

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF VIRGINIA  
Alexandria Division**

MILLENNIUM FUNDING, INC., SCREEN MEDIA VENTURES, LLC, VOLTAGE HOLDINGS, LLC, MILLENNIUM MEDIA, INC., PARADOX STUDIOS, LLC, DALLAS BUYERS CLUB, LLC, WONDER ONE, LLC, FW PRODUCTIONS, LLC, MILLENNIUM IP, INC., I AM WRATH PRODUCTIONS, INC., FAMILY OF THE YEAR PRODUCTIONS, LLC, AMBI DISTRIBUTION CORP., KILLING LINK DISTRIBUTION, LLC, BADHOUSE STUDIOS, LLC, LF2 PRODUCTIONS, INC., LHF PRODUCTIONS, INC., LAUNDRY FILMS, INC., VENICE PI, LLC, RAMBO V PRODUCTIONS, INC., SPEED KILLS PRODUCTIONS, INC., NIKOLA PRODUCTIONS, INC., BODYGUARD PRODUCTIONS, INC., OUTPOST PRODUCTIONS, INC., HITMAN 2 PRODUCTIONS, INC. and MORGAN CREEK PRODUCTIONS, INC.

Plaintiffs,

v.

SURFSHARK LTD., KEEPSOLID, INC. d/b/a/ VPN UNLIMITED, ZENGUARD GMBH, EXPRESS VPN INTERNATIONAL LTD (a BVI Limited Company), EXPRESS VPN INTERNATIONAL LTD (an Isle of Man Limited Company), VPN CONSUMER NETWORK and VPN CONSUMER NETWORK SERVICES,

Defendants.

Civil Action No. 1:21-cv-00643-RDA-MSN

**JURY TRIAL DEMANDED**

**FIRST AMENDED COMPLAINT**

MILLENNIUM FUNDING, INC., SCREEN MEDIA VENTURES, LLC, VOLTAGE HOLDINGS, LLC, MILLENNIUM MEDIA, INC., PARADOX STUDIOS, LLC, DALLAS

BUYERS CLUB, LLC, WONDER ONE, LLC, FW PRODUCTIONS, LLC, MILLENNIUM IP, INC., I AM WRATH PRODUCTIONS, INC., FAMILY OF THE YEAR PRODUCTIONS, LLC, AMBI DISTRIBUTION CORP., KILLING LINK DISTRIBUTION, LLC, BADHOUSE STUDIOS, LLC, LF2 PRODUCTIONS, INC., LHF PRODUCTIONS, INC., LAUNDRY FILMS, INC., VENICE PI, LLC, RAMBO V PRODUCTIONS, INC., SPEED KILLS PRODUCTIONS, INC., NIKOLA PRODUCTIONS, INC., BODYGUARD PRODUCTIONS, INC., OUTPOST PRODUCTIONS, INC., HITMAN 2 PRODUCTIONS, INC. and MORGAN CREEK PRODUCTIONS, INC. (“Plaintiffs”), by and through their counsel, bring this First Amended Complaint against SURFSHARK LTD. (“Surfshark”), KEEPSOLID, INC. d/b/a VPN Unlimited (“KeepSolid”), ZENGUARD GMBH (“ZenGuard”), EXPRESS VPN INTERNATIONAL LTD. (BVI Limited Company), EXPRESS VPN INTERNATIONAL LIMITED (Isle of Man Company) (both ExpressVPN entities collectively referred to as “ExpressVPN”), VPN CONSUMER NETWORK, and VPN CONSUMER NETWORK SERVICES (collectively “Defendants”) and allege as follows:

## **I. NATURE OF THE ACTION**

1. Plaintiffs bring this action under the United States Copyright Act of 1976, as amended, 17 U.S.C. §§ 101, *et seq.* (the “Copyright Act”), and allege that Defendants are liable directly and secondarily for copyright infringements in violation of 17 U.S.C. §§ 106 and 501, secondarily for violations under the Digital Millennium Copyright Act (“DMCA”), 17 U.S.C. § 1202 and for injunctive relief pursuant to 17 U.S.C. §§ 512(j).

2. Plaintiffs allege that Defendants ExpressVPN, VPN Consumer Network Services and VPN Consumer Network are liable for negligent misrepresentations and fraudulent misrepresentations under Virginia law.

## II. JURISDICTION AND VENUE

3. This Court has subject matter jurisdiction over this action pursuant to 17 U.S.C. §§ 101, *et seq.*, (the Copyright Act), 28 U.S.C. § 1331 (federal question), 28 U.S.C. § 1338 (patents, copyrights, trademarks, and unfair competition), and 28 U.S.C. § 1367 (supplemental jurisdiction).

4. Defendants solicit, transact, or are doing business within this jurisdiction, and have committed unlawful and tortious acts both within and outside this jurisdiction with the full knowledge that their acts would cause injury in this jurisdiction.

5. Particularly, Defendants committed many of the infringing acts complained of herein at servers located in Manassas, Virginia with the full knowledge that their actions were occurring in Virginia.

6. Each of Defendants Surfshark, KeepSolid and ExpressVPN entered into a sales contract with the Virginia headquartered corporation Leaseweb, Inc. (“Leaseweb”) for hosting and network service including leasing servers and Internet Protocol (“IP”) addresses at locations including Leaseweb’s data center in Manassas, Virginia and thus in this District to engage in widespread piracy of Plaintiffs’ copyright protected motion pictures.

7. Upon information and belief, per the terms of conditions of Defendants’ sales contract with Leaseweb, Defendants agreed that all matters arising from the sales contract would be governed by the laws of the Commonwealth of Virginia and that Federal Courts for Prince William County, Virginia shall have exclusive jurisdiction. *See, e.g.*, Sales Contract at ¶28.1 Governing Law and Jurisdiction.

[https://www.leaseweb.com/sites/default/files/Legal/LSW\\_US\\_B2B\\_Sales\\_Schedule%20\\_v1July2021\\_Leaseweb\\_Sales\\_Terms\\_and%20Conditions\\_0.pdf](https://www.leaseweb.com/sites/default/files/Legal/LSW_US_B2B_Sales_Schedule%20_v1July2021_Leaseweb_Sales_Terms_and%20Conditions_0.pdf) [last accessed on Aug. 20, 2021].

8. ExpressVPN does business in the US under the name of its alter ego VPN Consumer Network Services, a Panamanian company and VPN Consumer Network, upon information and belief, a California unregistered DBA.

9. Each of VPN Consumer Network and VPN Consumer Network Services entered into a registration agreement with the Virginia company American Registry of Internet Numbers (“ARIN”) to receive IP addresses.

10. Each of VPN Consumer Network and VPN Consumer Network Services agreed to be governed by the laws of the commonwealth of Virginia and subject to jurisdiction thereof per the registration agreement with ARIN.

11. Plaintiffs’ claims for negligent and fraudulent misrepresentation based upon Virginia law arise from VPN Consumer Network and VPN Consumer Network Services publishing false information in the ARIN Whois records in violation of the registration agreement.

12. KeepSolid prominently advertises the ability of subscribers to use its service to access its server in Virginia.



13. KeepSolid prominently advertises information about the performance of its server in Manassas, Virginia.



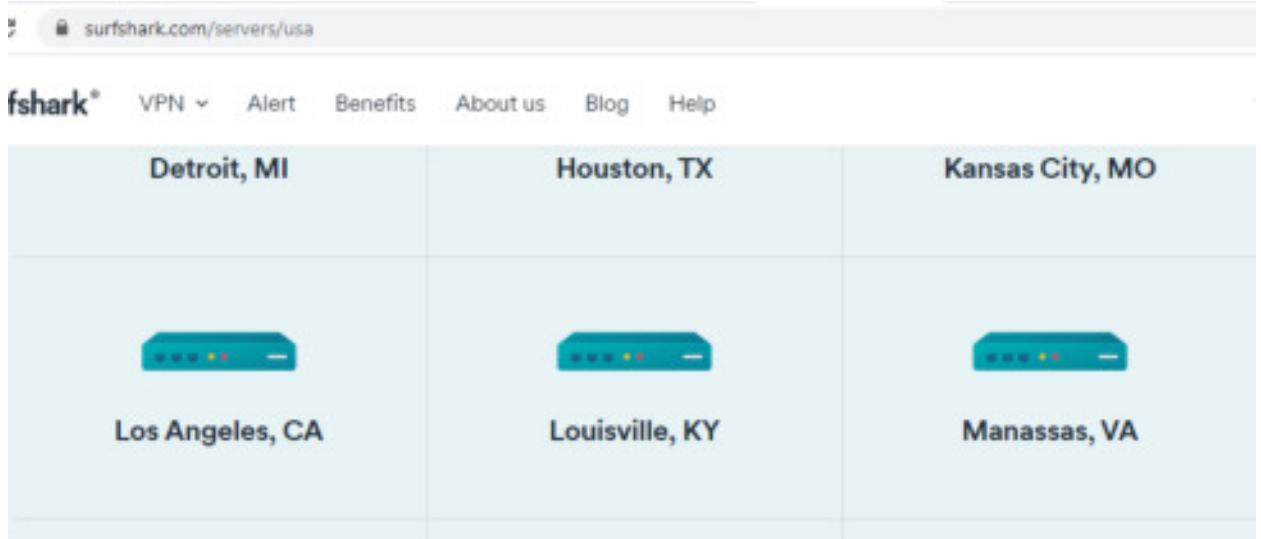
14. KeepSolid has registered the trademark “VPN UNLIMITED” for the service that is the subject of Plaintiffs’ claims with the United States Patent and Trademark Office (“USPTO”) in Alexandria, Virginia and thus in this District.

15. Surfshark registered the trademark “Surfshark” for the service that is the subject of Plaintiffs’ claims with the USPTO in Alexandria, Virginia and thus in this District.

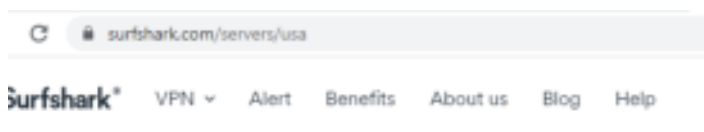
16. ZenGuard attempted to register the trademark “ZenMate” for the service that is the subject of Plaintiffs’ claims with the USPTO in Alexandria, Virginia and thus in this District.

17. ExpressVPN (Isle of Man) registered the trademark “EXPRESSVPN” for the service that is the subject of Plaintiffs’ claims with the USPTO in Alexandria, Virginia and thus in this District.

18. Surfshark prominently advertises the ability of subscribers to use its service to access its server in Virginia.



19. KeepSolid instructs their subscribers nearby to connect to the Virginia server.



20. ExpressVPN (BVI) advertises the ability of subscribers to use its service to access its servers in Washington, DC which, upon information and belief, are actually located in Manassas, VA.

21. In the alternative, the Court has jurisdiction over Defendants Surfshark, ZenGuard, ExpressVPN and VPN Consumer Network Services pursuant to Fed. R. Civ. P. 4(k)(2), the so-called federal long-arm statute, for at least the following reasons: (1) Plaintiffs' claims arise under federal law; (2) Defendants purposely direct its electronic activity into the United States ("US") and target and attract a substantial number of users in the US and, more particularly, this District;

(3) Defendants do so with the manifest intent of engaging in business or other interactions with the US; (4) Defendants are not subject to jurisdiction in any state's courts of general jurisdiction; and (5) exercising jurisdiction is consistent with the US Constitution and laws.

22. Defendants Surfshark, ZenGuard, ExpressVPN and VPN Consumer Network Services purposefully target the US market by using many US-based sources for operating their services and promote their service as providing access to US servers.

23. Defendant Surfshark advertises that it operates hosting and network service at over 500 servers in over 20 US cities.

24. Surfshark uses US payment providers such as Paypal, Amazon Pay, and Google Pay to receive funds in US dollars from US residents.

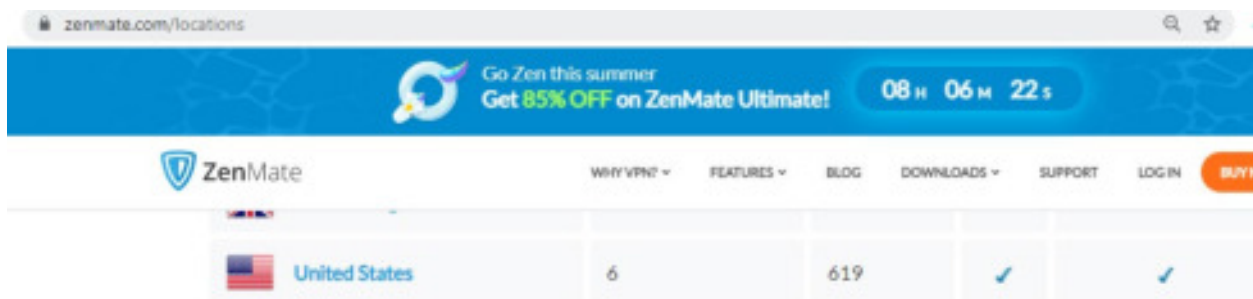
25. Surfshark uses US social media platforms such as TWITTER, FACEBOOK, INSTAGRAM, and YOUTUBE to promote its services to US consumers.

26. Defendant ZenGuard filed an application register its trademark ZenMate with the United States Patent and Trademark Office on May 25, 2017.

27. ZenGuard advertises its service in English from the website zenmate.com.

28. ZenGuard uses the US company CloudFlare for hosting its website.

29. ZenGuard promotes the availability of 619 servers in 6 US cities.



30. ZenGuard uses US payment providers such as Paypal to receive funds in US dollars from US residents.

31. ZenGuard attempted to register the trademark “ZenMate” for the service that is the subject of Plaintiffs’ claims with the United States Patent and Trademark office.

32. ExpressVPN (Isle of Man) and Surfshark registered the trademarks “EXPRESSVPN” and “SURFSHARK”, respectively, for the services that are the subject of Plaintiffs’ claims with the USPTO and thus in the US.

33. To register the trademarks, ExpressVPN (Isle of Man) and Surfshark signed declarations under the penalty of perjury affirming their intent to provide services in the US.

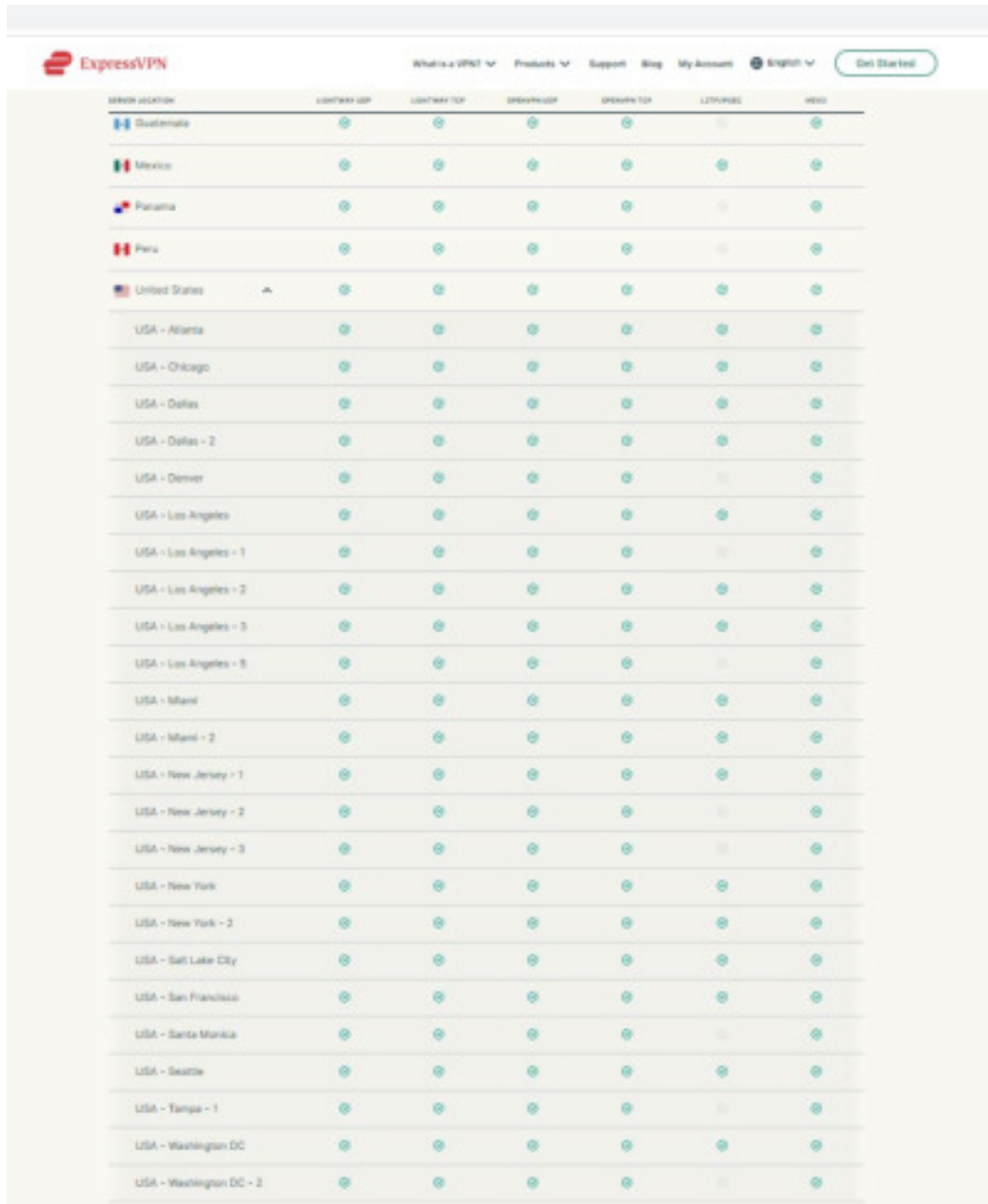
34. ExpressVPN (BVI) uses US payment providers such as Paypal to receive funds in US dollars from US residents.

