Michael O. Stevens, OSB No. 095198
michael@hillsborofirm.com
STEVENS & LEGAL, LLC
3699 NE John Olsen Avenue
Hillsboro, OR 97124
Tel: (971) 533-6178
Fax: (971) 228-2608

J. Curtis Edmondson, CASB No. 236105 (*pro hac vice*)
jcedmondson@edmolaw.com
Kiren Rockenstein, OSB No. 175638
kirenr@edmolaw.com
EDMONDSON IP LAW
3699 NE John Olsen Avenue
Hillsboro, OR 97124
Tel: (503) 336-3749
Fax: (503) 482-7418

David H. Madden, OSB No. 080396
dhm@mersenne.com
MERSENNE LAW LLC
9600 SW Oak Street, Suite 500
Tigard, OR 97223
Tel: (503) 679-1671
Fax: (503) 512-6113

Attorneys for Defendant JOHN HUSZAR

UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

PORTLAND DIVISION

DALLAS BUYERS CLUB, LLC, Plaintiff, v. **JOHN HUSZAR,** Defendant.	Case No.: **3:15-cv-0907-AC** DEFENDANT'S MOTION FOR SUMMARY JUDGMENT FRCP 56 **ORAL ARGUMENT REQUESTED**

NOTICE OF MOTION

Defendant John Huszar ("Huszar") moves for summary judgment of non-infringement on the grounds that Huszar has absolute immunity under 17 U.S.C. §§ 512(a) and 512(b) as the transactions at issue were routed through a Tor Exit Node; Plaintiff Dallas Buyers Club ("DBC") failed to produce a true and correct "depository copy" by the close of discovery, precluding DBC from proving its case under the best evidence rule; and DBC's torrent monitoring company misled this Court and other Courts about the quality and integrity of MaverickMonitor. This motion will be heard before the Honorable John Acosta in the District of Oregon, Federal Courthouse, located at 1000 SW 3rd Ave #740, Portland, OR 97204 pursuant to the scheduling order at Docket 133.

MEMORANDUM

I. SUMMARY

Huzar moves for summary judgment of non-infringement on the following grounds:

- Huszar has statutory copyright infringement immunity under 17 U.S.C. §§ 512(a) and 512(b) for an ISP (internet service provider), as he operated as an ISP with a Tor server; and/or
- DBC cannot "prove up" its case as DBC has failed to produce a true and correct "depository copy" by the close of discovery. This precludes DBC from satisfying an essential element of infringement; and/or
- Any data generated from the "MaverickMonitor" torrent monitoring system cannot be relied upon for the purposes of proving any "infringement". The software was built without any formal specifications, has no documentation, has never been tested, and has no reports on error rates.

II. INTRODUCTION

Huszar is the last defendant in an extensive litigation campaign, stretching from Sydney to Portland, the long way around, where DBC has sued thousands of defendants for allegedly downloading the movie *Dallas Buyers Club*, and has then asked for payments ranging from $2,000.00 to $10,000.00 for a $2.99 movie. The allegations are the same in all countries – defendants went to torrent sites, like "PirateBay" and downloaded the movie and infringed. What

these cases have in common, oddly enough, is a software company in Germany, known by various names, but here known as "Maverickeye" which makes the "detection" software "MaverickMonitor". MaverickMonitor is allegedly the cat's meow in torrent monitoring technology.

What distinguishes this case, from the other thousands, is that Huszar ran a Tor Server as an ISP, giving him statutory immunity. Also, Huszar did not agree with DBC, and rather than take their assertions at face value that the monitoring software was anything special, he hired an expert to look at and evaluate the code – Dr. Kal Toth. Dr. Toth's evaluation is telling; the code is nothing but a stitched together patchwork of open source software based on "Monotorrent". Despite the fact that MaverickMonitor could have chosen to verify the entire movie on the alleged infringer's hard drive, MaverickMonitor chose instead to grab only 16KB of raw data to "prove" infringement. 16KB out of a 4GB movie is a miniscule drop in the bucket, and certainly wholly insufficient to 'prove' infringement.

