhibit “3” is a true and accurate print out of website <https://best10vpn.com/what-is-the-best-vpn-for-popcorn-time/> as it appeared on 10/22/2021. Because the website includes a discount code for TorGuard, I believe this website operator is an affiliate of TorGuard. Below is a true and accurate partial screenshot of a portion of website made on 10/26/2021 with circled portions for emphasis showing movies Defendant’s affiliates promotes that can be watched with Popcorn Time while running Defendant’s VPN service. The copyright for movie *Dallas Buyer’s Club* is owned by Plaintiff Dallas Buyer’s Club, LLC. The copyright for movie *2 Guns* is owned by Plaintiff Screen Media Ventures, LLC. The copyright for movie *Homefront* is owned by Plaintiff Millennium IP, Inc.

What is the Best VPN for Popcorn Time?

ALI RAZA DECEMBER 20, 2018 NO COMMENTS BLOG



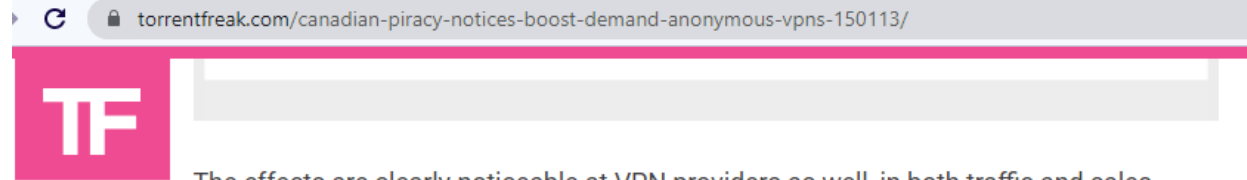
58.

59. Exhibit "4" is a true and accurate print out of the website

<https://cryptmode.com/best-vpn-for-official-popcorn-time-sh-client/> as it appeared on 10/22/2021. Because the website includes a discount code for TorGuard, I believe this website operator is an affiliate of TorGuard.

Defendant promotes TorGuard for piracy and profits from piracy

60. The news website *TorrentFreak* quoted Defendant boasting that after Canada implemented a rule requiring mandatory piracy notifications to deter copyright infringement, its Canadian sales increased by 100%. Below is a true and accurate partial screenshot of the article at the website <https://torrentfreak.com/canadian-piracy-notices-boost-demand-anonymous-vpns-150113/> as it appeared on 10/24/2021.



The effects are clearly noticeable at VPN providers as well, in both traffic and sales.

[TorGuard](#), a VPN and BitTorrent proxy provider saw the number of Canadian visitors and subscribers double this year.

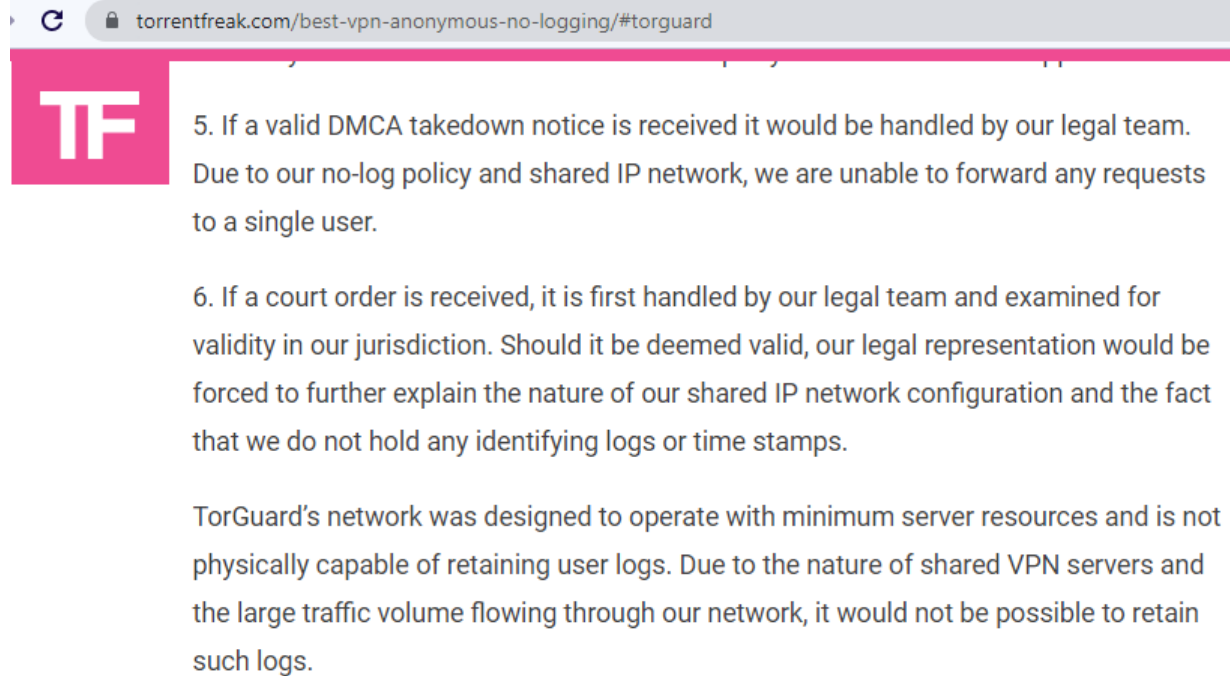
“Since the start of 2015 TorGuard has seen a drastic jump in Canadian traffic and subscribers. At the time of this writing our Canadian sales are up roughly 100% and this trend appears to be increasing,” TorGuard’s Ben Van der Pelt tells us.

TorGuard traffic from Canada



61.

62. Defendant provided information to the news website *TorrentFreak* in response to questions about its VPN service that was published. Below is a true and accurate partial screenshot of the website <https://torrentfreak.com/best-vpn-anonymous-no-logging/#torguard> where Defendant’s answer was published as it appeared on 10/24/2021. Defendant states, “Due to our no-log policy and shared IP network, we are unable to forward any requests to a single user.”