35. ExpressVPN (BVI) and VPN Consumer Network uses the US company Amazon Web Servers for hosting the websites [expressvpn.com](http://expressvpn.com) and [vpnconsumer.com](http://vpnconsumer.com).

36. Through about October of 2011, ExpressVPN (BVI) used the US domain registrar 1&1 Internet, Inc. in Chesterbrook, PA to register the website domain [expressvpn.com](http://expressvpn.com).

37. ExpressVPN (BVI) promotes the availability of multiple servers in over 20 US locations.





38. Upon information and belief, ExpressVPN secretly does business in the US under the name VPN Consumer Network.

39. ExpressVPN used an address in San Francisco, CA when registering for services with ARIN under the name VPN Consumer Network and the handle VCN-38.

40. ExpressVPN leases servers and IP addresses from the US companies Web2Objects, LLC (New York) and Sharktech, Inc. (Nevada) for its VPN service.

41. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a) - (c) because: (a) all or a substantial part of the events or omissions giving rise to the claims occurred in this District; and/or (c) Defendants are subject to the court's personal jurisdiction with respect to the present action. Additionally, venue is proper in this District pursuant 28 U.S.C. § 1400(a) (venue for copyright cases), because the Defendants or Defendants' agents resides and/or can be found in this District.

### **III. PARTIES**

#### **A. The Plaintiffs**

42. The Plaintiffs are owners of the copyrights for the motion pictures (hereafter: "Works"), respectively, as shown in Exhibit "1".

43. Each of Plaintiffs MILLENNIUM FUNDING, INC., MILLENNIUM MEDIA, INC., MILLENNIUM IP, INC., LF2 PRODUCTIONS, INC., LHF PRODUCTIONS, INC., BODYGUARD PRODUCTIONS, INC., RAMBO V PRODUCTIONS, INC., NIKOLA PRODUCTIONS, INC., OUTPOST PRODUCTIONS, INC., and HITMAN 2 PRODUCTIONS, INC. is a Nevada corporation with its principal place of business at 318 N. Carson Street, Ste 208, Carson City, NV 89701.

44. Plaintiff SCREEN MEDIA VENTURES, LLC is a Delaware limited liability company with its principal place of business at 800 Third Ave., 3rd Floor, New York, NY 10022.

45. Plaintiff VOLTAGE HOLDINGS, LLC is a Nevada limited liability company with its principal place of business at 116 N. Robertson Blvd, Suite 200, Los Angeles, CA 90048.

46. Plaintiff PARADOX STUDIOS, LLC is a Delaware limited liability company with its principal place of business at 919 North Market Street, Suite 950 Wilmington, DE 19801.

47. Plaintiff DALLAS BUYERS CLUB, LLC is a Texas limited liability company with its

principal place of business at 7 Switchbud Pl., Ste 192, The Woodlands, TX 77380.

48. Plaintiff WONDER ONE, LLC is a Wyoming limited liability company with its principal place of business at 4164 Weslin Ave. Sherman Oaks, CA 91423.

49. Plaintiff FW PRODUCTIONS, LLC is a California limited liability company with its principal place of business at 9454 Wilshire Blvd., Suite M-16 Beverly Hills, CA 90212.

50. Plaintiff I AM WRATH PRODUCTIONS, INC. is a California corporation with its principal place of business at 1901 Ave of the Stars Suite 1050, Los Angeles, CA 90067.

51. Plaintiff FAMILY OF THE YEAR PRODUCTIONS, LLC is a Louisiana limited liability company with its principal place of business at Baton Rouge, LA.

52. Plaintiff AMBI DISTRIBUTION CORP. is a Delaware corporation with its principal place of business at 3415 S. Sepulveda Blvd., 11th Fl. Los Angeles, California 90034.

53. Plaintiff KILLING LINK DISTRIBUTION, LLC is a California limited liability company with its principal place of business at 9190 Olympic Blvd. Suite 400, Beverly Hills, CA 90212.

54. Plaintiff BADHOUSE STUDIOS, LLC is a Wyoming limited liability company with its principal place of business at 8265 Sunset Blvd., Suite 107, West Hollywood, CA 90046.

55. Plaintiff LAUNDRY FILMS, INC. is a California corporation with its principal place of business in Venice, California.

56. Plaintiff VENICE PI, LLC is a California limited liability company with its principal place of business at 116 N Robertson Blvd Ste #200, Los Angeles, CA 90048.

57. Plaintiff SPEED KILLS PRODUCTIONS, INC. is a Wyoming corporation with its principal place of business at 8265 Sunset Blvd., Suite 107 West Hollywood, CA 90046.

58. Plaintiff MORGAN CREEK PRODUCTIONS, INC. is a Delaware corporation

with its principal place of business at 10 E Lee St # 2705, Baltimore, MD 21202.

59. Plaintiffs are producers of popular motion pictures currently available for sale in online and brick and mortar retail stores. Many of these critically acclaimed motion pictures were released in theaters throughout the world and feature A-list actors such as Matthew McConaughey, Samuel Jackson, Ryan Reynolds, Sylvester Stallone, Nicholas Cage, and Angela Basset, among others.

60. Plaintiffs invested significant financial resources, time and effort in making and marketing these motion pictures based upon the expectation that they would have an opportunity to get a return on their investment from rentals and sales. Massive piracy of these motion pictures by Defendants and their subscribers have hindered this opportunity.

#### **B. The Defendants**

61. Defendant Surfshark is a limited company organized under the laws of the British Virgin Islands with its principal place of business in Tortola, British Virgin Island.

62. Defendant KeepSolid is a corporation organized under the laws of New York with its principal place of business in New York, New York.

63. KeepSolid does business under the registered US trademark “VPN Unlimited”.

64. Defendant ZenGuard is a fictional entity organized, upon information and belief, under the laws of Germany.

65. ZenGuard does business under the name “ZenMate”.

66. Defendant ExpressVPN (BVI) is, upon information and belief, a limited company organized under the laws of the British Virgin Islands with its principal place of business in Tortola, British Virgin Island.

67. Defendant ExpressVPN (Isle of Man) is, upon information and belief, a limited company organized under the laws of the Isle of Man with its principal place of business in Glen Vine, Isle of Man.

68. Defendant VPN Consumer Network is, upon information and belief, a California company.

69. Defendant VPN Consumer Network Services is, upon information and belief, a Panamanian company.

70. Upon information and belief, the same individuals/entities own ExpressVPN (BVI), ExpressVPN (Isle of Man), VPN Consumer Network Services and VPN Consumer Network.

71. Upon information and belief, ExpressVPN (BVI) and ExpressVPN (Isle of Man) are mere alter egos of each other and therefore are referred to collectively as ExpressVPN.

72. Upon information and belief, VPN Consumer Network Services and VPN Consumer Network are mere alter egos of each other and of ExpressVPN.

73. There is such a unity of interest between ExpressVPN (BVI), ExpressVPN (Isle of Man), VPN Consumer Network Services and VPN Consumer Network that the individuality, or separateness, of ExpressVPN (BVI), ExpressVPN (Isle of Man), VPN Consumer Network Services and VPN Consumer Network have ceased, and the facts are such that an adherence to the fiction of the separate existence of ExpressVPN (BVI), ExpressVPN (Isle of Man), VPN Consumer Network Services and VPN Consumer Network would, under the particular circumstances, sanction a fraud or promote injustice.

74. ExpressVPN uses the VPN Consumer Network and VPN Consumer Network Services entities to commit fraudulent misrepresentations.

75. VPN Consumer Network and VPN Consumer Network Services allocate/reassign IP addresses to ExpressVPN but intentionally publishes false ARIN Whois records to show that VPN Consumer Network Services (in Panama) is the proper abuse contact.

76. Accordingly, rightsholders such as Plaintiffs are hindered from sending notices directly to ExpressVPN.

77. Non-party Leaseweb is a corporation organized under the laws of Delaware with its principal place of operations in Manassas, Virginia.

78. Leaseweb operates datacenters and provides hosting services, IP addresses, Internet access, dedicated servers and co-location to its customers at its data centers.

79. Defendants are customers of Leaseweb.

80. Defendants provide Virtual Private Network (“VPN”) services to their subscribers.

81. A VPN is a type of Internet Service that provides access to the Internet. A conventional ISP will assign its subscriber an IP address and log the subscriber’s activities on the Internet while using the assigned IP address. In comparison, many VPN providers provide their subscribers “anonymous” usage by, for example, not logging subscriber access, assigning the subscriber IP addresses that are simultaneously shared among many users, and/or encrypting traffic.

82. Defendants promote their VPN services as a tool that can be used to pirate copyright protected content without getting caught.

83. Defendants even partner with notorious movie piracy websites to promote their VPN service as an essential tool for movie piracy.

84. Emboldened by Defendants’ promises that their identities cannot be disclosed, Defendants’ subscribers use the VPN services not only to engage in widespread movie piracy, but

other outrageous conduct such as posting messages in support of white supremacy, sharing child pornography, encouraging murder and even committing murder.

85. An unknown ExpressVPN subscriber used the VPN services to hide details concerning the assassination of the Russian Ambassador to Turkey, Andrei Karlov in 2017. *See* <https://www.comparitech.com/blog/vpn-privacy/expressvpn-server-seized-in-turkey-verifies-no-logs-claim/> [last accessed on Aug. 24, 2017].

86. ExpressVPN used this tragic incident to tout its VPN service by bragging that law enforcement could not find information to locate the murder suspects even though their server was seized. *See* <https://torrentfreak.com/expressvpn-anonymous-review/> [last accessed on Aug. 24, 2017] (“Not storing any sensitive information also protects user privacy and security in the event of law enforcement gaining physical access to servers. This was proven in a high-profile case in Turkey in which law enforcement seized a VPN server leased by ExpressVPN but could not find any server logs that would enable investigators to link activity to a user or even determine which users, or whether a specific user, were connected at a given time”).

87. ExpressVPN subscriber Frank Beyer admitted to using the VPN service in connection with the disgusting act of downloading sexual videos of prepubescent children. *See United States of America v. Frank Richard Beyer*, 0:19-cr-60360-RAR (S.D. FL), Affidavit of Nicholas P. Masters in Support of Criminal Complaint [Doc. #1] at ¶20 (“He also admitted to...using a Virtual Private Network...offered through ExpressVPN...”)

88. Upon information and belief, Frank Beyer also used the ExpressVPN service to share copies of copyright protected Works including *Angel Has Fallen*.

89. Surfshark subscriber using username “Harry S Cornhole” posted the following outrageous message using the Disqus forum on 9/9/2020 from IP address 192.111.134.213 (of Total Server Solutions and reallocated/reassigned to Surfshark):

**“Anybody can murder another person at least once before getting caught.”**

90. The same Surfshark subscriber posted the following series of outrageous messages using the Disqus forum on 9/6/2020 from IP address 45.43.14.76 (of Tier.Net and reallocated/reassigned to Surfshark):

**“You do realize that Homeless BLM ANTIFA etc, are all the same to normal people. A Potpourri of Scum.”**

**“A normal person thinks homeless antifa and blm are all the same. Gross!”**

**“Bring your children with you downtown. When you start killing those homeless, blm, and antifa losers, you will have a great excuse for why you did it. Truck will become a lawnmower.”**

91. The Surfshark subscriber posted the following series of outrageous messages using the Disqus forum on 9/6/2020 from IP address 212.103.49.148 (of Tier.Net and reallocated/reassigned to Surfshark):

**“Every time these losers die to a bullet, the Taxpayer saves money.”**

**“What happens if a person throws a flare in a mailbox? I wonder if those votes would be counted? Most mailboxes are in liberal neighborhoods. Not many in the country...”**

92. The Surfshark subscriber chose an image of a Caucasian hand making the “ok” hand gesture as the icon representing his username.





Harry S Cornhole · a year ago

You do realize that Homeless BLM ANTIFA etc, are all the same to normal people. A Potpourri of Scum.

1 ^ | v 3 · Reply · Share >

93. The Anti-Defamation League states that the hand gesture chosen by this Surfshark subscriber as the icon for his username is a common expression indicating support for white supremacy. See <https://www.adl.org/education/references/hate-symbols/okay-hand-gesture> [last accessed on Aug. 22, 2021].

94. The Surfshark subscriber purposely chose this username to show his disdain towards Plaintiffs' counsel who is African American, named Kerry S. Culpepper and resides in Hawaii for representing copyright holders.

95. On Jan. 27, 2021, the Surfshark subscriber posted a message on the website TorrentFreak suggesting that Plaintiffs' counsel be murdered.

**“Culpepper appears to be wanting an early funeral. Folks will murder for just about anything these days.”**

96. The following day the Surfshark subscriber posted again from IP address 154.16.168.185 with detailed description of Plaintiffs' counsel.

97. On Feb. 2, 2020, the Surfshark subscriber used the Harry S Cornhole username to state “Kerry Culpepper the Hawaiian Negro...”.



Harry S Cornhole · 5 days ago

Kerry Culpepper the Hawaiian Negro. Can't be hard to spot.

^ | v · Reply · Share >

#### IV. JOINDER

98. Pursuant to Fed. R. Civ. P. 20(a)(1), each of the Plaintiffs are properly joined because, as set forth in detail above and below, the Plaintiffs assert: (a) a right to relief arising out of the same transaction, occurrence, or series or transactions, namely Defendants' use of the services of Leaseweb to infringe Plaintiffs' copyright protected Works; and (b) that there are common questions of law and fact.

99. Pursuant to Fed. R. Civ. P. 20(a)(2), each of the Defendants are properly joined because, as set forth in more detail below, Plaintiffs assert that the infringements complained of herein by each of the Defendants (a) arises out of the same transaction, occurrence, or series of transactions or occurrences, and (b) there are common questions of law and fact. That is, (i) Defendants obtain servers for their essential services from Leaseweb and promote their VPN service for the purpose of engaging in piracy, and (ii) Defendants' subscribers use the VPN service to infringe Plaintiffs' copyrights as instructed and encouraged to do by Defendants.

## **V. FACTUAL BACKGROUND**

### ***A. The Plaintiffs Own the Copyrights to the Works***

100. The Plaintiffs are the owners of the copyright in the Works, respectively. The Works are the subjects of copyright registrations, and this action is brought pursuant to 17 U.S.C. § 411. *See* Exhibit "1".

101. The Plaintiffs are either the original authors by work for hire agreements or have become owners from valid assignments.

102. Each of the Works are motion pictures currently offered for sale in commerce.

103. Defendants had notice of Plaintiffs' rights through at least the credits indicated in the content of the motion pictures which bore proper copyright notices.

104. Defendants also had notice of Plaintiffs' rights through general publication and advertising associated with the motion pictures, and packaging and copies, each of which bore a proper copyright notice.

105. Defendants also had notice of Plaintiffs' rights through notices Plaintiffs' agent sent to Leaseweb's abuse contact, which Leaseweb promptly forwarded to them as discussed below.

***B. Defendants directly infringe Plaintiffs' Copyrights***

106. Defendants distribute, reproduce and/or publicly perform (stream) Plaintiffs' Works from servers they leased from data centers such as Leaseweb for these subscribers in violation of Plaintiffs' exclusive rights.

107. Defendants advertise their service for allowing their subscribers to bypass regional restrictions of streaming platforms to stream copies of copyright protected content including Plaintiffs' Works from locations Plaintiffs have not authorized the platform to stream the Works.

108. Defendant KeepSolid advertises its service for allowing its subscribers not located in the United States to stream content restricted to United States locations to their non-United States location in violation of Plaintiffs' exclusive rights to authorize distribution, public performance and/or reproduction of their Works. *See* <https://www.vpnunlimited.com/help/streaming> [last accessed on Aug. 22, 2021].

---

## **Access the US Netflix with VPN Unlimited®**

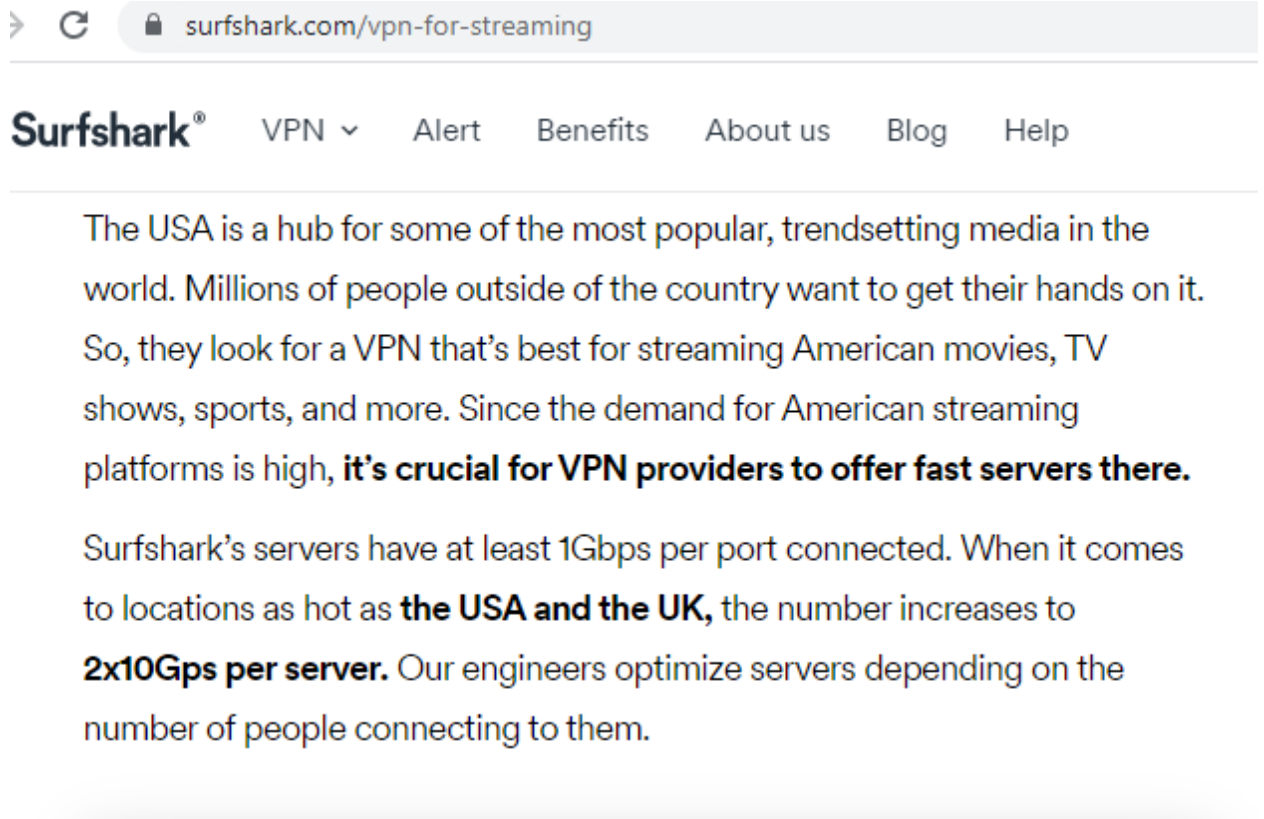
If you are the biggest fan of American Netflix catalogue who lives abroad, VPN Unlimited® will save your day. Our app bypasses Netflix VPN blocks and provides you with the widest selection of movies and shows.