What is equally strange is despite producing this blockbuster hit, DBC, who has sued thousands of people, has never had a copy of the depository copy of the movie. The depository copy was sitting on film reels, likely at Universal Studios. That raises a bigger question – what was MaverickMonitor looking at when they compared the thousands of infringed works?

III. UNDISPUTED FACTS

A. There are both a theatrical film version and a DVD version of *Dallas Buyers Club*

DBC applied for and received a copyright certificate on the theatrical version of *Dallas Buyers Club*. (RJN 1-1). The theatrical version was published on November 1, 2013. *Id.* Six reels of film was deposited with the Copyright Office by Carly Seabrook. (RJN 1-2). The theatrical version of the movie was released in the United States at the Mill Valley Film Festival on October 10, 2013. (RJN 1-3).

The theatrical version was subsequently reedited into a "DVD". The DVD version of the film was released on February 4, 2014. (RJN 1-4). The DVD version contains extra material not present in the theatrical version. (See *Vorrath* Decl,). Namely, the DVD version contains extra material not present in the theatrical version.

B. DBC hires MaverickMonitor to track infringements

Beginning in 2013, DBC began a campaign to sue individuals in the United States and other countries for alleged infringement. Over 300 lawsuits were filed in the United States against at least 1000 defendants.

The MaverickMonitor software has no formal specifications, no test plan, no user manual, or any documentation commonly associated with commercial software development. (See *Toth* Decl.). There is no documentation describing how the software works in real-time, what type of computer servers it operates on, how many computer servers it operates on, the failure rate of either the computer servers and/or the software. There was no documentation on how a particular torrent is located, how the torrent is processed, how the hash is processed, how data is collected from the swarm, and how a PCAP (packet capture) is generated. (See *Rockenstein* Decl., Exhibit 1, *Toth* Expert Report)

This software was developed by one or two programmers in German who have had no formal training in software development or validation processes.

C. Defendant Huszar operates an ISP with Tor installed

Huszar runs a small ISP in Oregon City where he configured a "Tor Exit Relay" using IP address 173.11.1.241. The Tor virtual machine (VM) was located on a server that also stored multiple business-related VMs. The Tor VM operated entirely independently and was the only VM with access to the IP address at issue in this case. (Docket 40 aka Second Huszar Decl. ¶ 17;

Docket 39 aka First Huszar Decl. ¶ 8; Huszar Dep. 47:24-48:2.)

D. This Lawsuit

On May 27, 2015, DBC sued Integrity Computer Systems for the infringement of Dallas Buyers Club (Docket 1) as a "Doe". On October 29, 2015, Huszar made a "pro-se" appearance at Docket 15, stating that his system had no record of the infringing materials. Huszar offered to help then Plaintiff's attorney Carl Crowell locate the infringer, but was rebuffed. On November 3, 2015, Crowell moved to strike Huszar's appearance; oddly Crowell made no mention that Huszar tried to cooperate. Then Crowell filed an opposition to Huszar's motion appearance at docket 15. (Docket 22). Huszar responded to Crowell's opposition. (Docket 26). Huszar raised several defenses, including the DMCA Defense. (Docket 27-1).

The case progressed. An order was entered instructing an adverse jury instruction be entered. (Docket 95). Discovery was taken on DBC's 30(b)(6) designee on topics regarding the "works" (Michael Wickstrom); and the operation of the BitTorrent monitoring system, (Robert Young).

IV. ARGUMENT

Summary judgment is appropriate "if the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law." *Celotex Corp. v. Catrett,* 477 U.S. 317, 323, 106 S. Ct. 2548 (1986). "To establish a claim of copyright infringement by reproduction, the plaintiff must show ownership of the copyright and copying by the defendant." *Kelly v. Arriba Soft Corp.,* 336 F.3d 811, 817 (9th Cir. 2003).