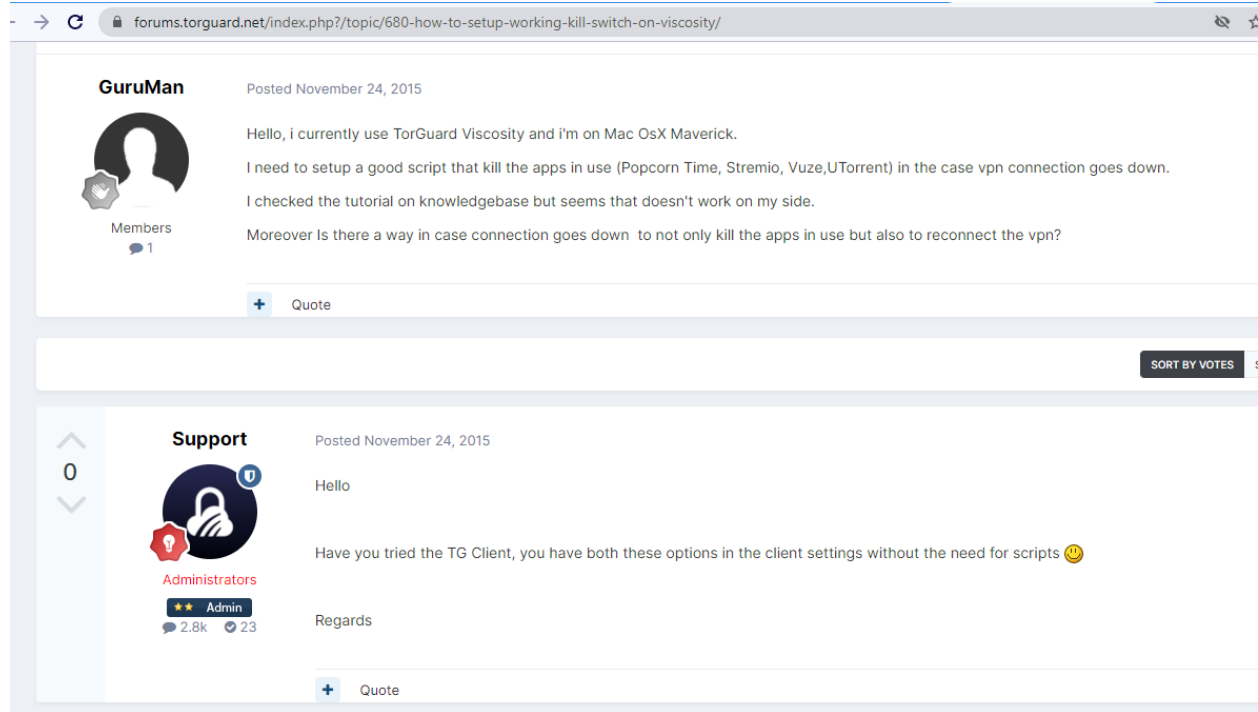


63.

64. Below is a true and accurate screenshot of Defendant's website forum at

<https://forums.torguard.net/index.php?/topic/680-how-to-setup-working-kill-switch-on-viscosity/>

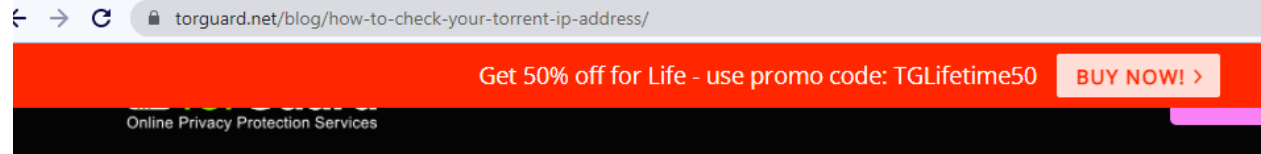
Defendant's administrator advised a TorGuard end user who sought help with a script to kill the app in use (Popcorn Time) when the VPN connection goes down and reconnect when the VPN reconnects.



65.

66. Below is a true and correct screenshot from Defendant's website at:

<https://torguard.net/blog/how-to-check-your-torrent-ip-address/> Here Defendant states, "it's wrong to illegally download things, but it doesn't need to be anybody's business what you are downloading. When you use a VPN or a proxy to download torrents, you're hiding yourself and your activity from anyone..."



Do I Need a VPN or Proxy to Download Torrents?

Technically, you don't need a VPN or proxy to download torrents. You can download a torrent directly from your browser, publicly, on the open internet. When you do that, you assume all the risks that come with it. Anytime you are downloading a torrent file your IP address is visible to the larger swarm that is provided you the download.

If you're downloading something under other circumstances, or your ISP doesn't allow BitTorrent then you're going to raise some red flags. Your internet service provider can see what you're doing. If the content you're downloading is through your personal IP address then your IP address and personal identity could be linked to that download.

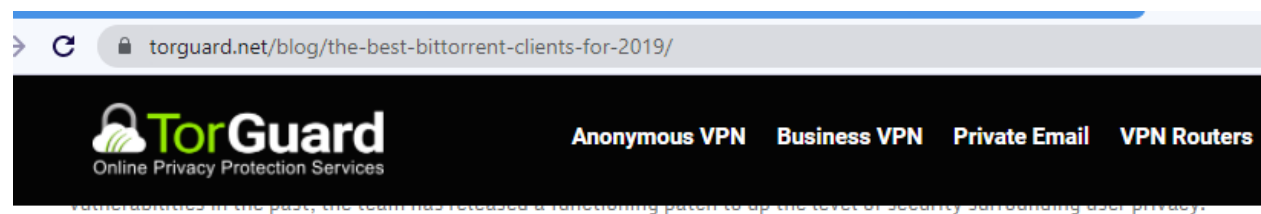
Of course it's wrong to illegally download things, but it doesn't need to be anybody's business what you're downloading. When you use a VPN or a proxy to download torrents, you're hiding yourself and your activity from anyone who may feel inclined to watch it. What you do is your business, and it should stay that way.

Why Do I Need to Check My Torrent IP Address?

67. _____ checking your torrent IP address is necessary to establish that using VPN services is indeed not it should be for now basic

68. Below is a true and correct partial screenshot from Defendant's website at:

<https://torguard.net/blog/the-best-bittorrent-clients-for-2019/> as it appeared on 10/23/2021. Here Defendant acknowledges that "Many people are afraid to torrent things because the repercussions, especially those from their internet service provider can be severe. Using a torrent VPN like TorGuard for file sharing eliminates those worries."