What to watch on Netflix with KeepSolid VPN Unlimited®?

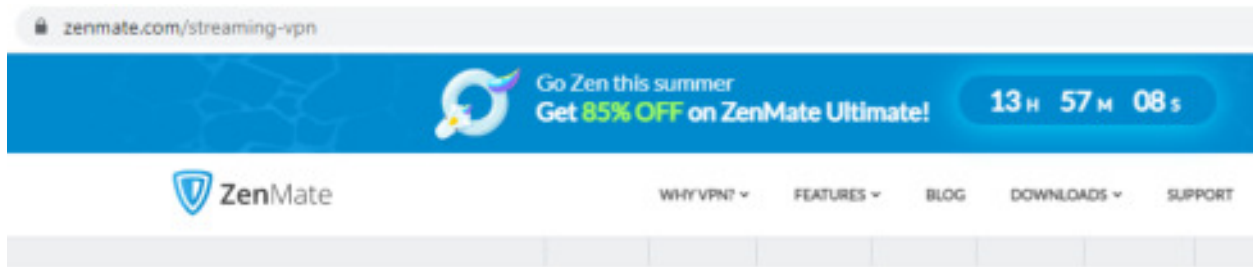
**Top 3 TV Shows:**

**Top 3 movies:**

109. Defendant Surfshark advertises its service for allowing its subscribers not located in the United States to stream content restricted to United States locations to their non-United States location in violation of Plaintiffs' exclusive rights to authorize distribution, public performance and/or reproduction of their Works. *See* <https://surfshark.com/vpn-for-streaming> [last accessed on Aug. 22, 2021].



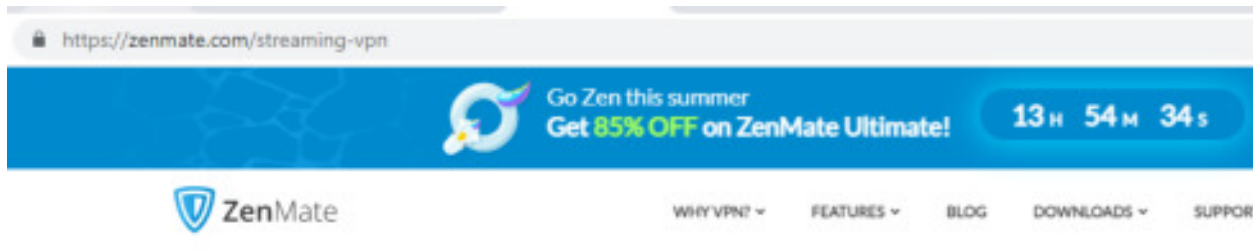
110. Defendant ZenGuard advertises its service for allowing its subscribers not located in the United States to stream content restricted to United States locations to their non-United States location in violation of Plaintiffs' exclusive rights to authorize distribution, public performance and/or reproduction of their Works. *See* <https://zenmate.com/streaming-vpn> [last accessed on Aug. 22, 2021].



## Why Use a VPN For Streaming?

Streaming services are great. But sometimes they can be a pain. Who hasn't been annoyed by YouTube's "this video isn't available in your area" message? How many times have you seen an article about Netflix's newest releases only to later discover they won't be available in your country?

Luckily, there's a simple solution to watch your favorite shows, movies, sporting events, and unblock YouTube videos even if they're blocked in your country. It's called a virtual private network. Try out ZenMate VPN for free. You'll be able to override streaming geo-restrictions and discover all the content you're missing out on right now.

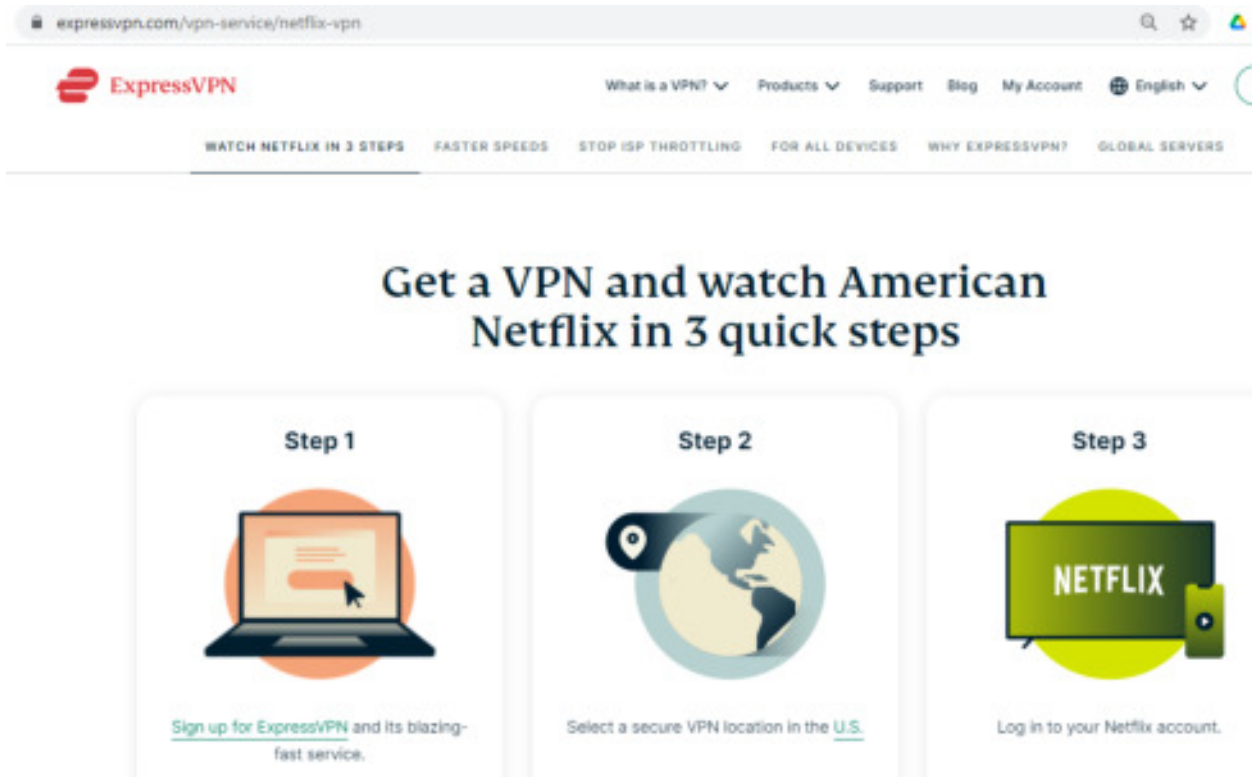


## What Streaming Websites Can You Unblock?

- ✓ Netflix US
- ✓ Netflix FR
- ✓ Netflix DE
- ✓ Netflix UK
- ✓ YouTube
- ✓ HBO Now
- ✓ BBC iPlayer
- ✓ Amazon Prime
- ✓ 7TV
- ✓ ORF
- ✓ Globo
- ✓ Yle
- ✓ Globo Sportiv
- ✓ ZDF
- ✓ ARD
- ✓ Fox Sport (Brazil)
- ✓ Comedy Central DE
- ✓ Zattoo DE

111. ExpressVPN advertises its service for allowing its subscribers not located in the United States to stream content restricted to United States locations to their non-United States

location in violation of Plaintiffs’ exclusive rights to authorize distribution, public performance and/or reproduction of their Works. See <https://www.expressvpn.com/vpn-service/netflix-vpn> [last accessed on Aug. 24, 2021].



***1. Defendants’ subscribers installed a BitTorrent Client onto his or her Computer***

112. Defendants’ subscribers use BitTorrent to infringe Plaintiffs’ exclusive rights of reproduction and distribution.

113. BitTorrent is one of the most common peer-to-peer file sharing protocols (in other words, set of computer rules) used for distributing large amounts of data.

114. The BitTorrent protocol’s popularity stems from its ability to distribute a large file without creating a heavy load on the source computer and network. In short, to reduce the load on the source computer, rather than downloading a file from a single source computer (one computer directly connected to another), the BitTorrent protocol allows users to join a “swarm” of host

computers to download and upload from each other simultaneously (one computer connected to numerous computers).

115. A BitTorrent Client is a software program that implements the BitTorrent Protocol. There are numerous such software programs which can be directly downloaded from the Internet.

116. Once installed on a computer, the BitTorrent Client serves as the user's interface during the process of uploading and downloading data using the BitTorrent protocol.

117. Defendants' subscribers installed a BitTorrent Client such as "Popcorn Time" as promoted and instructed by Defendants onto their respective computers.

118. Popcorn Time has been referred to in the news media as "Netflix for pirates". <http://fortune.com/2016/02/26/popcorn-time-netflix-pirates/> [accessed on March 1, 2021].

119. The United States Trade Representative ("USTR") placed the Popcorn Time promoted by LiquidVPN on a list of examples of Notorious Markets engaged in and facilitating substantial piracy. *See* USTR, 2020 Review of Notorious Markets, Jan. 14, 2021, pg. 26, Available at [https://ustr.gov/sites/default/files/files/Press/Releases/2020%20Review%20of%20Notorious%20Markets%20for%20Counterfeiting%20and%20Piracy%20\(final\).pdf](https://ustr.gov/sites/default/files/files/Press/Releases/2020%20Review%20of%20Notorious%20Markets%20for%20Counterfeiting%20and%20Piracy%20(final).pdf) [last accessed on May 24, 2021].

120. Popcorn Time provides an interface so that users can easily copy and share copies of copyright protected content, including Plaintiffs'.

121. The home interface of Popcorn Time includes a collection of title art of popular motion pictures and a search bar where a user can enter words associated with a copyright protected motion picture they wish to copy.

122. Simply entering words associated with a motion picture automatically generates a



pull down tab below the search bar with a narrowed selection of motion pictures associated with the words.

123. Defendants instruct their subscribers how to setup their BitTorrent clients to use their VPN services. See <https://zenguard.zendesk.com/hc/en-us/articles/360001620757-How-to-torrent-with-ZenMate-5>; <https://surfshark.com/blog/utorrent-vpn> (Surfshark instructions how to setup BitTorrent Client uTorrent); <https://www.vpnunlimited.com/help/torrents> (instructions on different operating systems).

## ***2. The Initial Seed, Torrent, Hash and Tracker***

124. A BitTorrent user that wants to upload the new file, known as an “initial seeder,” starts by creating a “torrent” descriptor file using, for example, the Client he or she installed onto his or her computer.

125. The initial user or seeder of a file used a process referred to as “ripping” to create a copy of motion pictures from either Blu-ray or legal streaming services.

126. The initial seeder often modifies the file title of the Work to include a wording such as “FGT”, “RARBG” or “YTS” in the title of the torrent files and file copies in order to enhance a reputation for the quality of his or her torrent files and attract users to his or her piracy website.

127. The Client takes the target computer file, the “initial seed,” here the copyrighted Work, and divides it into identically sized groups of bits known as “pieces.”

128. The Client then gives each one of the computer file’s pieces, in this case, pieces of the copyrighted Works, a random and unique alphanumeric identifier known as a “hash” and records these hash identifiers in the torrent file.

129. When another peer later receives a particular piece, the hash identifier for that piece is compared to the hash identifier recorded in the torrent file for that piece to test that the piece is

error-free. In this way, the hash identifier works like an electronic fingerprint to identify the source and origin of the piece and that the piece is authentic and uncorrupted.

130. Torrent files also have an "announce" section, which specifies the URL (Uniform Resource Locator) of a "tracker," and an "info" section, containing (suggested) names for the files, their lengths, the piece length used, and the hash identifier for each piece, all of which are used by Clients on peer computers to verify the integrity of the data they receive.

131. The "tracker" is a computer or set of computers that a torrent file specifies and to which the torrent file provides peers with the URL address(es).

132. The tracker computer or computers direct a peer user's computer to other peer user's computers that have particular pieces of the file, here the copyrighted Work, on them and facilitates the exchange of data among the computers.

133. Depending on the BitTorrent Client, a tracker can either be a dedicated computer (centralized tracking) or each peer can act as a tracker (decentralized tracking.)

134. Initial seeders use Defendants' services to seed copies of Plaintiffs' Works to torrent sites such as 1337x.

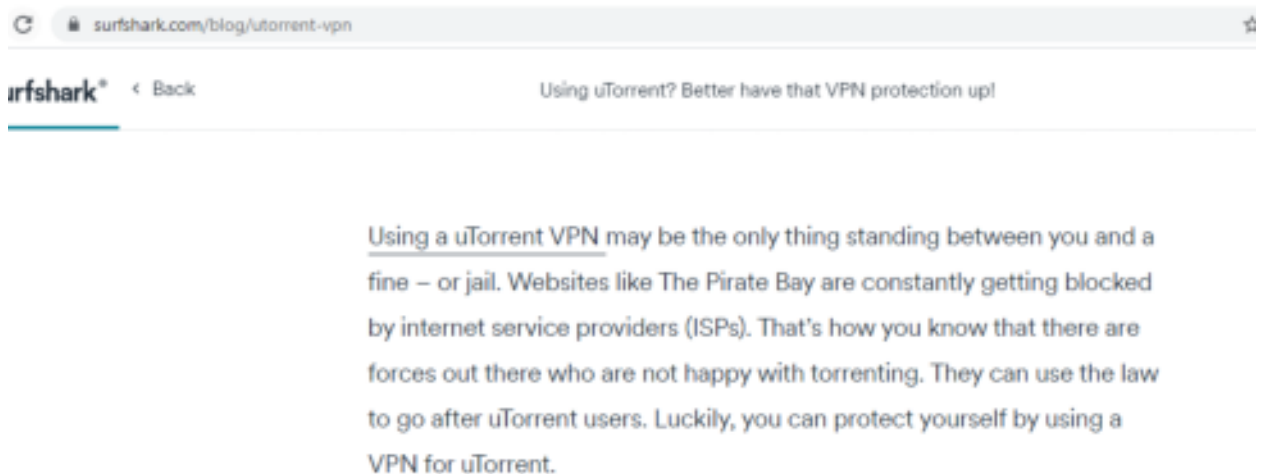
135. An initial seeder seeded copies of *London Has Fallen*, *The Mechanic: Resurrection*, *All Eyez on Me*, and *The Hitman's Bodyguard* from IP address 207.244.78.5 (of Zenguard).

### ***3. Torrent Sites***

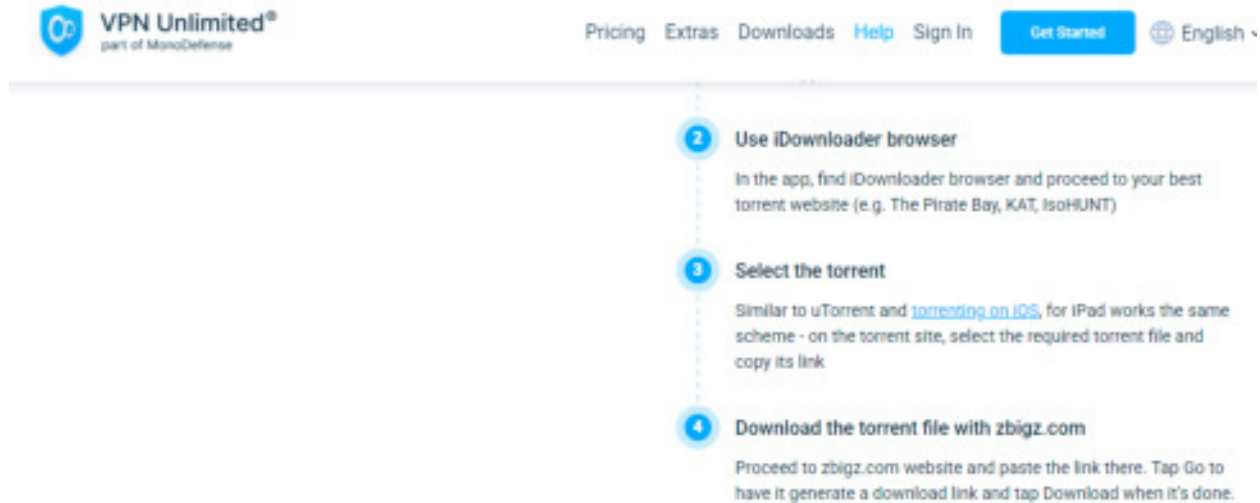
136. "Torrent sites" are websites that index torrent files that are currently being made available for copying and distribution by entities using the BitTorrent protocol such as servers controlled by Defendants. There are numerous torrent websites including the notorious Pirate Bay, YTS, 1337x and RARBG websites.