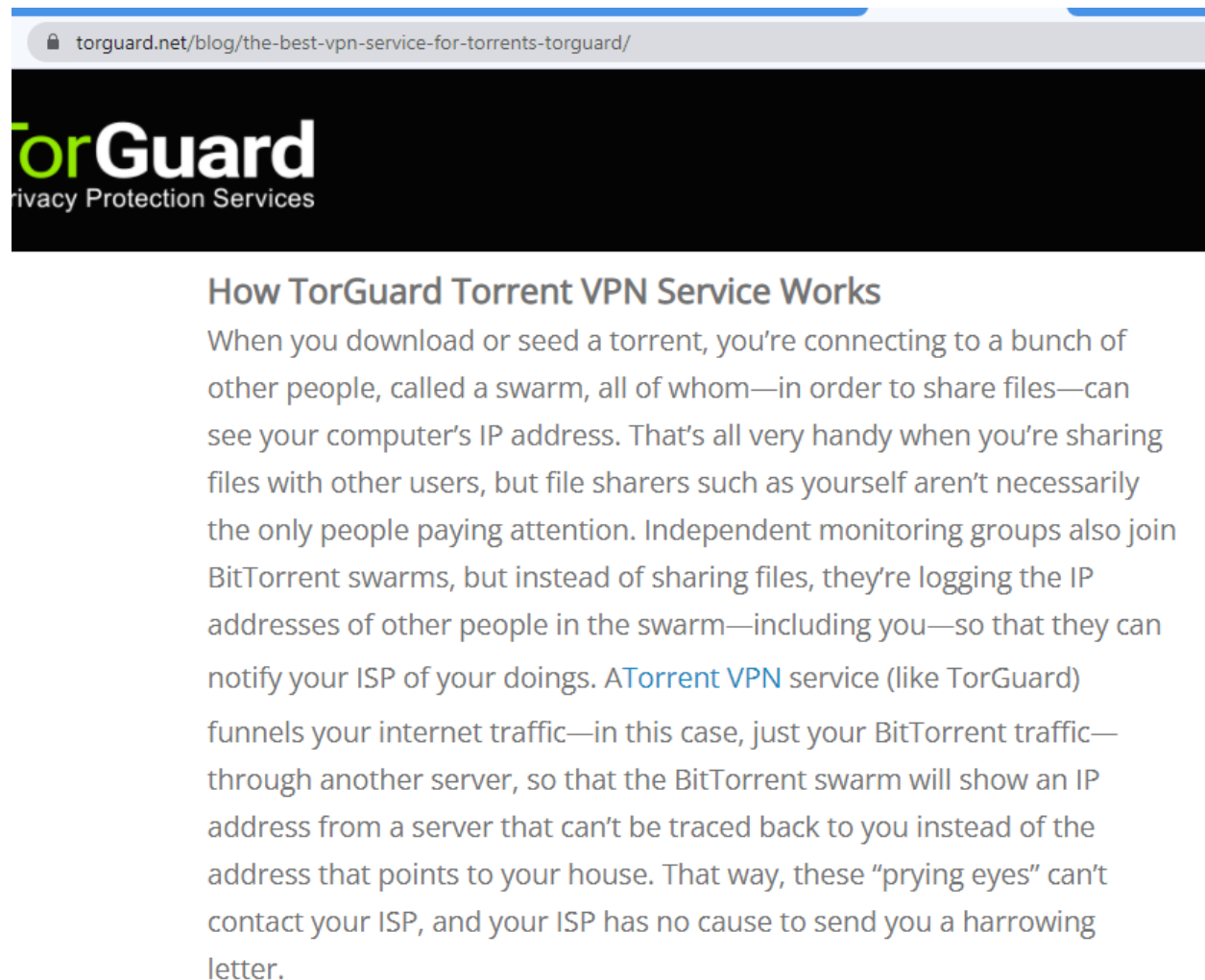
Keeping Yourself Safe While Torrenting

Many people are afraid to torrent things because the repercussions, especially those from their internet service provider, can be severe. Using a **torrent VPN** like TorGuard for file sharing eliminates those worries. TorGuard shields all of your activities, including torrenting, from absolutely everyone. If no one can see what you're doing, you're free to do whatever you want. Stay safe and secure while torrenting by using TorGuard.

69. _____

70. Below is a true and correct screenshot from Defendant's website at:

<https://torguard.net/blog/the-best-vpn-service-for-torrents-torguard/> as it appeared on 10/23/2021. Defendant warns his end users that other monitoring groups are logging the IP addresses on the swarm so that they can notify the ISP of the things you do, but if the end users use TorGuard, their BitTorrent traffic will be routed through another server that can't be traced back to them so that these monitoring groups cannot contact your ISP, and your ISP has no cause to send you a harrowing letter. Defendant can only be talking about rightsholders' agents that monitor swarms for piracy and law enforcement that monitors swarms for child pornography when it says "monitoring groups".

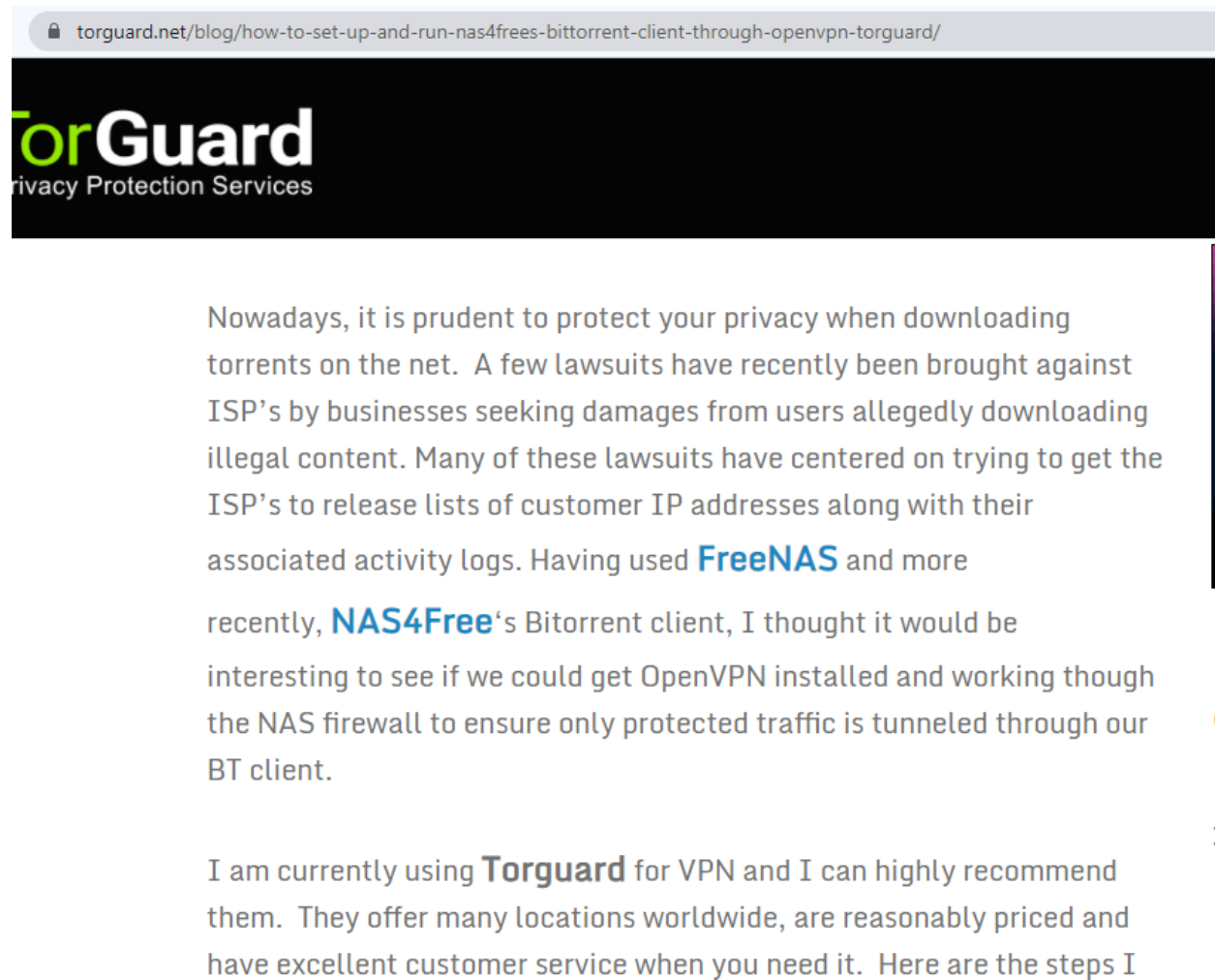


71.