137. The Pirate Bay, YTS, 1337x and RARBG websites were noted by the USTR as examples of Notorious Markets defined as an online marketplace reportedly engaged in and facilitating substantial piracy. See USTR, 2014 Out-of-Cycle Review of Notorious Markets, Mar. 5, 2015, pg. 17, Available at [https://ustr.gov/sites/default/files/2014%20Notorious%20Markets%20List%20-%20Published\\_0.pdf](https://ustr.gov/sites/default/files/2014%20Notorious%20Markets%20List%20-%20Published_0.pdf) [last accessed on May 7, 2021]; USTR, 2018 Out-of-Cycle Review of Notorious Markets, April 2019, pgs. 24, 27-28 Available at [https://ustr.gov/sites/default/files/2018\\_Notorious\\_Markets\\_List.pdf](https://ustr.gov/sites/default/files/2018_Notorious_Markets_List.pdf) [accessed on May 7, 2021].

138. Defendant Surfshark promotes its service as being able to allow subscribers to access Pirate Bay without “...a fine – or jail.” <https://surfshark.com/blog/utorrent-vpn> [last accessed on Aug. 22, 2021].



139. Defendant KeepSolid encourages its users to access torrent sites including the Pirate Bay. <https://www.vpnunlimited.com/help/torrents/how-to-download-torrents-on-ipad> [last accessed on Aug. 22, 2021] (“proceed to your best torrent website (e.g. The Pirate Bay, KAT, IsoHUNT)”).



***4. Defendants’ subscribers access the torrent sites from IP addresses received from Leaseweb***

140. Defendants’ subscribers accessed torrent sites including the YTS website to upload and download Plaintiffs’ copyrighted Works from IP addresses provided by Defendants. *See* Decl. of Tayah Durnan.

***5. The Peer Identification***

141. The BitTorrent Client will assign an identification referred to as a Peer ID to the subscriber’s computer so that it can share content (here the copyrighted Work) with other peers.

***6. Uploading and Downloading a Work Through a BitTorrent Swarm***

142. Once the initial seeder has created a torrent and uploaded it onto one or more torrent sites, then other peers begin to download and upload the computer file to which the torrent is linked (here the copyrighted Work) using the BitTorrent protocol and BitTorrent Client that the peers installed on their computers.

143. The BitTorrent protocol causes the initial seeder’s computer to send different pieces of the computer file, here the copyrighted Works, to the peers seeking to download the computer file. Defendants transmit the pieces to the peers from the initial seeder.

144. Once a peer receives a piece of the computer file, here a piece of the copyrighted Work, it starts transmitting that piece to the other peers. Defendants transmit the pieces to the peers for the other peers.

145. In this way, all of the peers and seeders are working together in what is called a “swarm.”

146. Here, the Defendants’ subscribers participated in a swarm and directly interacted and communicated with other members of the swarm through digital handshakes, the passing along of computer instructions, uploading and downloading, and by other types of transmissions, Plaintiffs’ Works.

147. Defendants distributed their subscribers’ transmissions to other members of the swarm.

148. Once a peer has downloaded the full file, the BitTorrent Client reassembles the pieces and the peer is able to view the movie. Also, once a peer has downloaded the full file, that peer becomes known as “an additional seed,” because it continues to distribute the torrent file, here the copyrighted Work.

***7. The Plaintiffs’ Computer Investigator Identified Defendants’ IP Addresses as Participants in Swarms That Were Distributing Plaintiffs’ Copyrighted Works.***

149. The Plaintiffs retained Maverickeye UG (“MEU”) to identify the IP addresses that are being used by those people that are using the BitTorrent protocol and the Internet to reproduce, distribute, display or perform the Plaintiff’s copyrighted Work.

150. MEU used forensic software to enable the scanning of peer-to-peer networks for the presence of infringing transactions.

151. MEU extracted the resulting data emanating from the investigation, reviewed the evidence logs, and isolated the transactions and the IP addresses associated therewith for the files identified by the SHA-1 hash value of the Unique Hash Number.

152. For example, the IP addresses 172.241.251.164, 207.244.76.224, and 207.244.76.228, Unique Hash Numbers, and hit dates contained in Exhibit “2” accurately reflect what is contained in the evidence logs.

153. Upon information and belief, the IP addresses 172.241.251.164, 207.244.76.224, and 207.244.76.228 were assigned/reallocated from Leaseweb to KeepSolid.

154. The logged information in Exhibit “2” show that Defendant KeepSolid distributed pieces of the Plaintiffs’ copyrighted Works identified by the Unique Hash Number from IP addresses provided by Leaseweb.

155. Defendant KeepSolid’s subscribers connected from the identified IP addresses in Exhibit “2” to the investigative server from the servers Defendant KeepSolid leased from Leaseweb in order to transmit a full copy, or a portion thereof, of a digital media file identified by the Unique Hash Number.

156. MEU’s agent analyzed each BitTorrent “piece” distributed by the IP addresses listed on Exhibit “2” and verified that re-assembly of the pieces using a BitTorrent Client results in a fully playable digital motion picture of the Works.

157. MEU’s agent viewed the Works side-by-side with the digital media file that correlates to the Unique Hash Number and determined that they were identical, strikingly similar or substantially similar.

***C. The Operator of the YTS website confirmed that the subscribers downloaded torrent files for copying the Work from the YTS website.***

158. The YTS website operator maintained records of activity of registered user accounts. *See* Exhibit “3” at pg. 71 (Certificate of Authenticity).

159. As shown in Exhibit “3”, the records include the email address of the registered user account, the torrent files the registered account downloaded, the IP address from where the registered user accessed the YTS website, and the time.

160. The records show Defendants’ subscribers downloaded the torrent files for reproducing Plaintiffs’ motion pictures such as *The Brass Teapot*, *Hellboy*, *Rambo V: Last Blood*, *Angel Has Fallen*, *London Has Fallen*, *2 Guns*, *And So It Goes*, *Beyond a Reasonable Doubt*, *Flypaper*, *Lone Survivor*, *The Hurricane Heist*, *The Last Full Measure*, *The Ledge*, *Universal Soldier Day of Reckoning*, and *I Feel Pretty* from IP addresses Leaseweb assigned to Defendants Surfshark, Keepsolid, ZenGuard and ExpressVPN and in, some cases, in Manassas, Virginia.

***D. Defendants distributed copies of Plaintiffs’ Works.***

161. Defendants distributed copies of each of Plaintiffs’ Works over network connections to other peers in the swarm from IP addresses allocated from Leaseweb and other data service providers with file names that included modified copyright management information (“CMI”) to promote other piracy sources.

162. For example, Surfshark distributed copies of the motion pictures *Ava* from IP addresses 45.43.14.76, 192.111.134.213, 198.8.80.88 and 154.16.168.185 by the file names *Ava* (2020) [1080p] [WEBRip] [5.1] [YTS.MX]; *Ava* (2020) [720p] [WEBRip] [YTS.MX]; *Ava.2020.1080p.BluRay.H264.AAC-RARBG* at or near the same time the Surfshark subscriber “Harry S. Cornhole” used the same IP addresses to post messages in support of using YTS for piracy.

163. For example, KeepSolid distributed copies of Plaintiffs by the following file names from just IP address 207.244.76.228: Speed Kills (2018) [BluRay] [720p] [YTS.AM]; Hunter Killer (2018) [BluRay] [1080p] [YTS.AM]; Hellboy (2019) [WEBRip] [720p] [YTS.LT]; Future World (2018) [BluRay] [720p] [YTS.AM]; and Hellboy.2019.1080p.WEBRip.x264-RARBG.

164. For example, ExpressVPN distributed copies of the Works of Plaintiffs by the following file names from just IP address 104.143.92.63: Shock And Awe (2017) [WEBRip] [1080p] [YTS.AM]; All Eyez On Me (2017) [1080p] [YTS.AG]; I Feel Pretty (2018) [WEBRip] [720p] [YTS.AM]; The.Outpost.2020.720p.GPLAY.WEBRip.900MB.x264-GalaxyRG[TGx]; Rambo Last Blood (2019) [BluRay] [1080p] [YTS.LT] and Rambo Last Blood (2019) [BluRay] [720p] [YTS.LT].

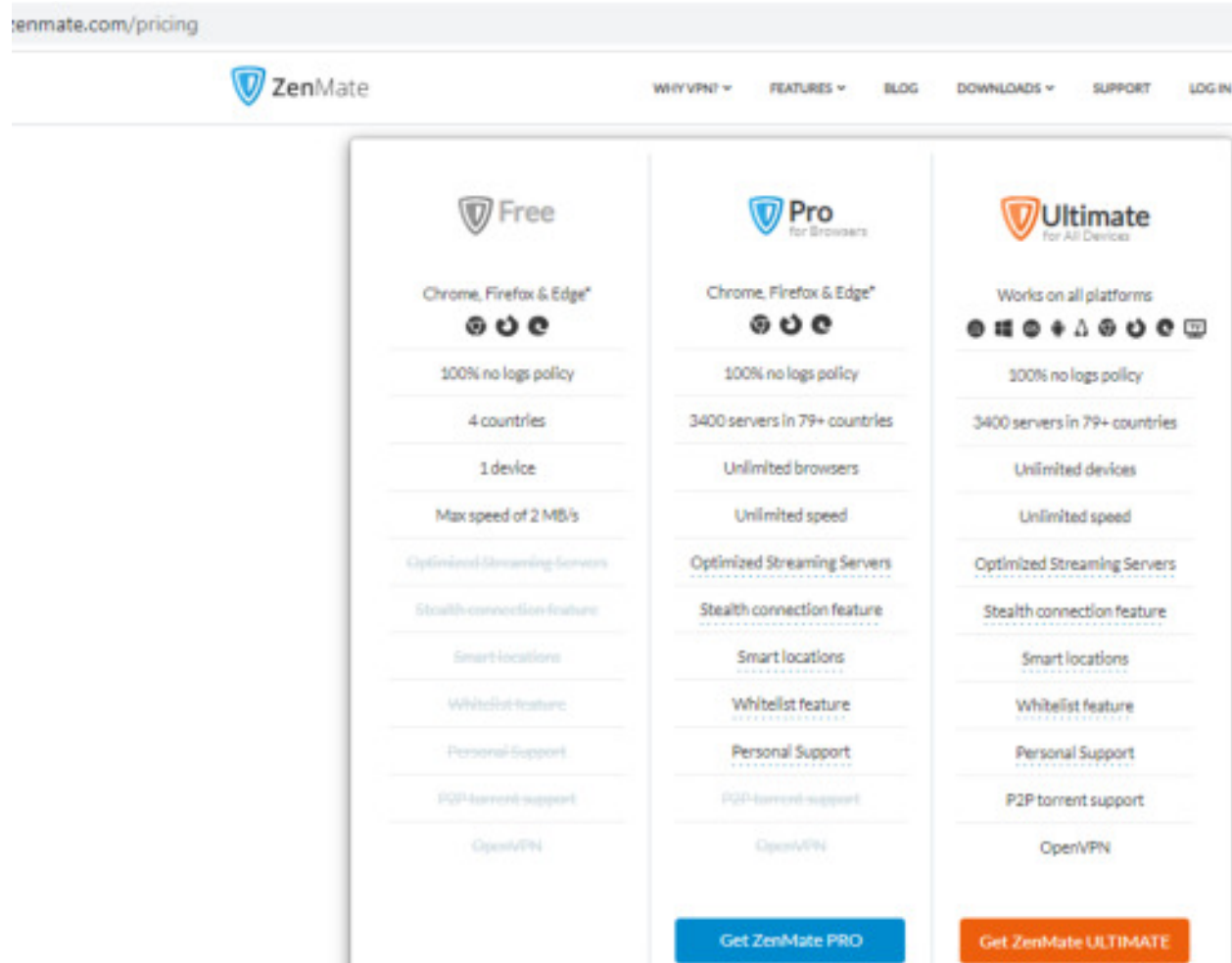
165. For example, ZenGuard distributed copies of the Works of Plaintiffs by the following file names from just IP address 207.244.78.5:  
USS.Indianapolis.Men.of.Courage.2016.HDRip.XviD.AC3-EVO;  
The.Hitmans.Bodyguard.2017.WEBRip.x264-FGT; The.Hitmans.Bodyguard.2017.720p.WEB-DL.950MB.MkvCage.mkv; All.Eyez.On.Me.2017.UNCENSORED.HDTS.x264-NoGRP;  
Singularity.2017.720p.HDRip.x264.AAC.-.Hon3y;  
Vengeance.A.Love.Story.2017.1080p.BRRip.x264.AAC-ETRG; www.torrenting.com -  
Singularity.2017.BRRip.XviD.AC3-EVO; Chuck.2016.720p.BluRay.H264.AAC-RARBG;  
Singularity (2017) 1080p WEBRip [xPau.se]; Leatherface (2017) 1080p WEBRip [xPau.se];  
Revolt (2017) 1080p WEBRip [xPau.se].mp4; Singularity.2017.WEB-DL.x264-FGT; The  
Hurricane Heist 2018 1080p HC HDRip x264 [MW]; and The.Hurricane.Heist.2017.D.WEB-DLRip.1400MB.avi; and Singularity (2017) [1080p] [YTS.AG].



*E. Defendants promote their service for piracy and encourage their subscribers to pirate copyright protected Works including Plaintiffs’.*

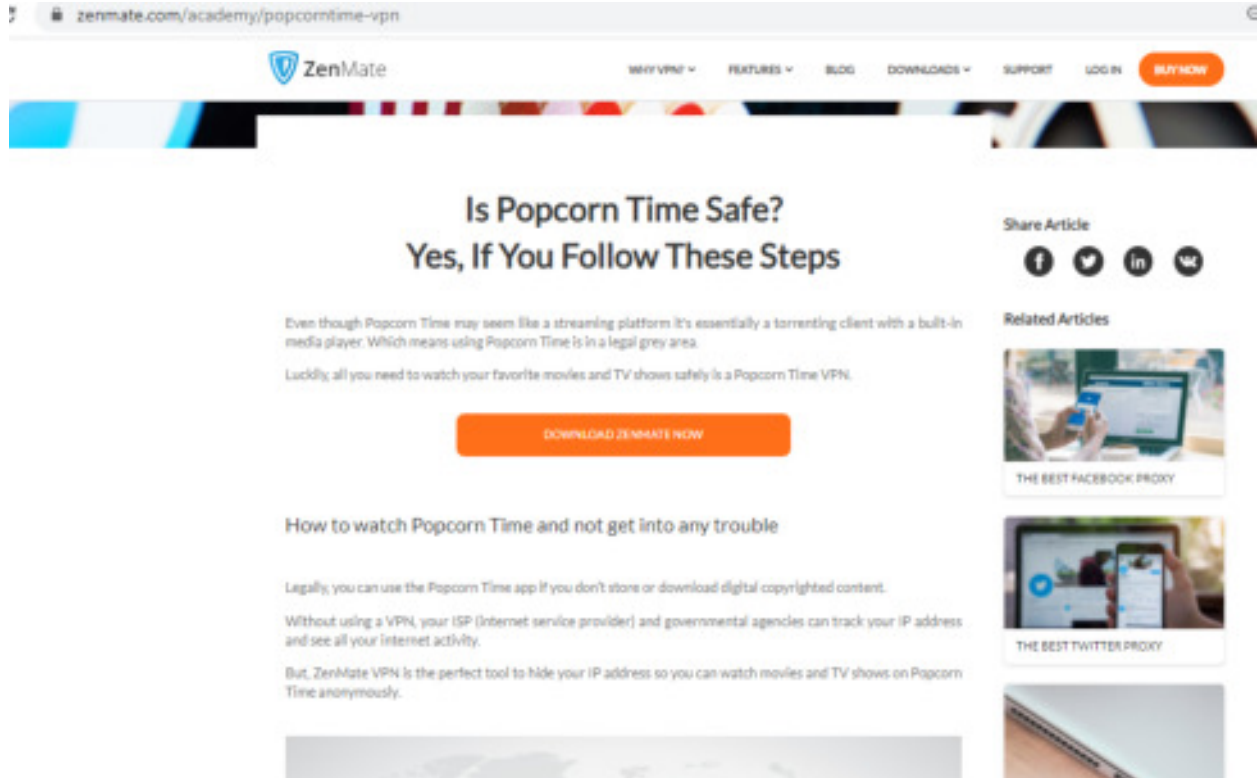
166. Defendants promote their services for the purpose of piracy.

167. Defendant ZenGuard advertises specific priced VPN service “Ultimate” that includes “P2P torrent support”. <https://zenmate.com/pricing> [last accessed on Aug. 20, 2021] (excerpt below).



168. ZenGuard even tells its end users that “Legally, you can use the Popcorn Time app if you don’t store or download digital copyrighted content.” <https://zenmate.com/academy/popcorn-time-vpn> [last accessed on May 25, 2021] (excerpt below).

169. ZenGuard advertises its VPN service as “the perfect tool to hide your IP address so you can watch movies and TV shows on Popcorn Time anonymously.” Id.