72. Exhibit “5” is a true and accurate print out of Defendant’s website

[https://torguard.net/blog/how-to-set-up-and-run-nas4frees-bittorrent-client-through-openvpn-](https://torguard.net/blog/how-to-set-up-and-run-nas4frees-bittorrent-client-through-openvpn-torguard/)

[torguard/](https://torguard.net/blog/how-to-set-up-and-run-nas4frees-bittorrent-client-through-openvpn-torguard/) as it appeared on 10/23/2021. Also below is a partial screenshot as it appeared on 10/23/2021. Here Defendant warns that it is “prudent to protect your privacy when downloading torrents” because lawsuits have been brought by businesses against ISPs for damages from users allegedly downloading illegal content that center on “trying to get the [sic] ISP’s to release lists of customer IP addresses along with their associated activity logs.”

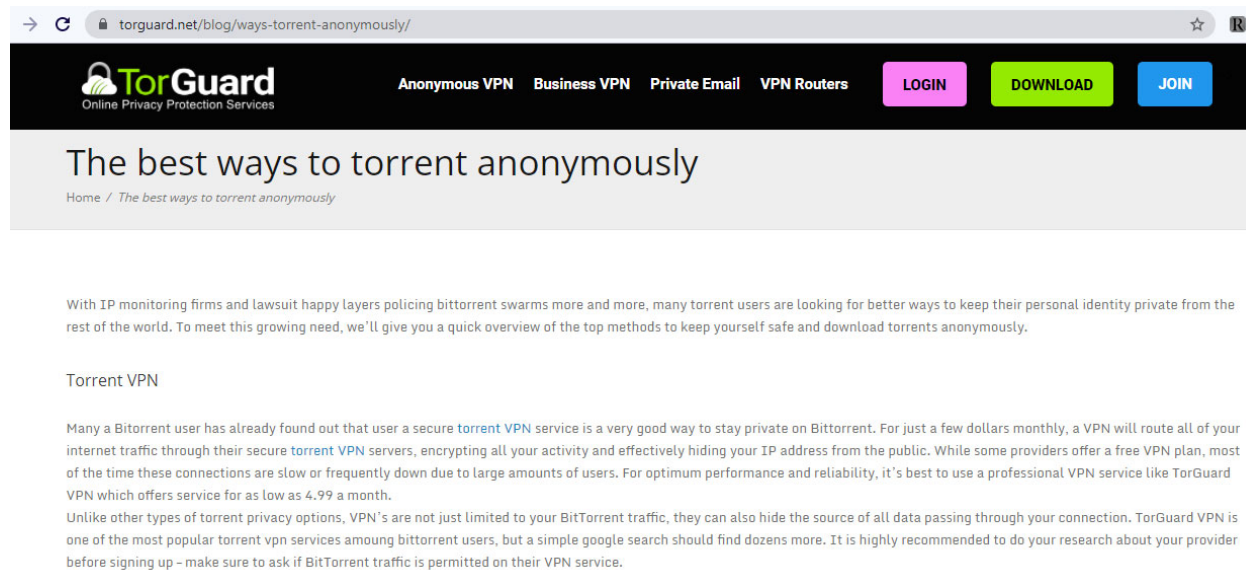


73.

74. Exhibit “6” is a true and accurate print out of Defendant’s website

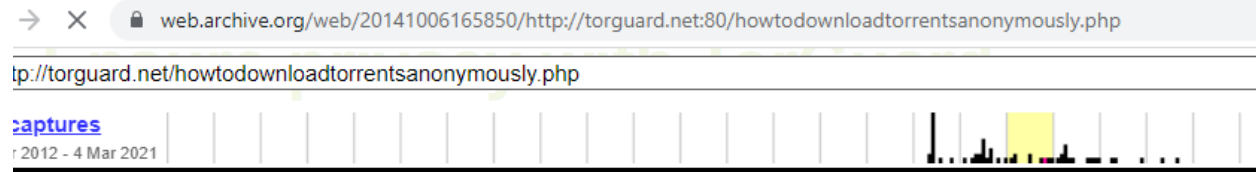
<https://torguard.net/blog/ways-torrent-anonymously/> as it appeared on 10/23/2021. Also below

is a partial screenshot as it appeared on 10/23/2021. Here Defendant clearly states, “With IP monitoring firms and lawsuit happy [sic] layers policing bittorrent swarms more and more, many torrent users are looking for better ways to keep their personal identity private from the rest of the world. To meet this growing need...”



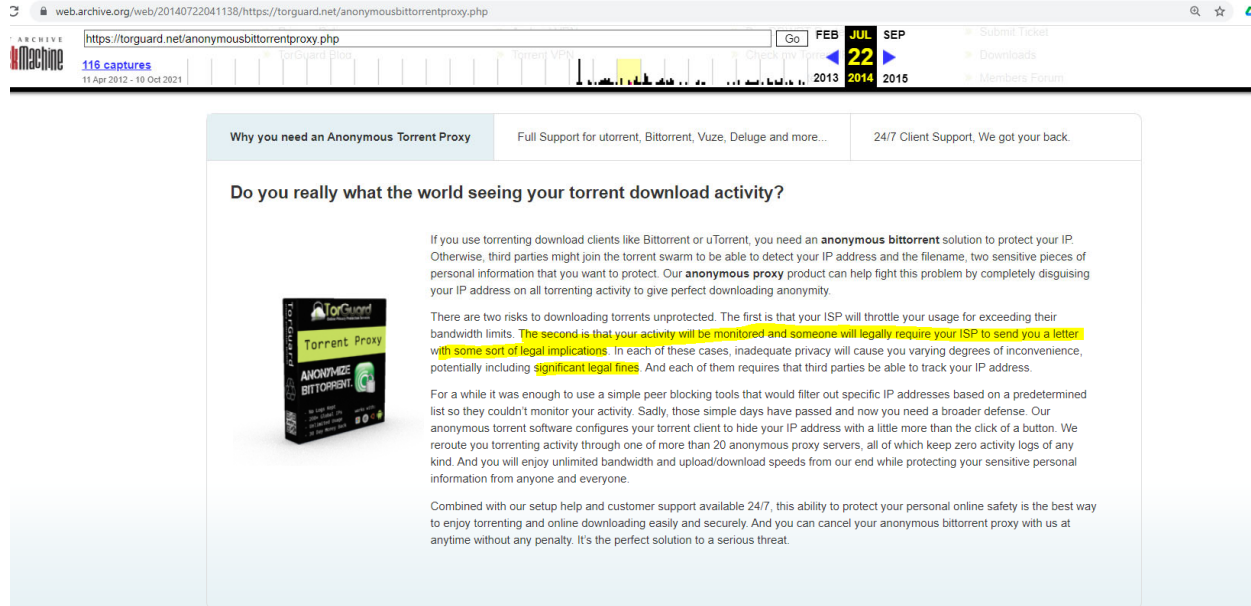
75.

76. On Oct. 25, 2021, I used the Internet Archive website “Wayback Machine” to look at previous versions of Defendant’s website. I have used the Wayback Machine numerous times and have found it to be reliable. Exhibit “8” is a true and accurate print out of the October of 2014 previous version of Defendant’s website <http://torguard.net/howtodownloadtorrentsanonymously.php> from the Wayback Machine. Below is a true and accurate partial screenshot with highlighting showing how the website appeared in October of 2014.



77.

78. On Oct. 25, 2021, I used the Wayback Machine to look at previous versions of Defendant's website <https://torguard.net/anonymusbittorrentproxy.php>. Below is a true and accurate partial screenshot with highlighting showing how the website appeared in July of 2014. When Defendant states "significant legal fines", it must be referring to statutory damages for copyright infringement.



79.

80. Below is a true and accurate partial screenshot of a now removed article posted on the TorGuard subreddit announcing that the payment service PayPal stopped accepting payments from Defendant in 2019. According to an article from TorrentFreak, PayPal had earlier stopped doing business with Defendant over concerns with piracy. See <https://torrentfreak.com/paypal-bans-bittorrent-friendly-vpn-provider-120622/> [last accessed on 10/24/2021].




81.

82. Even BitTorrent, Inc., the company behind the BitTorrent client app “uTorrent” rejected advertisements from Defendant because it considered Defendant’s promotions created a “high risk” of it being associated with piracy. See <https://torrentfreak.com/utorrent-and-bittorrent-reject-high-risk-vpn-ads-130506/> [last accessed on 10/24/2021].

I declare under penalty of perjury that the foregoing is true and correct.

DATED: Kailua-Kona, Hawaii, October 26, 2021.

CULPEPPER IP, LLLC



Kerry S. Culpepper

Virginia Bar No. 45292

Hawaii Bar No. 9837

CULPEPPER IP, LLLC

75-170 Hualalai Road, Suite B204

Kailua-Kona, Hawai'i 96740

Exhibit "3"

Have you checked out the world's first VPN tier list? It's like gaming tier lists, but for VPNs!

Best iOS VPN Best Torrent VPN Best Mac VPN Best Android VPN Best Windows VPN Best Linux VPN



About/Contact

Reviews

Blog

VPN Comparison Chart

YouTube

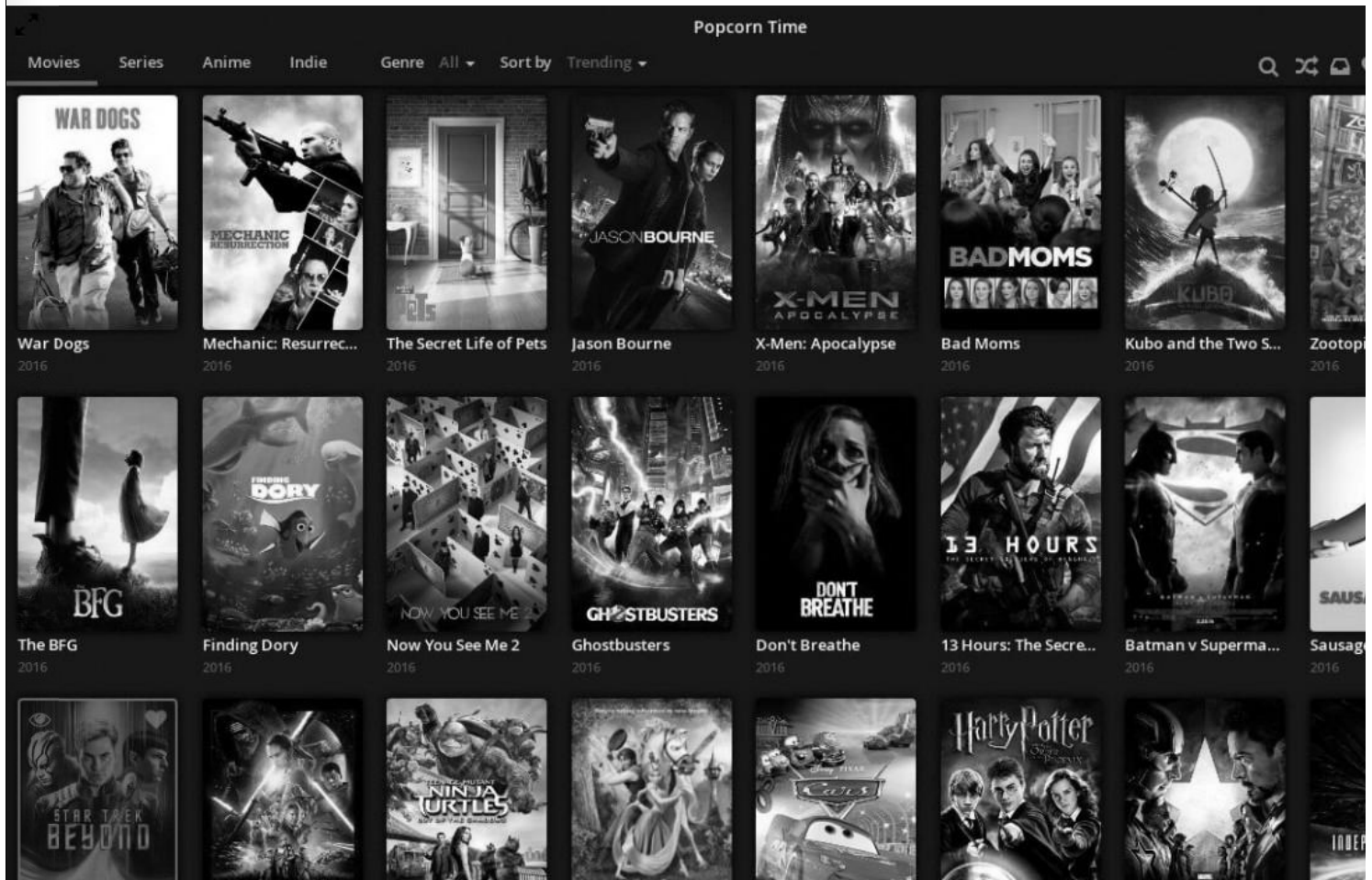
What is the Best VPN for Popcorn Time?

ALI RAZA DECEMBER 20, 2018 NO COMMENTS BLOG



Torrenting is awfully entertaining, and a very straightforward process. However, it can get you in contact v unwanted agents, so you would be best served if you protect while you value. Popcorn Time, a torrent-be platform, would be even better than it already is with a VPN.

Popcorn Time: a top-notch torrent-based client



Widely known around the torrenting environment, Popcorn Time is an incredible source of movies of all genres. You can stream a science-fiction marvel, an action-packed production, a hilarious sitcom, a profound dramatic, a horror, a comedy, a thriller, a romance, a documentary, a cartoon, a TV series, and other shows. All are available in this network, as are animated and short features.

Popcorn Time is a free software BitTorrent client that comes with an integrated media player. It is similar to Stremio and Powder Player in their core functionality, which is to reproduce torrent files found on the web. It is compatible with multiple platforms, and it functions as a no-cost alternative to streaming giants Netflix, Hulu, BBC iPlayer, and Amazon Prime Video, among others.