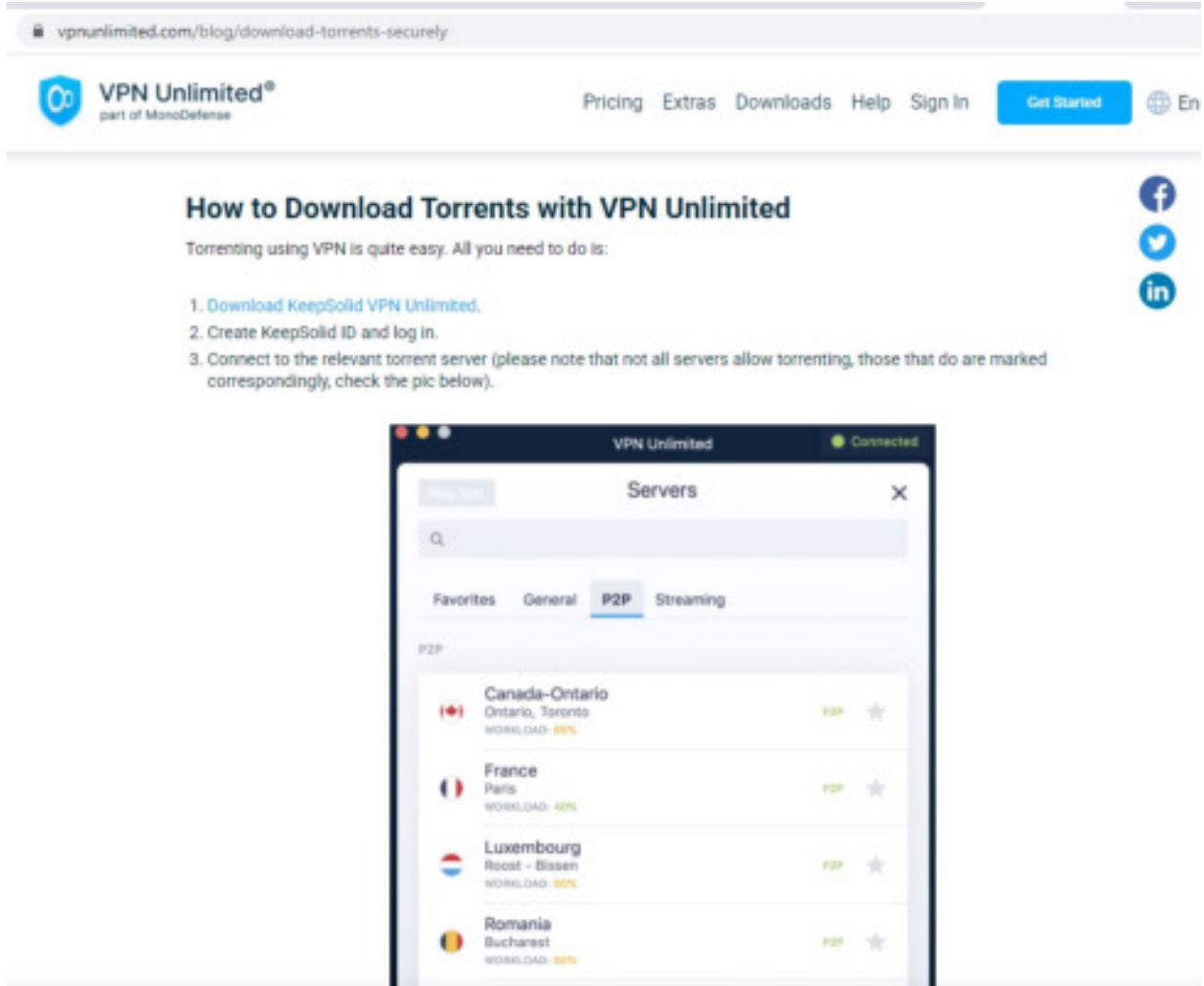
170. ZenGuard states, “We have a strict no-logs policy and we never record any of our users’ internet activity. This way you can rest assured knowing nobody can find out you’re using Popcorn Time.” Id.

171. ZenGuard advertises its “kill switch feature” whereby “...If your VPN service drops for any reason, ZenGuard immediately shuts down your internet connection to make sure nobody will find out you’re using Popcorn Time.” Id.

172. Defendant KeepSolid actively promotes its service VPN Unlimited for the purpose of movie piracy, including the infringing of Plaintiffs’ Works.

173. KeepSolid actively promotes its VPN service as a necessary tool to “Download Torrents”. <http://vpnunlimited.com/blog/download-torrents-securely> [last accessed August 20,

2021] (excerpt below).



174. KeepSolid provides “Tips and Tricks” for downloading torrents, including “How to download torrents faster”, “How to download torrents safely without getting caught”, and

“How to download torrents with VPN Unlimited”. *Id.*



175. KeepSolid warns its users “there are still risks” and advertises its safeguard “Kill Switch” feature to shut down internet connection when the VPN service fails.

<http://vpnunlimited.com/blog/how-to-protect-yourself-while-torrenting> [last accessed August 20,

2021] (excerpt below).



The screenshot shows a web browser window with the URL [vpnunlimited.com/blog/how-to-protect-yourself-while-torrenting](https://vpnunlimited.com/blog/how-to-protect-yourself-while-torrenting). The page header includes the VPN Unlimited logo (part of NordDefense), navigation links for Pricing, Extras, Downloads, Help, and Sign In, a Get Started button, and a language selector set to English. The main content area features the title "Kill Switch feature for extra security" and a 3D-rendered image of a red keyboard key labeled "Shut down" next to a white "Shift" key. To the right of the image are social media icons for Facebook, Twitter, and LinkedIn. Below the image, the text explains that the Kill Switch feature is on guard and instantly shuts down the internet connection if it detects any disruptions in the VPN connection, preventing privacy leaks and protecting the user's real IP address and location. A link is provided for more information about the Kill Switch option.

Kill Switch feature for extra security



Don't get too comfortable, however, as there are still risks. Even the most reliable VPN services may have occasional disruptions. If any third parties are interested in your online activities, they can just wait for the right time to discover your real IP address.

Whatever the reason for a disconnect may be (poor signal strength or congested network), the Kill Switch feature is on guard. It instantly **shuts down your internet connection** if it detects any disruptions in your VPN connection. This measure **prevents privacy leaks** and **protects your real IP address** and location from accidentally getting revealed to any third parties.

For more information about the Kill Switch option, check out [this page](#).

176. KeepSolid explicitly acknowledges that using bittorrent to download copyright protected content is illegal. *Id.*


vpnunlimited.com/blog/how-to-protect-yourself-while-torrenting

VPN Unlimited®  
part of NordDefense

Pricing Extras Downloads Help Sign In Get Started English ▾

Blog > Unpaid Fine for \$22,500 Per One Song: Truth, Fake, or Nightmare

## To Torrent or Not To Torrent... Don't!



4min read

**Updated on July 13, 2021:** From now on, traffic filtering, malware protection, and suspicious DNS activity blocking are available as a part of the separate [DNS Firewall](#) app.

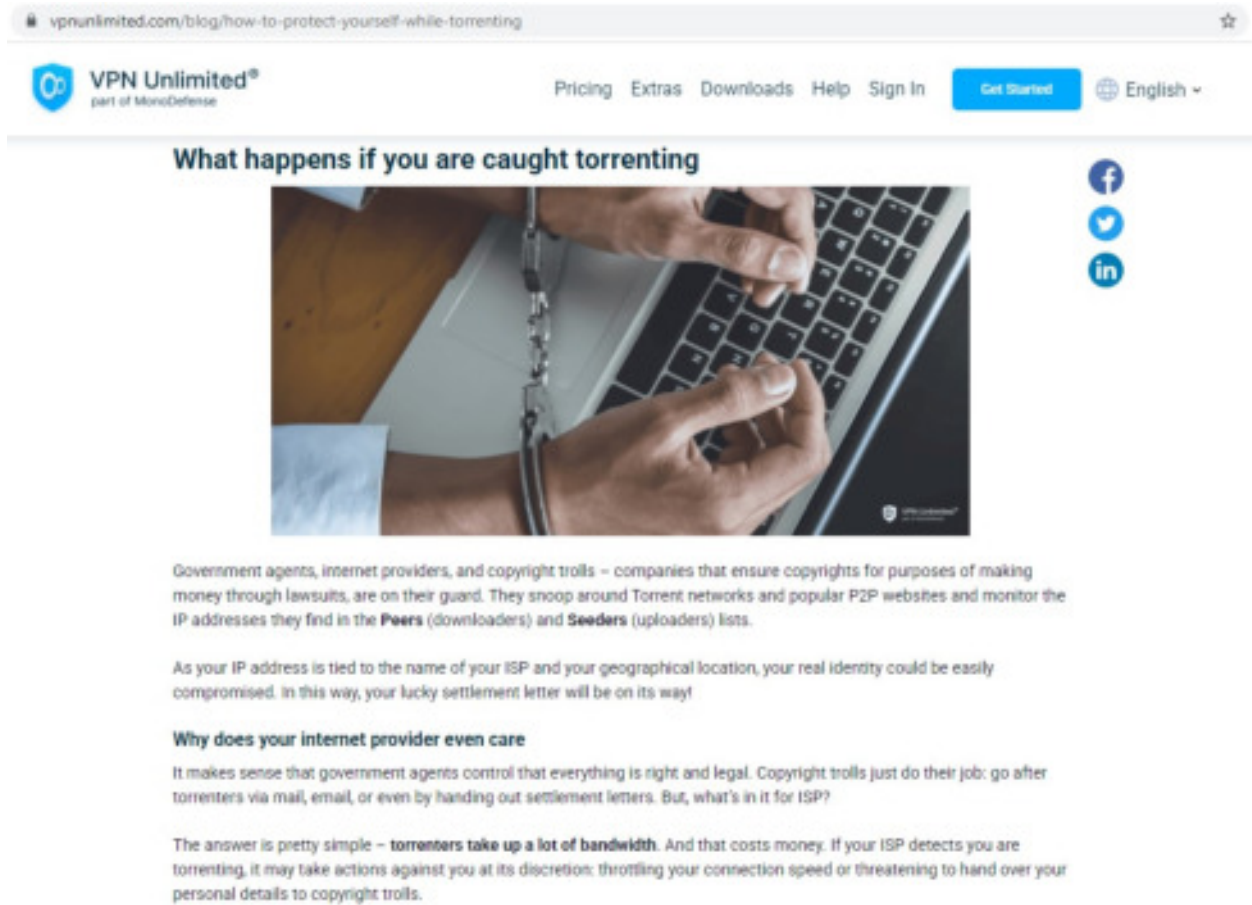
First of all, **downloading copyrighted material is illegal**. Secondly, if you get caught, you receive a **huge fine** for copyright infringement. And finally, you would have to **make a slight moral compromise** (you know, "you wouldn't steal a car").

The frequency of legal actions against torrenters peaked in the 2000s. Nowadays, there are much fewer lawsuits. However, that doesn't mean you can freely download torrents without fear of punishment, especially since the fine can be extremely high. It varies from **\$200 to \$150,000** for each downloaded video or audio file, plus legal fees.

You could receive a settlement letter not only for torrenting brand new films and popular songs. Even if you torrent an old movie or a 90s' single from a pirated source, legally speaking, you're still breaking the law.

Facebook  
Twitter  
LinkedIn

177. KeepSolid explains how a user may get caught torrenting and the reasons why ISPs may want to stop torrenting. *Id.*



The screenshot shows a web browser window with the URL [vpnunlimited.com/blog/how-to-protect-yourself-while-torrenting](https://vpnunlimited.com/blog/how-to-protect-yourself-while-torrenting). The page header includes the VPN Unlimited logo (part of MonoDefense), navigation links for Pricing, Extras, Downloads, Help, and Sign In, a 'Get Started' button, and a language selector set to English. The main heading is 'What happens if you are caught torrenting'. Below the heading is an image of a person's hands typing on a laptop keyboard while wearing metal handcuffs. To the right of the image are social media sharing icons for Facebook, Twitter, and LinkedIn. The text below the image explains that government agents, ISPs, and copyright trolls monitor torrent networks and P2P websites, tracking IP addresses of Peers (downloaders) and Seeders (uploaders). It notes that an IP address is tied to an ISP and geographical location, making real identity easy to compromise. A section titled 'Why does your internet provider even care' explains that ISPs care because torrenters use a lot of bandwidth, which costs money. ISPs may throttle connection speeds or hand over personal details to copyright trolls.

Government agents, internet providers, and copyright trolls – companies that ensure copyrights for purposes of making money through lawsuits, are on their guard. They snoop around Torrent networks and popular P2P websites and monitor the IP addresses they find in the **Peers** (downloaders) and **Seeders** (uploaders) lists.

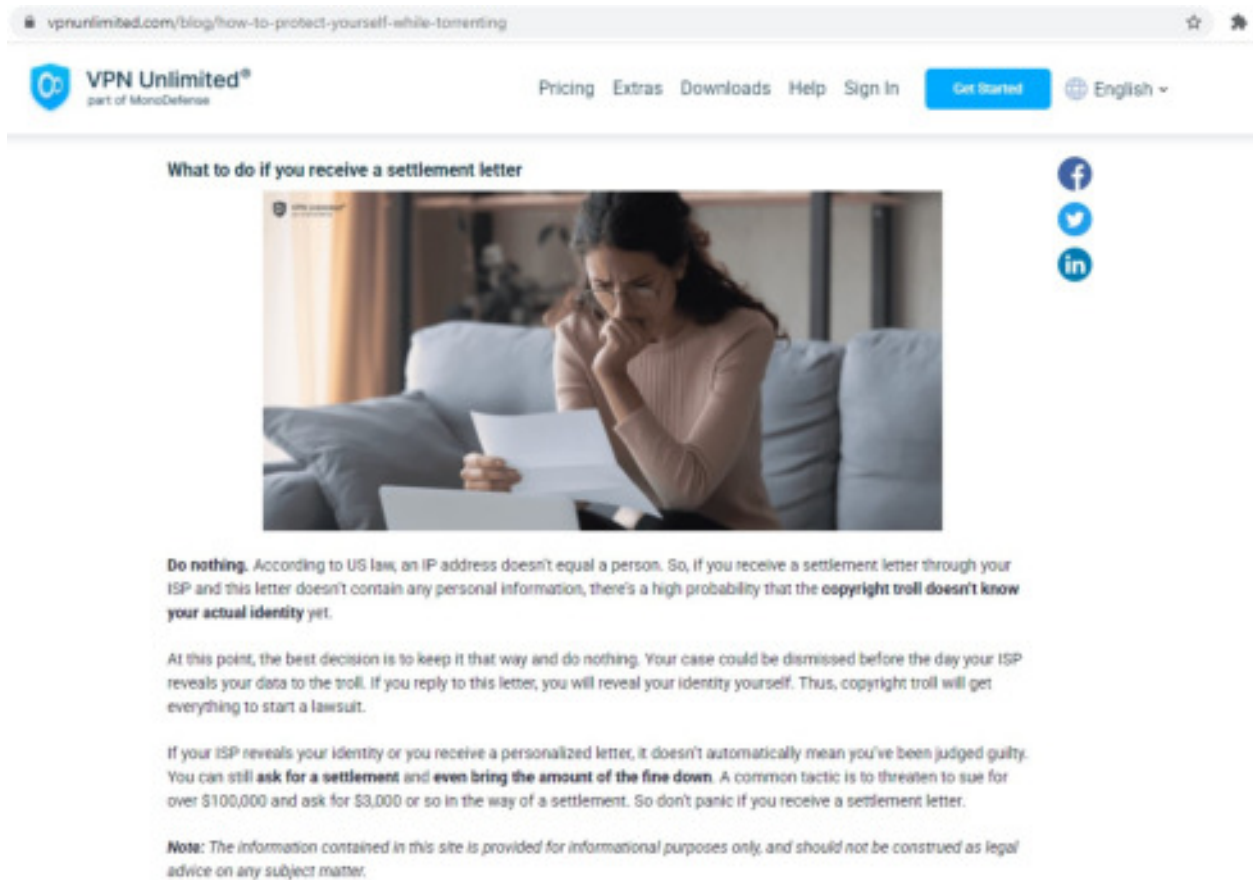
As your IP address is tied to the name of your ISP and your geographical location, your real identity could be easily compromised. In this way, your lucky settlement letter will be on its way.

**Why does your internet provider even care**

It makes sense that government agents control that everything is right and legal. Copyright trolls just do their job: go after torrenters via mail, email, or even by handing out settlement letters. But, what's in it for ISP?

The answer is pretty simple – **torrenters take up a lot of bandwidth**. And that costs money. If your ISP detects you are torrenting, it may take actions against you at its discretion: throttling your connection speed or threatening to hand over your personal details to copyright trolls.

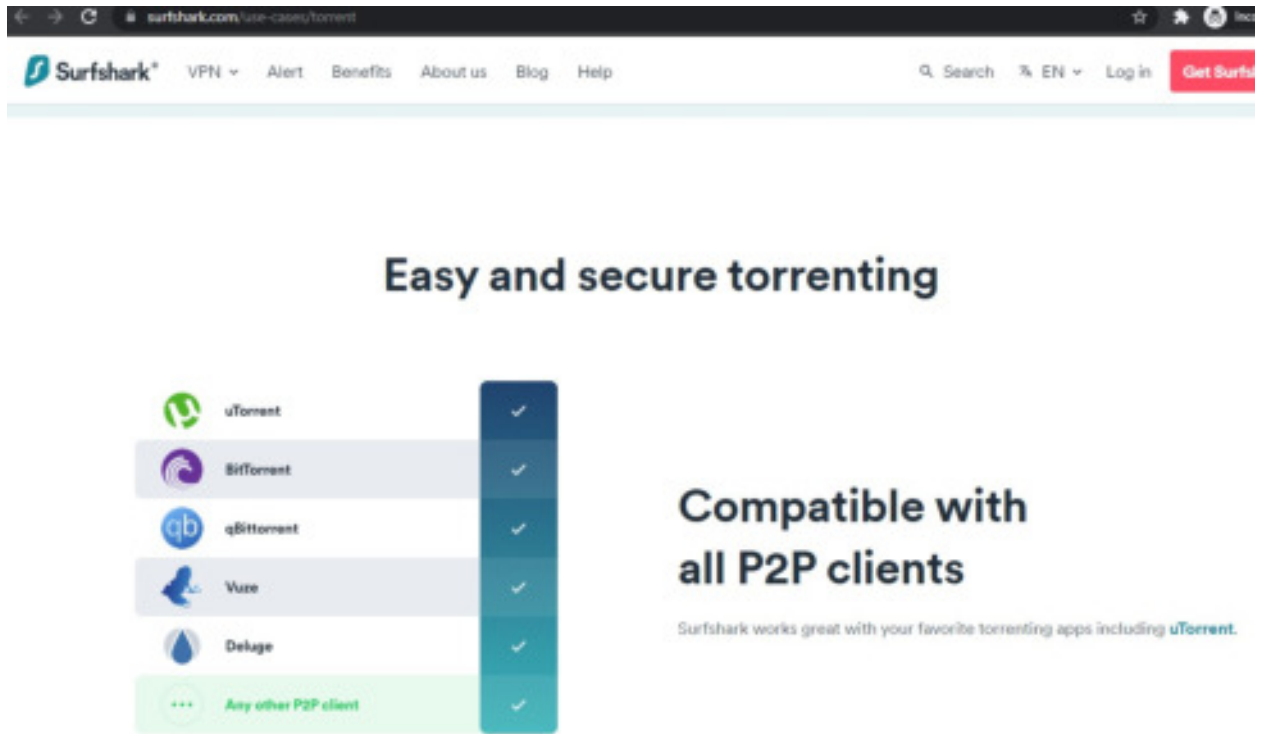
178. KeepSolid goes as far as providing its users advice on what to do if the user is caught. *Id.*



179. Defendant Surfshark actively promotes its VPN service for the purpose of movie piracy, including the infringing of Plaintiffs' Works.