To achieve its streaming purpose, Popcorn Time implements sequential downloading of files listed by various sources, namely torrent websites. Users can also add third-party trackers manually.

The Popcorn Time app is straightforward to use, which is one of the things that has made it a favorite among the online streaming community worldwide. When it was at its peak, Popcorn Time was taken down in 2014 because of increasing pressure by the MPAA. After that moment, the software has been repeatedly forked with other

development teams. In four years, the original developers used several domains, such as popcorn.time.io and popcorn.time.sh.

Popcorn Time is compatible with Linux, OS X, Windows, and Android, which are the most widely spread operating systems. It is available in 44 languages, and it is written in HTML, JavaScript, and CSS.

Popcorn Time is similar to Netflix as its interface presents thumbnails and movie titles in a way that resembles the biggest streaming company in the world. People can look for options to stream by categories, title, or genre. When they click on the name of the file they want to enjoy, it is then downloaded through the BitTorrent protocol.

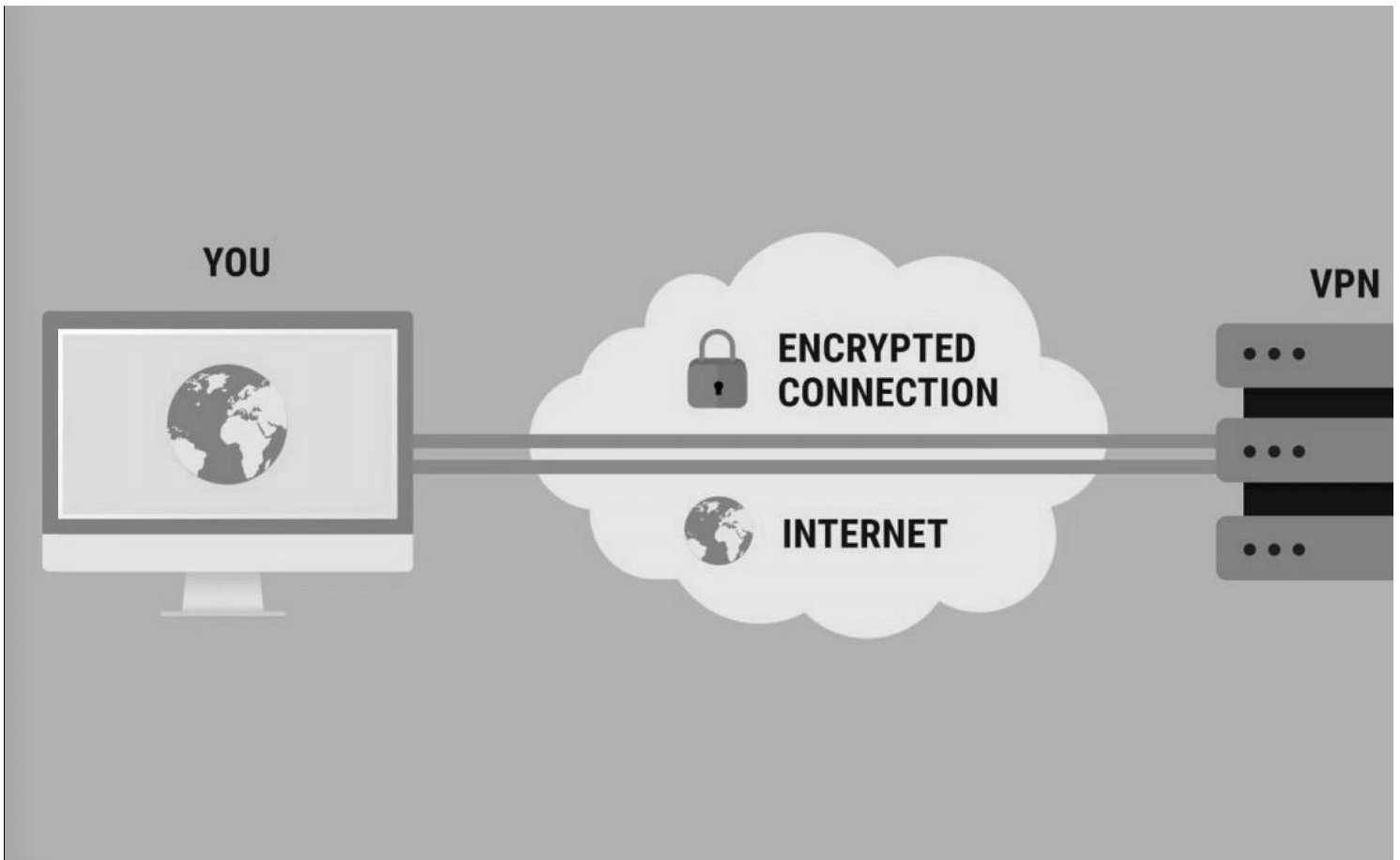
And, in a similar way that it happens in other torrent clients when Popcorn Time begins a file download, it starts sharing the file with other peers in the network, effectively seeding the torrent to others.

Bypassing geo-blocks and protecting your privacy

While Popcorn Time seems like an excellent option to enjoy torrenting activity from the comfort of your home, there are a few things you should know. The platform is excellent, but as it happens with nearly every torrent client and streaming client or network, you can't access content from other countries under normal circumstances.

That is called geo-blocking. Channels, streaming sites, networks, and torrent clients all over the world require content under the consent of studios, production companies, labels, and other entities, and more often than not they prefer their content to be shown only in the country in which the material was made, edited, and published. Trying to enter one of these pages from abroad will be a futile exercise without a VPN.

A VPN is what you need



Your Popcorn Time experience will be significantly better with a VPN. Disguising your IP address is necessary if you want to access internationally blocked content in your location because these sites can recognize where you are by seeing your IP number, and use that information to restrict you from entering if you are not within the server client's jurisdiction.

To enjoy 100 percent of control over your online entertainment, implementing a Virtual Private Network (VPN) is the perfect idea. VPNs are apps or clients available online (some of them are free, others require a paid subscription) that can unblock restricted content by hiding the user's IP address and traffic.



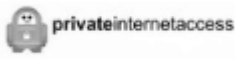
The content that the user generates is encrypted and rerouted to remote servers that the VPN company owns and travels through a virtual tunnel that it builds thanks to the implementation of protocols, such as OpenVPN, L2TP/IPSec, SSTP, and others.

VPN technology can offer users privacy and security because it will mask their exact location and shared data online. VPNs, therefore, provide the ability to browse the web in complete anonymity, which is essential to protect against hackers, copyright trolls, law enforcement agencies, malware developers, and other threats that may compromise your safety.

Sometimes when you torrent, you may accidentally incur in copyright infringement, since much of what you download is protected. To avoid being seen or tracked by a copyright enforcement agency, connect to a VPN.

server to protect your identity from leaking around the web.