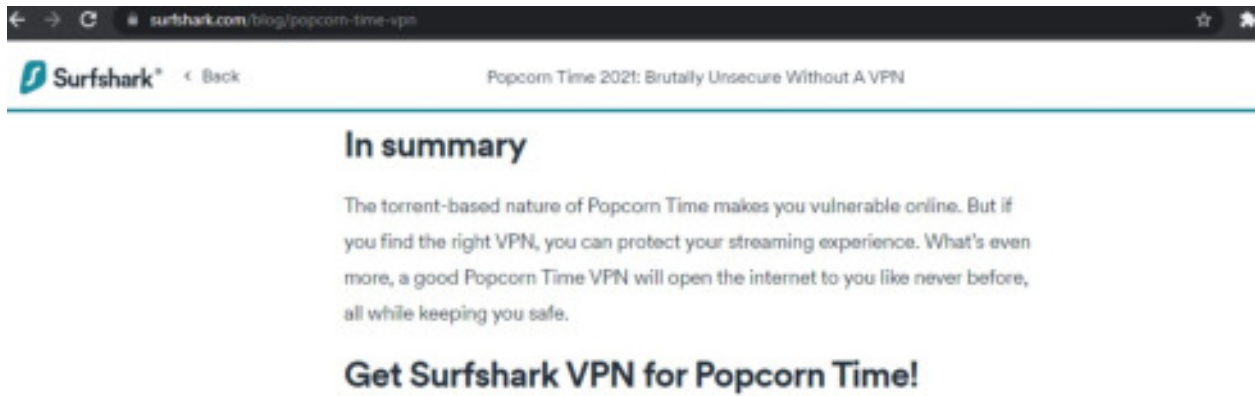
180. Surfshark actively promotes its VPN service as a tool to utilize peer-to-peer Bittorrent clients, even naming some of the most popular Bittorrent clients for compatibility.



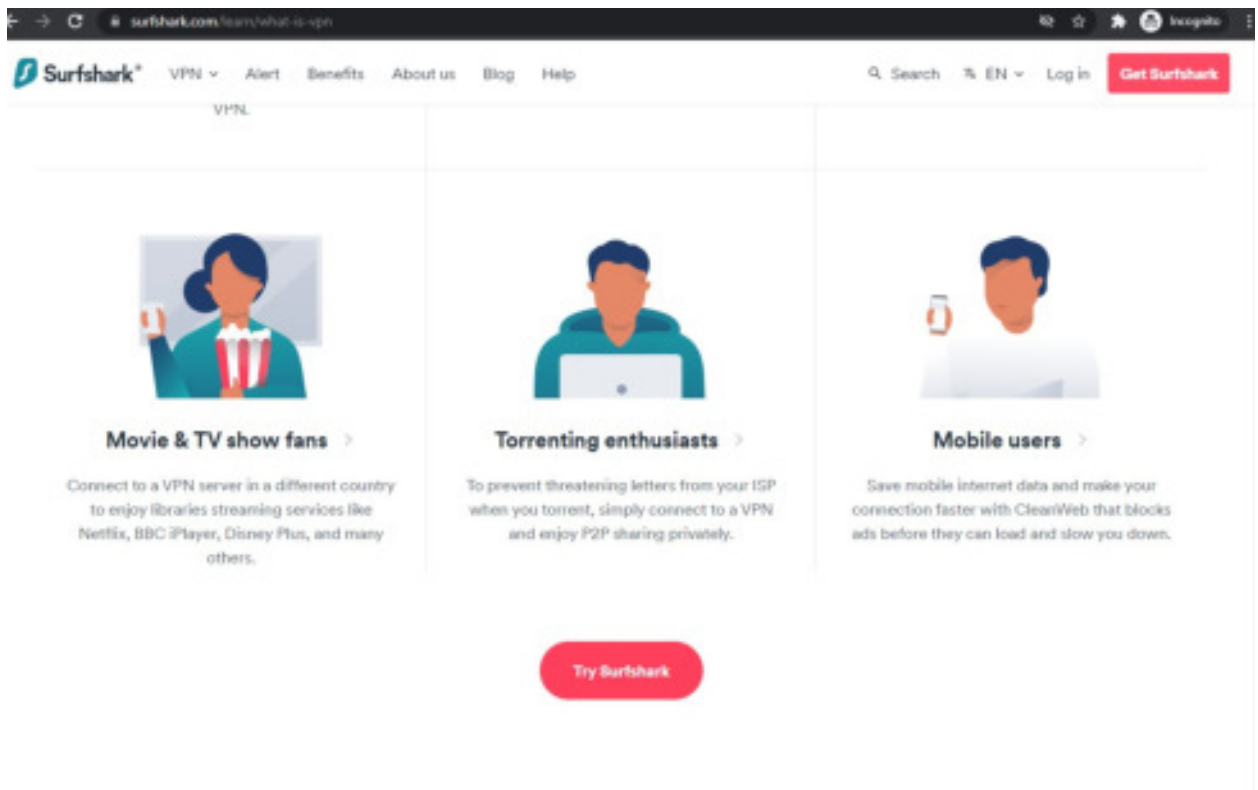


181. Defendant Surfshark promotes its VPN service for the notorious “Popcorn Time” piracy tool, while simultaneously acknowledging that using Popcorn Time for its intended purpose of piracy may be illegal.

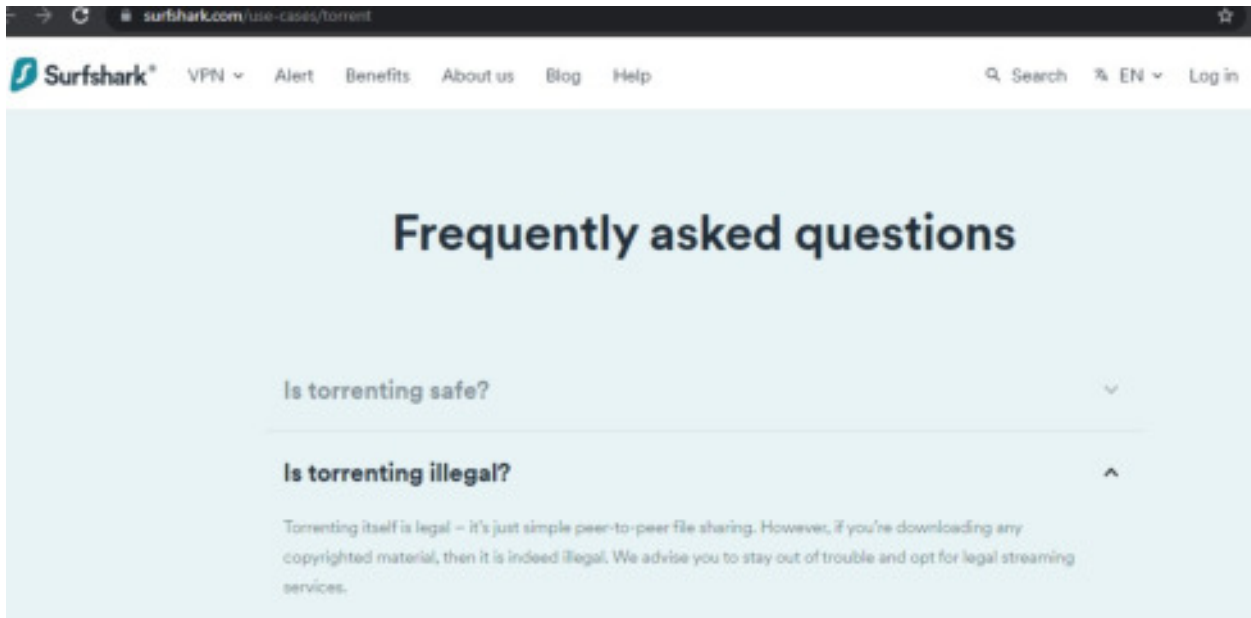




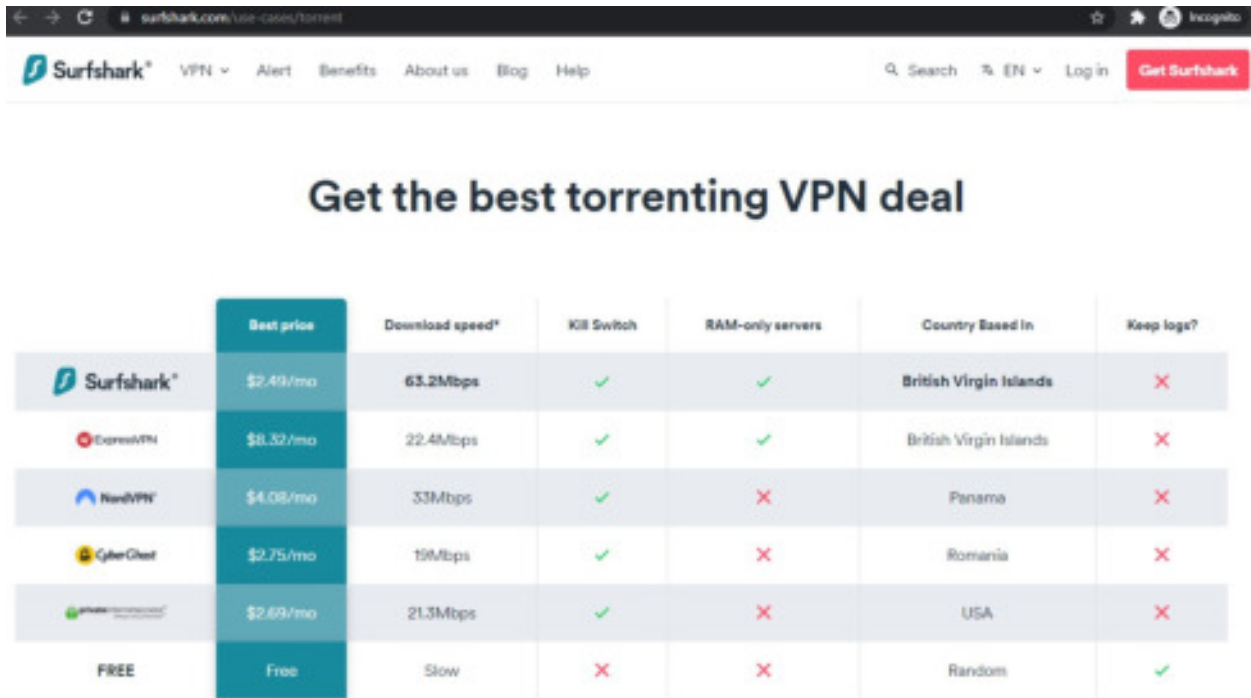
182. Defendant Surfshark blatantly encourages customers to torrent by advertising its services specifically for “torrenting enthusiasts”.

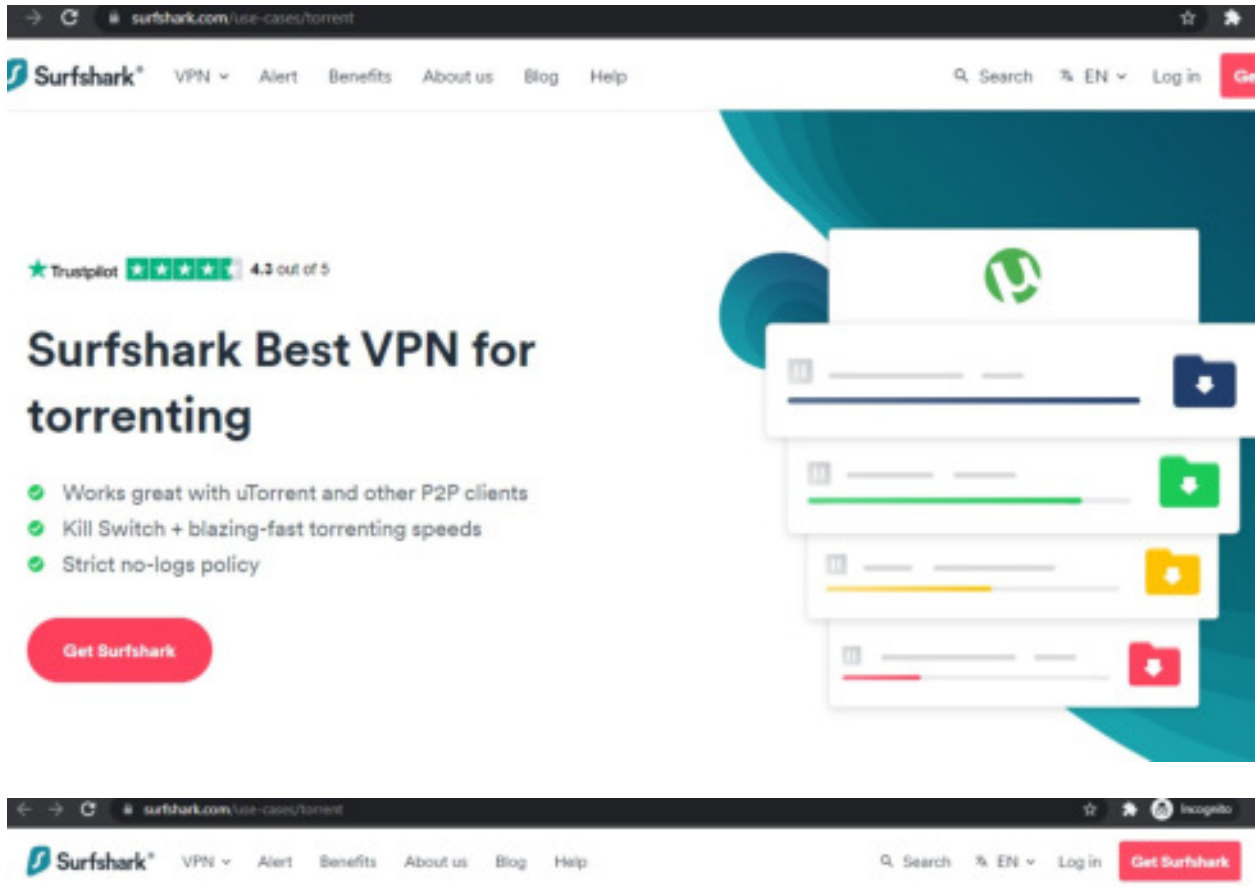


183. Defendant Surfshark acknowledges that torrenting copyright protected materials is illegal.



184. Still, Defendant Surfshark encourages its VPN service for torrenting.





## You need a VPN for torrenting to:

- 1 Stay private when you download torrents. A VPN ensures that only you know you're torrenting.
- 2 Enjoy the internet with no restrictions. With a VPN, you can access any content that you love.
- 3 Get the highest bandwidth speeds with zero throttling. Some providers may choose to slow down your connection based on the data you download, and a VPN helps to prevent that.



185. Defendant ExpressVPN actively promotes its VPN service for the purpose of movie piracy, including the infringing of Plaintiffs' Works.

186. ExpressVPN emphasizes that its service has "No restriction" and its subscribers can "Stream or download anything...with your IP address hidden..."

ExpressVPN with the push of a button.



## No restrictions

Stream or download anything, from any of our servers, anywhere on Earth, with your IP address hidden from prying eyes.

187. In response to a question of whether BitTorrent and other file-sharing traffic is allowed on all ExpressVPN servers, ExpressVPN replied that “ExpressVPN allows all traffic, including BitTorrent and other file-sharing traffic (without rerouting), from all of our VPN servers.” See <https://torrentfreak.com/expressvpn-anonymous-review/> [last accessed on Aug. 24, 2021].

***F. Defendants knew the Copyright Management Information included in the files they distributed to other peers had been removed or altered without the authority of Plaintiffs.***

188. Legitimate file copies of the Works include CMI indicating the respective title.

189. The initial seeder of the infringing file copies of Plaintiff’s Work added wording to the file titles to “brand” the quality of piracy files he or she released and attract further traffic to his or her website.

190. For example, the initial seeder of the infringing file copies of *Angel Has Fallen* added the wording “YTS” to the file titles to brand the quality of piracy files he or she released and attract further traffic to the YTS website.

191. The word YTS is not included in the file title of legitimate copies or streams of the Plaintiffs’ Works. The initial seeders of the Work altered the title to falsely include the words “YTS” in the CMI.

192. The file copies Defendants’ subscribers distributed to other peers in the Swarm included the altered CMI in the file title.

193. Defendants’ subscribers knew that FGT, YTS and RARBG were not the author of Plaintiffs’ Works.

194. Defendants’ subscribers knew that FGT, YTS and RARBG were not a licensed distributor of Plaintiffs’ Works. Indeed, the YTS website includes a warning to this effect.

195. Defendants' subscribers knew that the CMI that included YTS and RARBG in the file names was false.

196. Defendants' subscribers knew that the file copies of the Work that they distributed to other peers from in the Swarm included the altered CMI without the authority of Plaintiffs.

197. Defendants' subscribers knew that the CMI in the title they distributed to other peers in the Swarm included the altered CMI without the authority of Plaintiffs.