The best VPN for Popcorn time, then, will have to allow unrestricted and unlimited P2P and torrenting act while also hosting servers in several locations around the world and having fast speeds for downloading (

Pick a VPN!	VPN	Price for 1 month sub	Site Rating	Buy Now
Best VPN		\$5 a month (code "best10VPN")	9.9	GO TO WE
Good VPN		\$9 a month	8.9	GO TO WE
Decent VPN		\$6.95 a month	8.8	GO TO WE

TorGuard: the best VPN for Popcorn Time

The banner features the TorGuard logo at the top left, with navigation links for Home, Anonymous VPN, Anonymous Proxy, Business VPN, Email, and Routers. A prominent circular badge in the upper right corner reads "7 DAY FREE TRIAL". The main headline is "Protect Your Privacy With Anonymous VPN." Below this, it states: "TorGuard VPN Service encrypts your internet access and provides an anonymous IP so you can browse securely." A "Get TorGuard Now" button is positioned in the lower left. The background shows a computer monitor displaying the TorGuard interface, which includes connection status (United States, Connected), connection time (00:00:02), protocol (UDP), cipher (AES 128-CBC), HMAC (SHA1), and PFS/TLS (Yes / v1.2). A video player is overlaid on the bottom right of the banner, showing a scenic landscape.

TorGuard is genuinely one of the best VPNs for Popcorn Time, offering a wide array of security features that guarantee that your identity and content will be away from the claws of malware developers, ransomware hackers, and especially copyright trolls that may track you if you don't encrypt your traffic.

For starters, TorGuard implements the military-grade AES 256-bit encryption in addition to a no logging policy that will make sure the brand won't share your logs with law enforcement agencies or other third parties. Also available are a kill switch and DNS leak protection. Additional security options that can be hired in a separate subscription: they are anonymous email, anonymous proxy, and a privacy bundle.

TorGuard is among the best VPN alternatives for torrent clients like Popcorn Time because it manages one of the broadest networks known by the industry, with more than 3,000 servers in 55 nations. You can connect five simultaneous devices, which is perfect because TorGuard is highly compatible.

[Visit TorGuard](#)

How to set up TorGuard, the best VPN for Popcorn Time

- Go to TorGuard's website
- Register for a monthly subscription (it costs \$10 per month)
- Download and install the app in your streaming device
- Launch the VPN app

- Sign in to your account
- Connect to your desired virtual server
- Done!



In conclusion, Popcorn Time is a torrent-based streaming platform that allows users to enjoy movies of all kinds and types. Essentially, it is a torrent client that comes with a media player included. It is compatible with many different operating systems and devices, as well.

However, you need to manage yourself with care while using it, because copyright trolls are always eager to sue offenders. If you want to protect your privacy and access content that is blocked due to geo-blocking, then hiring a reliable VPN provider is a good idea.

TorGuard has proven time and time again that it is, in fact, one of the best VPNs for Popcorn Time. Some people argue that it has no competition, thanks to its combination of P2P allowance, fast speeds, secure encryption, and robust privacy.

Related



How to Install Popcorn Time on MAC?
January 16, 2019
In "Blog"



Who Wins - Popcorn Time vs. Netflix?
January 16, 2019
In "Blog"



What are the Best Alternatives to Popcorn Time?
August 17, 2017
In "Blog"

POPCORN TIME STREAMING TORRENTING VPN



Ali Raza

Passion for Cyber Security and Technology.

At Best10VPN.com, we take privacy seriously and have researched today's best vpn services so you don't have to!

[Best Windows VPN](#)

[VPN Reviews](#)

[VPN Services](#)

Copyright © 2019 Best10VPN.com. All rights reserved. Contact Us! Privacy Policy.

Exhibit "6"



(index.php)

Anonymous VPN & Proxy Blog

The Latest TorGuard VPN News, How-To's, Security Updates and more.

The best ways to torrent anonymously

Home (<https://torguard.net/blog>) / *The best ways to torrent anonymously*

With IP monitoring firms and lawsuit happy layers policing bittorrent swarms more and more, many torrent users are looking for better ways to keep their personal identity private from the rest of the world. To meet this growing need, we'll give you a quick overview of the top methods to keep yourself safe and download torrents anonymously.

Torrent VPN

Many a BitTorrent user has already found out that using a secure torrent VPN (<http://torguard.net/anonymoustorrentvpn.php>) service is a very good way to stay private on BitTorrent. For just a few dollars monthly, a VPN will route all of your internet traffic through their secure torrent VPN (<http://torguard.net/anonymoustorrentvpn.php>) servers, encrypting all your activity and effectively hiding your IP address from the public. While some providers offer a free VPN plan, most of the time these connections are slow or frequently down due to large amounts of users. For optimum performance and reliability, it's best to use a professional VPN service like TorGuard VPN which offers service for as low as 4.99 a month.

Unlike other types of torrent privacy options, VPN's are not just limited to your BitTorrent traffic, they can also hide the source of all data passing through your connection. TorGuard VPN is one of the most popular torrent vpn services among bittorrent users, but a simple google search should find dozens more. It is highly recommended to do your research about your provider before signing up – make sure to ask if BitTorrent traffic is permitted on their VPN service.

Torrent Proxy

A torrent proxy (<http://torguard.net/anonymoustorrentproxy.php>) is similar to a torrent vpn as they both will hide your IP address on bittorrent. The main difference is a socks5 torrent proxy and a torrent vpn is a proxy only protects one application at a time – like uTorrent, bittorrent, deluge or vuze while a vpn encrypts your entire internet connection. With a torrent proxy you can tunnel all your torrent traffic through a secure server, while leaving the rest of your connection running through your local IP address. This is a good thing if you're connected to a work system or prefer to use a personal IP when browsing certain websites. Before purchasing a torrent proxy it is a good idea to do a fair amount of research into providers. Many torrent proxy companies over crowd users onto their servers driving download speeds to very low levels. When this happens, it completely defeats the reason to use BitTorrent as a means of fast file transfer. Torrent proxy services like TorGuard provide users with access to 20+ torrent proxy (<http://torguard.net/anonymoustorrentproxy.php>) IP's in over three different countries. While using a torrent proxy isn't as fast as using a torrent vpn, TorGuard guarantees fast speeds and no overcrowding on all of their torrent proxy connections.