198. Defendants' subscribers knew that the false or altered CMI in the titles would induce, enable, facilitate or conceal infringements of the Works when they distributed the false CMI, altered CMI or Works including the false or altered CMI.

199. Namely, Defendants' subscribers knew that other recipients would see the file titles and use the altered CMI to go to the website such as YTS from where the torrent files originated to obtain unlicensed copies of the Work.

200. By providing the website in the altered CMI to others, Defendants' subscribers induced, enabled and facilitated further infringements of the Works

201. Indeed, Defendants promote their VPN services for accessing piracy website such as YTS and RARBG and using Popcorn Time.

***G. Defendants had knowledge that their subscribers were infringing Plaintiffs' Works by distributing file copies of the Works with altered CMI but continued to provide service to its subscribers***

202. Plaintiffs engaged MEU to generate Notices of infringements ("Notices") styled per 17 U.S.C. §512(c)(3) of the DMCA to be sent to service providers of IP addresses where MEU confirmed infringement of copyright protected content.

203. 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 CMI, the IP address and port number at where infringement was confirmed and the time of infringement down to the second. *See* Exhibit “4” (excerpt below).

```
Protocol: BITTORRENT
Infringed Work: Hellboy
Infringing FileName: Hellboy (2019) [WEBRip] [1080p] [YTS.LT] Infringing FileSize: 2088501368 Infringer's IP Address:
209.58.139.35 Infringer's Port: 63368 Initial Infringement Timestamp: 2020-08-22 17:44:59
```

204. MEU determines the proper abuse contact email address for the service provider assigned the IP addresses at issue from publicly available information from ARIN.

205. Plaintiffs’ agent sent Notice to Leaseweb’s abuse contact email address ([abuse@us.leaseweb.com](mailto:abuse@us.leaseweb.com)).

206. For example, Plaintiffs’ agent sent 400 Notices to Leaseweb concerning observed infringements at each of IP addresses 209.58.139.35, 209.58.139.34, 209.58.130.210, 209.58.135.106, 209.58.137.94, 209.58.135.72, and 209.58.135.74 (total of over 2800 Notices for these seven IP addresses) that Leaseweb reallocated/reassigned to KeepSolid.

207. Upon information and belief, other rightsholders had similar Notices sent to Leaseweb concerning infringing activity at IP addresses Leaseweb reassigned and or reallocated to Defendants.

208. Leaseweb promptly forwarded the Notices to Defendants and requested they take immediate action.

209. Defendants falsely told Leaseweb that they had resolved any abusive activity.

210. Defendant Surfshark completely ignored a written request from Plaintiffs’ counsel to discuss this matter. *See* Exhibit “5”.

211. Plaintiffs’ agent sent thousands of Notices to VPN Consumer Network Services’ abuse contact email address [abuse-reports@vpnconsumer.com](mailto:abuse-reports@vpnconsumer.com).



212. Upon information and belief, other rightsholders had similar Notices sent to VPN Consumer Network Services concerning infringing activity at IP addresses associated with ExpressVPN.

213. Defendants failed to take any action toward their subscribers in response to these Notices.

***H. Defendants control the conduct of their subscribers.***

214. Defendants can terminate the accounts of their subscribers at any time.

215. Defendants promptly suspend and/or terminate subscriber accounts when said subscribers failed to pay for service.

216. Defendants have the ability to null-route IP addresses being used by subscribers to pirate Plaintiffs' Works.

217. Defendants have the capability to log their subscribers' access to their VPN service but purposely delete the logged information or set up their system so that the logged information is deleted so that they can promote their service as a means to pirate copyright protected Works anonymously.

218. Defendants monitor their subscribers' access to their service such as, for example, customer's consumption of data.

219. Defendant Surfshark states in its Terms of Service that it may limit the number of connected devices for any subscriber account in its network maintenance system.

220. Surfshark further has a list of violations that may result in termination without notice.

221. ExpressVPN states that "We reserve the right to block specific abusive traffic to protect the server network and other ExpressVPN customers". See <https://torrentfreak.com/best-vpn-anonymous-no-logging/#expressvpn> [last accessed on Aug. 24, 2021].

***I. Defendants do not have a safe harbor from liability.***

222. As part of the DMCA, Congress created a safe harbor that limits the liability of a service provider for copyright infringement when their involvement is limited to, among other things, “transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider.” 17 U.S.C. § 512(a). To benefit from this safe harbor, however, an ISP must demonstrate that it “has adopted and reasonably implemented...a policy that provides for the termination in appropriate circumstances of subscribers...who are repeat infringers.” 17 U.S.C. § 512(i)(1)(A).

223. Defendants have not adopted and/or reasonably implemented a policy of terminating repeat infringers.

224. Plaintiffs’ agent has sent over 32,000 Notices to Leaseweb concerning infringements at IP addresses Leaseweb reassigned to Defendants which Leaseweb promptly forwarded to Defendants.

225. Upon information and belief, other rightsholders sent Notices to Leaseweb that were forwarded to Defendants.

226. Plaintiffs’ agents have also sent thousands of Notices to other data centers such as Total Server Solutions, QuadraNet and Digital Ocean that were forwarded to Defendants.

227. Defendants have failed to terminate subscriber accounts and/or take any meaningful actions against its subscribers in response to these Notices consistent with a reasonably implemented policy for termination of subscribers and account holders of the service provider’s system or network who are repeat infringers necessary to support a safe harbor from liability (“policy”).

228. Defendants interfere with standard technical measures used by copyright holders to identify or protect copyright works by purposefully deleted their end users’ logged information. *See* 17 U.S.C. § 512(i)(1)(B).

229. Defendants specifically admit that they delete their end users' logged information to protect the end users' piracy activities in promotions and advertisements. *See e.g.* Ernesto, "Which VPN Providers Really Take Privacy Seriously in 2021?", June 14, 2021, <https://torrentfreak.com/best-vpn-anonymous-no-logging/> [last accessed on Aug. 20, 2021] (In response to questions concerning BitTorrent activity, Surfshark states "We do not keep any logs, data, timestamps, or any other kind of information that would enable anyone to identify neither current nor former users of our service.")

230. Congress created a safe harbor that limits the liability of a service provider for copyright infringement "...by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider" does not have the requisite knowledge, "...responds expeditiously to remove or disable access to, the material..." and has the appropriate designated agent for receiving notices. 17 U.S.C. § 512(c)(1), (2).

231. Leaseweb leased use of its servers to Defendants so that the subscribers can host VPN networks on its servers.

232. Defendants store copies of Plaintiffs' Works on Leaseweb's servers and use Leaseweb's servers to distribute copies of Plaintiffs' Works.

233. The over 32,000 Notices Plaintiffs' agent sent to Leaseweb concerning infringements included information such as the IP addresses that Leaseweb forwarded to Defendants that Defendants could have used to remove or disable access to infringing material.

234. Defendants failed to respond and expeditiously remove or disable access to the material in response to the over 32,000 Notices Plaintiffs' agent sent to Leaseweb and that were forwarded to them.

235. Defendant KeepSolid failed to designate and register an agent with the Copyright Office as provided by 17 U.S.C. § 512(c)(2) until April 23, 2019.

236. Defendants Surfshark, ExpressVPN and ZenGuard have failed to designate and register an agent with the Copyright Office as provided by 17 U.S.C. § 512(c)(2).

237. Surfshark states that since it is outside of the US it does not need to even have a DMCA policy. See <https://torrentfreak.com/best-vpn-anonymous-no-logging/#surfshark> [last accessed on Aug. 20, 2021] (“DMCA takedown notices do not apply to our service as we operate outside the jurisdiction of the United States. In case we received a non-US equivalent, we would not be able to provide any information because we have none (strict no logs policy)”).

238. Defendants’ conduct renders them ineligible for safe harbor immunity from copyright liability under the DMCA.

***J. The copyright infringements arise from Defendants’ advertisements.***

239. Defendants advertise their VPN services for the purpose of engaging in movie piracy.

240. Defendants’ subscribers are motivated to become customers from Defendants’ advertisements.

241. Defendants recruit affiliates to promote their services on various websites.

242. Defendants’ affiliates promote the VPN services with aggressive language that explicitly states that the VPN services are configured for P2P and great for piracy.

vpnrank.com/best-vpn/popcorn-time/

## 2. Surfshark – Budget-friendly VPN for Popcorn Time



Surfshark for Popcorn time is a great option, in my opinion. If you're looking for more or less a for Popcorn Time without compromising on privacy, then perhaps you might prefer Surfshark. after all, it only costs [\\$2.49/mo](#).

243. ExpressVPN even knowingly uses operators of notorious piracy websites such as YTS as affiliates that prominently promote ExpressVPN next to options to download pirated copies of Plaintiffs' Works.

yts.movie/torrent/angel-has-fallen/12467/

**YTS** Quick search



### Angel Has Fallen

2019  
Action / Thriller

Available in: 720p.BluRay 1080p.BluRay 720p.WEB 1080p.WEB

440  
39% - Critics  
93% - Audience  
IMDb 6.5 ★

Please enable your VPN when downloading torrents  
Assigned IP address **89.185.228.120**, located in **CZECHIA**. Your ISP can monitor you, unless you use a zero log VPN.

Download


Get Express VPN

5090200 the brass teapot 2012 torrent magnet yts

**YTS.MN** Search

### The Brass Teapot

2012  
Comedy / Fantasy / Thriller

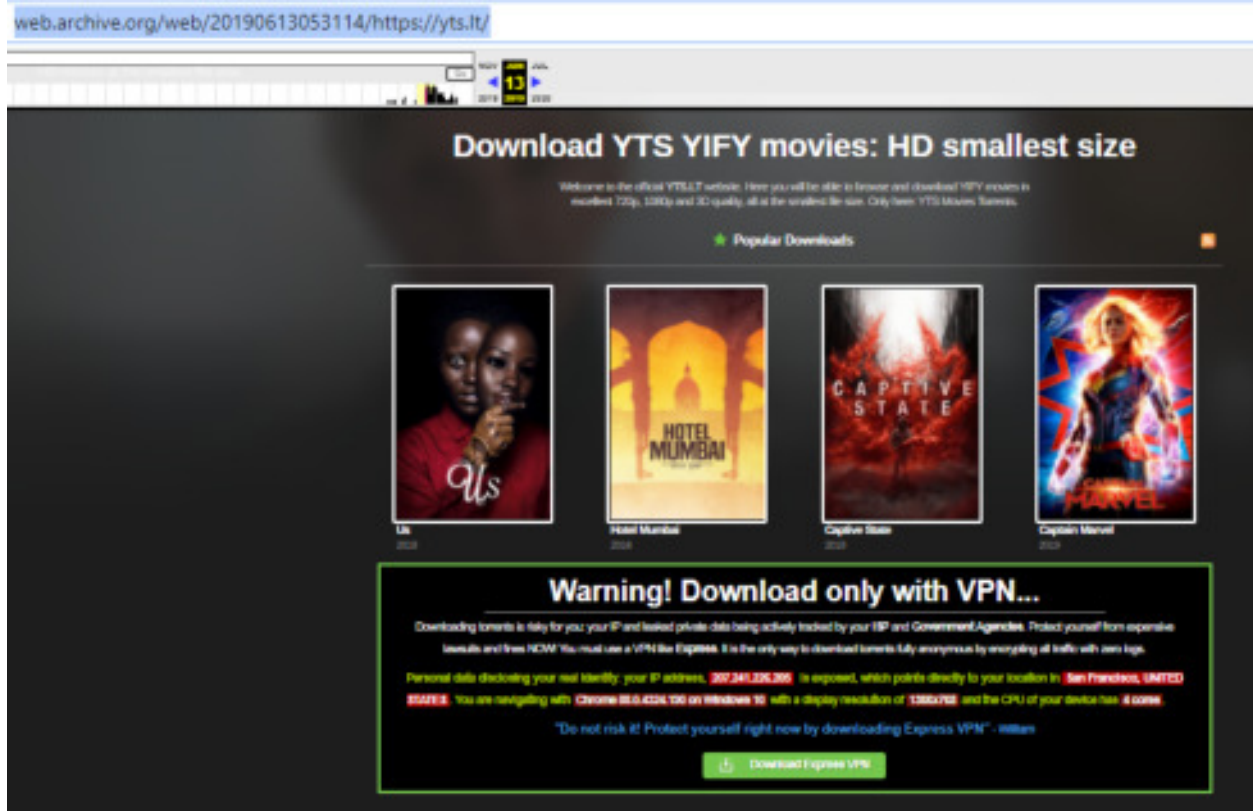


17  
IMDb 6.4

Please enable your VPN when downloading torrents  
Assigned IP address **31.220.40.43**, located in **GERMANY**. Your ISP can monitor you, unless you use a zero log VPN.

720p.BluRay  
1080p.BluRay

Get Express VPN



244. Defendants pay their affiliates for each subscriber that signs up through affiliate links.

245. Defendants provide their affiliates script code to be used that promotes and advertises their services for piracy.

246. Defendants' subscribers are motivated to become customers from Defendants' and their affiliates promotions of their VPN services for piracy.

247. Defendants' subscribers are motivated to become customers from the knowledge of Defendants' practices of ignoring notices of infringements or failing to take any meaningful action in response to said notices.

248. Defendants' subscribers are motivated to become customers from the knowledge that the VPN service can be used to pirate copyright protected content without getting caught.

***K. VPN Consumer Network Services intentionally misrepresents material information in the Whois***

*records of ARIN.*

249. VPN Consumer Network and VPN Consumer Network Services (collectively: “VPNCN”) allocates or reassigns IP addresses it received from ARIN to ExpressVPN.

250. Despite allocating or reassigning IP addresses to ExpressVPN, VPNCN publishes ARIN Whois records falsely indicating VPN Consumer Network Services as the proper abuse contact at these IP addresses rather than the contact of ExpressVPN in violation of its registration agreement with ARIN.

251. Despite allocating or reassigning these IP addresses to ExpressVPN, VPNCN knowingly failed to update the ARIN Whois records to indicate ExpressVPN as the proper abuse contact at these IP addresses in violation of its registration agreement with ARIN.

252. For example, VPNCN publishes in the ARIN Whois records concerning IP address 104.143.92.63 (and the complete block 104.143.92.0/24) that abuse notices should be sent to: abuse-reports@vpnconsumer.com at AZ Business Center, Avenida Perez Chitre Panama, New Territories,395.

253. VPNCN had allocated IP address 104.143.92.63 to ExpressVPN.

254. On May 4, 2018 when VPNCN last changed the ARIN record, VPN Consumer Network Services knowingly and intentionally published its name as the relevant contact rather than ExpressVPN.

255. Tayah Durnan used ExpressVPN’s IP address 104.143.92.63 allocated from VPN Consumer Network Services to download and share copies of the movie *Rambo: Last Blood* while concealing her identity in November of 2019. *See Decl. of Tayah Durnan.*

256. VPNCN’s failure to update the Whois ARIN records and/or publishing false Whois ARIN records for these IP addresses that it reassigned and/or reallocated to ExpressVPN constitute



misrepresentations of material facts.

257. Plaintiffs' agent relied on VPNCN's misrepresented information in the Whois ARIN records to determine the appropriate party to send the notices of infringements ("Notices").

258. Plaintiffs' agent had a right to rely on the Whois ARIN records to determine the appropriate party to send the Notices.

259. Relying on the Whois ARIN records is consistent with IT industry practices.

260. Courts throughout the US have relied on the identification information of the Whois ARIN records when approving warrants and subpoenas.

261. Rightsholders such as Plaintiffs are third party beneficiaries to VPNCN's agreement with ARIN to update the Whois ARIN records when VPNCN allocates or reassigns IP addresses to subscribers such as ExpressVPN. Rightsholders rely on the Whois records to stop abuse.

262. VPNCN intends for rightsholders such as Plaintiffs to rely on the false information it publishes in the Whois records of ARIN.

263. In reliance on VPNCN's misrepresented information in the ARIN Whois records, Plaintiffs' agent sent notices of infringement to VPN Consumer Network's abuse contact.

264. VPNCN failed to inform Plaintiffs' agent that the IP addresses at issue had been allocated and/or reassigned to ExpressVPN.

265. Plaintiffs have suffered damages as a result of VPNCN's misrepresentation. If VPNCN published accurate information in the ARIN Whois records, Plaintiffs' agent would have sent the Notices directly to ExpressVPN so that the abusive activity could be stopped.

266. If VPNCN published accurate information in the ARIN Whois records, Plaintiffs' agent would have taken legal action against ExpressVPN earlier.

267. Upon information and belief, VPNCN and ExpressVPN are motivated to publish false Whois records to prevent rightsholders from sending Notices to ExpressVPN.

268. Upon information and belief, VPNCN and ExpressVPN are motivated to publish false Whois records to prevent the public from knowing they have a location in the United States.

269. For example, ExpressVPN states that since it is “a British Virgin Islands (BVI) company...the BVI...is not party to any 14 Eyes intelligence sharing agreements, and has a dual criminality provision that safeguards against legal overreach.” <https://torrentfreak.com/expressvpn-anonymous-review/> [last accessed on Aug. 24, 2021]. However, in the ARIN records its alter ego VPN Consumer Network Services provides an address in San Francisco, CA.

**VI. FIRST CLAIM FOR RELIEF**  
**(Direct Copyright Infringement against Defendants)**

270. Plaintiffs re-allege and incorporate by reference the allegations contained in each of the foregoing paragraphs.

271. Plaintiffs are the copyright owners of the Works, each of which contains an original work of authorship.

272. Defendants’ subscribers use Defendants’ VPN services to pirate copyright protected content including Plaintiffs from IP addresses tied to Defendants’ servers exactly as promoted and instructed by Defendants.

273. Defendants copied the constituent elements of these copyright-protected Works.

274. Defendants connect their subscribers to sources for providing copies of Plaintiffs Works to be delivered to their subscribers over Defendants’ network.

275. Defendants distribute copies of Plaintiffs’ Works with knowledge that said copies infringes Plaintiffs’ rights.

276. Defendants' subscribers use Defendants' VPN services to stream copies of Plaintiffs' Works from Defendants' servers from unauthorized locations exactly as promoted and instructed by Defendants.

277. Plaintiffs did not authorize, permit, or provide consent to Defendants to copy, reproduce, distribute or perform their Works.

278. As a result of the foregoing, Defendants violated the Plaintiffs' exclusive right to reproduce the Works in copies, in violation of 17 U.S.C. §§ 106(1) and 501.

279. As a result of the foregoing, Defendants violated the Plaintiffs' exclusive rights to distribute copies of the Work in copies, in violation of 17 U.S.C. §§ 106(3) and 501.

280. As a result of the foregoing, Defendants violated the Plaintiffs' exclusive rights to publicly perform copies of the Work in copies, in violation of 17 U.S.C. §§ 106(4) and 501.

281. Defendants' infringements were committed "willfully" within the meaning of 17 U.S.C. § 504(c)(2).

282. Plaintiffs have suffered damages that were proximately caused by the Defendants' copyright infringements including, but not limited to lost sales, price erosion, and a diminution of the value of its copyright.

**VII. SECOND CLAIM FOR RELIEF**  
**(Contributory Copyright Infringement based upon material contribution)**

283. Plaintiffs re-allege and incorporate by reference the allegations contained in each of the foregoing paragraphs.

284. Through its activities, Defendants knowingly and intentionally took steps that are substantially certain to result in direct infringement of Plaintiffs' Copyrighted Works, and that have resulted in such direct infringement in violation of Plaintiffs' copyrights.

285. Despite Defendant's knowledge that their subscribers are using their service to engage in widescale copyright infringements, Defendants failed to take reasonable steps to minimize the infringing capabilities of their service.

286. Defendants are liable as contributory copyright infringers for the infringing acts of their subscribers. Defendants have actual and constructive knowledge of the infringing activity of their subscribers. Defendants knowingly caused and otherwise materially contributed to these unauthorized distributions of Plaintiffs' Works.

287. Defendants' infringements were committed "willfully" within the meaning of 17 U.S.C. § 504(c)(2).

288. By engaging in the contributory infringement alleged in this First Amended Complaint, Defendants deprived not only the producers of the Works from income that could have been derived when the respective film was shown in public theaters and offered for sale or rental, but also all persons involved in the production and marketing of this film, numerous owners of local theaters and retail outlets and their employees, and, ultimately, the local economy. Defendants' misconduct therefore offends public policy.

### **VIII. THIRD CLAIM FOR RELIEF (Vicarious Infringement)**

289. Plaintiffs re-allege and incorporate by reference the allegations contained in each of the foregoing paragraphs.

290. Defendants are vicariously liable for the infringing acts of their subscribers' infringements including but not limited to the subscribers' direct infringements of Plaintiffs' exclusive right to reproduce, distribute and publicly perform copies of their Works.

291. Defendants have the right and ability to supervise and control the infringing activities that occur through the use of their service, and at all relevant times have derived a direct financial benefit from the infringement of Plaintiffs' copyrights.

292. Defendants refused to take any meaningful action to prevent the widespread infringement by their subscribers despite having actual knowledge. Indeed, the ability of subscribers to use Defendants' service to reproduce and distribute copies of Plaintiffs' Works exactly as promoted and encouraged by Defendants without getting caught serves as a powerful draw for users of Defendants' services.

293. Moreover, the ability of subscribers to use Defendants' service to perform (stream) copies of Plaintiffs' Works from unauthorized locations exactly as promoted and encouraged by Defendants serves as a powerful draw for users of Defendants' services.

294. Defendants are therefore vicariously liable for the unauthorized reproduction, distribution and public performance of Plaintiffs' Works.

**VIII. FOURTH CLAIM FOR RELIEF  
(Contributory Copyright Infringement based upon Intentional Inducement)**

295. Plaintiffs re-allege and incorporate by reference the allegations contained in each of the foregoing paragraphs.

296. Defendants intentionally induced the infringement of Plaintiffs' exclusive rights under the Copyright Act, including infringement of Plaintiffs' exclusive rights to reproduce, publicly perform, and distribute copies of their Works.

297. As instructed and encouraged by Defendants, their subscribers purchase and install the VPN services of Defendants to conceal their identities while engaging in movie piracy.

298. As instructed and encouraged by Defendants, their subscribers install piracy

applications such as Popcorn Time on their devices while assigned IP addresses by the Defendants' VPN services to conceal their identities.

299. As instructed and encouraged by Defendants, their subscribers purchase and install the VPN service of Defendants so that subscribers can stream Plaintiffs' Works from legitimate platforms such as Netflix in violation of geographic restrictions.

300. Defendants' subscribers use piracy applications to connect to sources that publicly perform and/or distribute copies of Plaintiffs' Works while anonymously connected to the Internet by Defendants' VPN services.

301. Defendants' subscribers connect to notorious piracy websites such as YTS to download torrent files to reproduce and distribute copies of Plaintiffs' Works while anonymously connected to the Internet by Defendants' VPN services exactly as promoted and encouraged to do by Defendants.

302. Defendants induce direct infringements of Plaintiffs' Works by encouraging their subscribers to use movie piracy applications such as Popcorn Time and to access websites such as YTS that facilitate, enable, and create direct links between their customers and infringing sources, and by actively inducing, encouraging, and promoting their VPN services as a means to "safely" use movie piracy applications for blatant copyright infringement by assuring customers that their identification information will be concealed.

303. Defendants induce direct infringements of Plaintiffs' Works by encouraging their subscribers to use the VPN service to publicly perform (stream) copies of Plaintiffs' Works from and to unauthorized locations.

304. Defendants' intentional inducement of the infringement of Plaintiffs' rights in their Copyrighted Works constitutes a separate and distinct act of infringement.

**IX. FIFTH CLAIM FOR RELIEF  
(Digital Millennium Copyright Act Violations)**

305. Plaintiffs re-allege and incorporate by reference the allegations contained in each of the foregoing paragraphs.

306. Defendants' subscribers encourage their subscriber to access torrent files for copying copyright protected Works from notorious movie piracy websites such as YTS.

307. Defendants' subscribers knowingly and with the intent to induce, enable, facilitate, or conceal infringement of the Plaintiffs' copyright protected Works, distributed copyright management information ("CMI") that falsely included false wording such as "RARBG", "FGT", "MKVCAGE" and "YTS" in violation of 17 U.S.C. § 1202(a)(2).

308. Defendants' subscribers, without the authority of Plaintiffs, or the law, distributed removed or altered CMI knowing that the CMI had been removed or altered to include wording such as "RARBG", "FGT", "MKVCAGE" and "YTS" without the authority of Plaintiffs and knowing, or having reasonable grounds to know, that it will induce, enable, facilitate, or conceal infringement of Plaintiffs' copyright protected Works in violation of 17 U.S.C. § 1202(b)(2).

309. Defendants' subscribers, without the authority of Plaintiffs, or the law, distributed Plaintiffs' Copyright protected Works knowing that the CMI had been removed or altered to include wording such as RARBG", "FGT", "YTS" or "MKVCAGE", and knowing, or having reasonable grounds to know, that it will induce, enable, facilitate, or conceal infringement of the copyright protected Works in violation of 17 U.S.C. § 1202(b)(3).

310. Particularly, Defendants' subscribers knew that the CMI in the file names of the pieces had been altered to include wording such as "RARBG", "FGT", "YTS" or "MKVCAGE".

311. Particularly, Defendants' subscribers distributed the file names that included CMI that had been altered to include wording such as "MKVCAGE", "RARBG", "FGT" or "YTS".

312. Defendants' subscribers knew that the wording "MKVCAGE", "RARBG", "FGT" or "YTS" originated from notorious movie piracy websites which they themselves promoted.

313. Defendants' subscribers' acts constitute violations under the Digital Millennium Copyright Act, 17 U.S.C. § 1202.

314. Defendants are secondarily liable for the DMCA violations of their subscribers. Defendants had actual and constructive knowledge of their subscribers' DMCA violations. Defendants knowingly caused and otherwise materially contributed to these DMCA violations.

315. Defendants are vicariously liable for the DMCA violations of their subscribers. Defendants have the right and ability to supervise and control the DMCA violations that occur through the use of their service, and at all relevant times has derived a direct financial benefit from the DMCA violations complained of herein.

316. Defendants have refused to take any meaningful action to prevent the widespread DMCA violations by their subscribers. Indeed, the ability of Defendants' subscribers to distribute torrent files from torrent websites such as YTS that Defendants' subscribers themselves promote and obtain file copies of the Works with altered CMI and distribute said copies while concealing their end users' activities acts as a powerful draw for subscribers of Defendants. Defendants are therefore vicariously liable for its subscribers' DMCA violations.

317. Indeed, the ability of Defendants' subscribers to reproduces, stream and distribute illicit file copies of Plaintiffs' Works with altered CMI using BitTorrent Clients such as Popcorn Time that Defendants themselves promote while concealing their activities acts as a powerful draw for subscribers of Defendants. Defendants are therefore vicariously liable for their end users' DMCA violations.



318. Plaintiffs are entitled to an injunction to prevent Defendants from engaging in further violations of 17 U.S.C. § 1202.

319. Plaintiffs are entitled to recover from Defendants the actual damages suffered by Plaintiffs and any profits Defendants have obtained as a result of its wrongful acts that are not taken into account in computing the actual damages. Plaintiffs are currently unable to ascertain the full extent of the profits Defendant has realized by its violations of 17 U.S.C. § 1202.

320. Plaintiffs are entitled to elect to recover from Defendants statutory damages for its violations of 17 U.S.C. § 1202.

321. Plaintiffs are further entitled to costs and reasonable attorneys' fees.

**X. SIXTH CLAIM FOR RELIEF  
(Negligence against VPN Consumer Network Services and VPN Consumer Network)**

322. Plaintiffs re-allege and incorporate by reference the allegations contained in paragraphs 249-269.

323. VPN Consumer Network Services and VPN Consumer Network state in the Whois records of ARIN that it is the proper abuse contact for certain IP addresses.

324. VPN Consumer Network Services' and VPN Consumer Network's statement that it is the proper abuse contact for said certain IP addresses is false because they had allocated or reassigned said IP addresses to subscribers such as ExpressVPN that have their own end users.

325. VPN Consumer Network Services and VPN Consumer Network knew that their statement in the Whois records that it is the proper abuse contact for said certain IP addresses was false when it updated the Whois records.

326. VPN Consumer Network Services and VPN Consumer Network knows that their statement in the Whois records of ARIN that they are the proper abuse contact for said certain IP addresses is false, but it purposefully fails to update the Whois records.

327. VPN Consumer Network Services and VPN Consumer Network fail to exercise reasonable care or competence in publishing and maintaining the information in the Whois records. Indeed, VPN Consumer Network Services and VPN Consumer Network are obligated per their registration agreement with ARIN to update the Whois records when it assigned or reallocated said certain IP addresses to ExpressVPN.

328. Plaintiffs relied on VPN Consumer Network Services' and VPN Consumer Network's misrepresentations when determining the proper abuse contact for sending notices of infringement at the certain IP addresses.

329. Plaintiffs had a right to rely on VPN Consumer Network Services' and VPN Consumer Network's misrepresentations in the Whois records.

330. VPN Consumer Network Services and VPN Consumer Network knew that rightsowners including Plaintiffs were relying on their misrepresentations when determining the proper abuse contact for sending notices of infringement at the certain IP addresses.

331. Rights owners such as Plaintiffs are third party beneficiaries of VPN Consumer Network Services' and VPN Consumer Network's agreement with ARIN to properly update the Whois records so that they can promptly contact the responsible party to stop abuse.

332. VPN Consumer Network Services and VPN Consumer Network had a duty to rightsowners including Plaintiffs to publish accurate information in the Whois records.

333. Plaintiffs have suffered damages based upon VPN Consumer Network Services' and VPN Consumer Network's misrepresentations. Plaintiffs' agents have been unable to promptly send notices to the appropriate party that could and would have taken actions to stop further infringements of their Works.

334. The acts and misrepresentations of VPN Consumer Network Services and VPN

Consumer Network constitute negligent misrepresentation. Such conduct was the cause of Plaintiffs' damages, and Plaintiffs have incurred damage as a result of their misrepresentations.

335. ExpressVPN (BVI), ExpressVPN (Isle of Man), VPN Consumer Network Services and VPN Consumer Network are all alter egos and thus liable for the acts of each other.

**XIII. SEVENTH CLAIM FOR RELIEF  
(Fraud against VPN Consumer Network and VPN Consumer Network Services)**

336. Plaintiffs re-allege and incorporate by reference the allegations contained in paragraphs 249-269 and in the sixth claim for relief.

337. Defendant VPN Consumer Network Services and VPN Consumer Network falsely state in the Whois records that it is the proper abuse contact for said certain IP addresses.

338. VPN Consumer Network Services and VPN Consumer Network falsely stated in the Whois records on at least June 6, 2018 that VPN Consumer Network Services is the proper abuse contact for certain IP addresses in Miami, Florida where Plaintiffs' Works were pirated.

339. Plaintiffs had a right to rely on VPN Consumer Network Services' and VPN Consumer Network's misrepresentations in the Whois records. Indeed, VPN Consumer Network Services and VPN Consumer Network are obligated per their registration agreement with ARIN to update the Whois records.

340. VPN Consumer Network Services, VPN Consumer Network and ExpressVPN benefits by these false statements in the Whois records. For example, by false stating that VPN Consumer Network Services and VPN Consumer Network are the owner of the certain IP addresses, the general public would not know that ExpressVPN is subject to US jurisdiction from its alter ego VPN Consumer Network in San Francisco.

341. VPN Consumer Network Services, VPN Consumer Network and ExpressVPN benefit by their false statements in the Whois records because legitimate streaming platforms are

hindered from determining which IP addresses are allocated to ExpressVPN and thus should be blocked to prevent ExpressVPN's subscribers from streaming Plaintiffs' Works from unauthorized locations.

342. VPN Consumer Network Services and VPN Consumer Network benefits by their false statements in the Whois records by maintaining control of valuable IPv4 addresses allocated to them from ARIN.

343. Plaintiffs have suffered damages based upon these misrepresentations. Plaintiffs' agents have been unable to send notices to the appropriate party that could have and would have taken actions to stop further infringements of their Works.

344. The acts and misrepresentations of VPN Consumer Network Services and VPN Consumer Network constitute fraud and fraudulent misrepresentation. Such conduct was the cause of Plaintiffs' damages, and Plaintiffs have incurred damage as a result of VPN Consumer Network Services' and VPN Consumer Network's fraudulent acts and representations.

345. ExpressVPN (BVI), ExpressVPN (Isle of Man), VPN Consumer Network Services and VPN Consumer Network are all alter egos and thus liable for the acts of each other.

#### **PRAYER FOR RELIEF**

WHEREFORE, the Plaintiffs respectfully request that this Court:

(A) enter permanent injunctions enjoining Defendants from continuing to infringe and contribute to infringements of the Plaintiffs' copyrighted Works and contribute to DMCA violations;

(B) enter permanent injunctions ordering Defendants to stop interfering with standard technical measures by purposefully deleting subscriber log information;

(C) order Defendants to block their subscribers from accessing notorious piracy websites

of foreign origin including those listed in the annual trade report of Notorious Foreign Markets published by the United States Government such as (a) YTS; (b) Piratebay; (c) Rarbg; (d) 1337x; and (e) Popcorntime on networks under their control to prevent further pirating of Plaintiffs' Works;

(D) order Defendants to adopt a policy of logging user access and providing for the prompt suspension of subscribers for which it receives more than three unique notices of infringements of copyright protected Works and/or DMCA violations unless within 72 hours unless said subscriber makes a counter notification;

(E) award the Plaintiffs their actual damages from the copyright infringements and Defendants' profits in such amount as may be found; alternatively, at Plaintiffs' election, for statutory damages pursuant to 17 U.S.C. § 504(a) and (c) against (i) Defendants Surfshark, KeepSolid and ZenGuard, and (ii) against Defendants ExpressVPN (BVI), ExpressVPN (Isle of Man) VPN Consumer Network Services, and VPN Consumer Network jointly and severally;

(F) award the Plaintiffs actual damages from the DMCA violations and Defendants' profits in such amount as may be found; or, in the alternative, at Plaintiffs' election, for statutory damages per DMCA violation pursuant to 17 U.S.C. § 1203(c) for violations of 17 U.S.C. § 1202 against Defendants;

(G) award the Plaintiffs their reasonable attorneys' fees and costs pursuant to 17 U.S.C. § 505 and/or 17 U.S.C. § 1203(b)(5);

(H) enter an order pursuant to 17 U.S.C. §512(j) and/or 28 U.S.C §1651(a) that any service provider providing service for Defendants including but not limited to Leaseweb, Digital Ocean, QuadraNet and Total Server Solutions which they used to infringe Plaintiffs' Works immediately cease said service upon notice;

(I) award the Plaintiffs actual, special, general, compensatory, expectation, consequential, treble, exemplary, and/or punitive damages at an amount to be proven at trial for VPN Consumer Network Services' and VPN Consumer Network's negligent misrepresentations and/or fraudulent misrepresentations; and

(I) grant the Plaintiffs any and all other and further relief that this Court deems just and proper.

The Plaintiffs hereby demand a trial by jury on all issues properly triable by jury.

DATED: Kailua Kona, HI, August 24, 2021.

Respectfully submitted,

/s/ Kerry S. Culpepper

Kerry S. Culpepper,  
Virginia Bar No. 45292  
Counsel for Plaintiffs  
CULPEPPER IP, LLC  
75-170 Hualalai Road, Suite B204  
Kailua-Kona, Hawai'i 96740  
Tel.: (808) 464-4047  
Fax.: (202) 204-5181  
[kculpepper@culpepperip.com](mailto:kculpepper@culpepperip.com)