(index.php)

Support & Help

- [My Account \(/clientarea.php\)](#)
- [Support Center \(/support/\)](#)
- [Getting Started \(/gettingstartedvpn.php\)](#)
- [Submit Ticket \(/submitticket.php\)](#)
- [Downloads \(/downloads.php\)](#)
- [TorGuard Forums \(/forums/\)](#)
- [TorGuard FAQ \(/faq.php\)](#)
- [TorGuard Blog \(/blog/\)](#)
- [Proxy vs VPN \(/proxyvsvpn.php\)](#)

TorGuard Services

- [Buy VPN \(/buy-vpn.php\)](#)
- [WireGuard \(/wireguard.php\)](#)
- [VPN Service \(/vpnservice.php\)](#)
- [Torrent VPN \(/torrent-vpn-service-ip.php\)](#)
- [Android VPN \(/androidvpnservice.php\)](#)
- [Stealth VPN \(/stealth-vpn.php\)](#)
- [iPhone VPN \(/iphonevpnservice.php\)](#)
- [Business VPN \(/business-vpn.php\)](#)

Get 50% off for Life - use promo code: TGLifetime50
BUY NOW! >



[Anonymous Proxy \(/anonymousbittorrentproxy.php\)](#)

[Dedicated IP VPN \(/dedicated-ip-vpn.php\)](#)

TorGuard Links

[VPN Affiliates \(/vpn-reseller-affiliate.php\)](#)

[Whats My IP \(/whats-my-ip.php\)](#)

[DNS Leak Test \(/vpn-dns-leak-test.php\)](#)

[WebRTC Leak Test \(/vpn-webrtc-leak-test.php\)](#)

[Check my Torrent IP \(/checkmytorrentipaddress.php\)](#)

[VPN Network \(/network/\)](#)

[VPN Software \(/vpn-software.php\)](#)

[VPN Reviews \(/vpn-reviews.php\)](#)

[Unblock Websites \(/unblock-websites.php\)](#)

Available on Mobile and Tablet



<https://itunes.apple.com/gb/app/torguard-anonymous-vpn-service/id988743799?mt=8>

The top rated iOS VPN App



https://play.google.com/store/apps/details?id=net.torguard.openvpn.client&hl=en_GB&gl=US

The top rated Android VPN App

Copyright © 2021 TorGuard.net. All rights reserved.

[Terms of Use \(/terms.php\)](#) | [Privacy Policy \(/privacy.php\)](#) | [DMCA \(/dmca.php\)](#) | [Export \(/export.php\)](#)

Exhibit "8"

Client Login Register View Cart

Home Torrent Proxy Anonymous VPN » More Info... Members Area Contact Us

Stay Anonymous on Bittorrent

Ensure privacy with TorGuard

Anonymous Bittorrent Services

How to Anonymize Your BitTorrent Traffic with TorGuard

If you do not have protective measures in place to secure your connection to the torrent cloud, it is just a matter of time before your ISP responds to your downloading activities by throttling your connection or by sending you the infamous "love letter." The worst-case scenario is that they receive a subpoena from an attorney requesting your identity for a potential lawsuit. TorGuard offers proxy and VPN service to ensure your anonymity and security, protecting you from these risks. Our private VPN and torrent proxy tools can keep you completely safe when you use a BitTorrent client.



Traditional measures aren't enough to let you torrent anonymously and stay safe anymore. It is becoming increasingly easy for prying eyes to view torrent traffic. This includes representatives looking to target torrenters with lawsuits. If your ISP throttles BitTorrent traffic and you don't have a tool in place to anonymize your connection, you have an additional problem. As long as an ISP can detect that you are connecting to a BitTorrent cloud, they can throttle your connection to unbearably slow speeds, even if you are accessing perfectly legal downloads.

If you are serious about keeping your download activity private, you should route your BitTorrent connection through an external service. An anonymous VPN can hide your activity to keep "Big Brother" out of your personal business and protect you from your ISP. TorGuard provides BT-focused proxy servers, VPNs, and Anonymous email services to keep you safe and secure while torrenting.

Keep reading to learn how TorGuard works and how to set it up to privatize and anonymize your BitTorrent traffic with TorGuard.

Content on this page requires a newer version of Adobe Flash Player.



How TorGuard Works

When you download or seed a torrent, you connect to several other people. This is called a swarm, and everyone in the swarm can see your computer's IP address. But independent monitoring groups can also join swarms in order to monitor activity and log IP addresses. They can notify your ISP of your doings and use the information for

Client Login

Email

Password

Remember Me

[Request a Password Reset](#)

Quick Navigation

[Portal Home](#)

[Register](#)

[Client Area](#)

[Announcements](#)

[Knowledgebase](#)

[Submit Ticket](#)

[Downloads](#)

[Order](#)

Unblock the Web!

other purposes. Our proxy and VPN services funnel your internet and BitTorrent traffic through another server. Those in Torrent swarm see an IP address from our server that can't be traced back to you. So "prying eyes" can't identify you and share your torrenting information with your ISP, so it has no cause to send you a harrowing letter. TorGuard offers you both a proxy to combat spying and encryption to combat throttling.

It gets better. Hypothetically, snoopers in the swarm could go after TorGuard and request our logs to get the same information about your downloading. But we don't keep any logs of activity on our servers, so there's no trail leading back to you. Someone watching traffic on our servers would simply see them sharing a file, while your ISP only sees you connecting to TorGuard. Everything else is encrypted.

You still have to be careful of going over your ISP's bandwidth cap if they have one.

TorGuard Torrent Proxy and VPN Service Prices

At roughly \$6 per month, and as little as \$4 if you pay for a year in advance, the cost to protect yourself from throttling and potential lawsuits for a year is between \$48 and \$72 per year. On the other hand, settling a lawsuit would cost you thousands of dollars.

TorGuard Anonymous Bittorrent Proxy and VPN Services:

- **Pro VPN Service** - Connect to our VPN service to anonymously encrypt your internet activity from prying eyes. All applications on your computer that utilize your internet connection will become anonymous with just a click of a button; no technical experience is required due to our easy to use VPN software. We allow torrents and p2p connections on all of our servers for no extra charge! Enjoy true internet freedom and anonymity knowing that your sensitive web traffic is securely hidden behind our secure VPN servers.
- **Anonymous Torrent Proxy** - Protect your personal identity when downloading torrents with an anonymous torrent proxy from TorGuard. Cross compatible with any os, our secure socks5 torrent proxy will effectively hide your personal IP address on bittorrent. Installation is easy with our pre-configured torrent client. View our knowledgebase for step by step configurations of all torrent clients – uTorrent, bittorrent, vuze and more! Ensure your IP address is hidden with our FREE check my torrent IP tool!

If you're going to use BitTorrent to share and download files, we highly recommend getting some sort of protection from one of these TorGuard services so you can avoid ISP "love letters" and throttled speeds. Enjoy true internet freedom and anonymity knowing that your sensitive web traffic is securely hidden with TorGuard security and our VPN service.

Unblock the web worldwide!

- ✓ Unlimited Bandwidth
- ✓ Unlimited Speeds
- ✓ Access 100+ IP's
- ✓ Secure Encryption

Company Info

- Contact Us
- TOS Policy
- Privacy Policy
- TorGuard Blog
- DMCA Notice

Privacy Services

- Torrent Proxy
- VPN Service
- Android VPN
- Torrent VPN
- Anonymous Email

TorGuard Links

- FAQ Page
- DNS Leak Test
- Buy DDWRT Routers
- Check my Torrent IP
- Pre-Paid VPN Service

Members Area

- Affiliate System
- Knowledgebase
- Submit Ticket
- Contact Us
- Members Forum



- VPN Service | Torrent Proxy | Bittorrent VPN | VoIP VPN | Unblock Netflix | Unblock Facebook
- How to Bittorrent Anonymously | Anonymous VPN | Check your Torrent IP | Proxy vs VPN | Stealth VPN
- Torrent VPN | iPhone VPN | iPad VPN | Android VPN | Unblock Pandora | Anonymous Proxy

© Copyright TorGuard.net 2013. All rights reserved.