1. SUMMARY JUDGMENT IS APPROPRIATE AS HUSZAR OPERATED A TOR EXIT NODE; DBC FAILED TO PRODUCE THE DEPOSITORY COPY; AND DBC REPEATEDLY MISLED THIS COURT ABOUT THE SOURCE

AND INTEGRITY OF THE BITTORRENT MONITORING SYSTEM

A. Huszar has statutory immunity under 17 U.S.C. §§ 512(a) and 512(b)

When the world-wide-web exploded in 1993 with the introduction of the Mozilla web browser, copyrighted material was passed through ISPs. In 1998, Congress passed the Digital Millennium Copyright Act (DMCA) to protect computer operators from liability when transitory material passed through their networks. 17 U.S.C. § 512.

17 U.S.C. § 512(a) states as follows:

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

17 U.S.C. § 512(b) states as follows:

> (b) System Caching.—
> (1)Limitation on liability.—A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the

> intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which—
> (A) the material is made available online by a person other than the service provider;
> (B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and
> (C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A), if the conditions set forth in paragraph (2) are met.

17 U.S.C. § 512(a), provides broad immunity to service providers that merely serve as conduits or caching servers for internet communications. As stated in *Perfect 10, Inc. v. CCbill LLC*, 488 F.3d 1102 (9th Cir. 2007):

> Section 512(a) provides a broad grant of immunity to service providers whose connection with the material is transient. When an individual clicks on an Internet link, his computer sends a request for the information. The company receiving that request sends that request on to another computer, which sends it on to another. After a series of such transmissions, the request arrives at the computer that stores the information. The requested information is then returned in milliseconds, not necessarily along the same path. In passing the information along, each intervening computer makes a short-lived copy of the data. A short time later, the information is displayed on the user's computer.

Tor (The Onion Router) is open source software that allows a person to configure their computer to serve as an "exit point" for internet browsing for any other computer on the internet. (See *Edmondson* Decl, Exhibits 4 and 5). In short, the software allows a person to act as a public service "virtual private network". Tor has many laudable uses, for example, if you are critical of the Venezuelan government, you can make a post to a political blog from Caracas without having the security police trace your IP address and throw you in jail. The negative aspect of Tor is that some people may use it for infringing uses. In either case, the operator of the Tor exit node cannot

monitor the transactions, nor be held responsible for their transmission.

Plaintiff has made no allegations, nor produced any evidence, that would support its claims that Huszar did anything besides run an ISP. In fact, Plaintiff admitted as much as explaining that 17 U.S.C. § 512(c) cannot be used as a defense in this case. (See Docket 22). Further, under examination from Mr. Crowell at Huszar's deposition, there was no dispute a Tor node was used. (See Exhibit 1, Huszar Deposition on February 2, 2016).

Further, this Court recognized Huszar was running a Tor Service as a Service Provider. As stated at Docket 95:

> Defendant decided to stop running the Tor Node because of the demands of this lawsuit and Plaintiff's counsel, and as such Defendant was not concerned about migrating the Tor VM or losing the Tor software and associated data when he used the RAID tool to overwrite the hard drives in an attempt to repair the drives.

What distinguishes this case from the "run of the mill BitTorrent case" is Plaintiff produced evidence that the alleged infringer was using a Tor Node.

B. DBC failed to produce the depository copy

To establish a *prima facie* case of copyright infringement, a plaintiff "must show ownership of the allegedly infringed material" and "demonstrate that the alleged infringers violated at least one exclusive right granted to copyright holders under 17 U.S.C. § 106." *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1013 (9th Cir. 2001). In order to obtain a copyright registration, an applicant must deposit as a part of his application a "copy" or "copies" of the original work.

Put simply, DBC must do three things to prove infringement of its movie:

1) Provide the registration certificate;

2) Produce a copy of the work that is the subject of the registration certificate; and

3) Show that Huszar copied (e.g. violated the exclusive right) for that work.

DBC failed to produce evidence regarding the second element – the depository copy that it needs to make the comparison. Since DBC did not provide these documents to Huszar by the discovery cutoff, it is precluded from using substitute documents (such as the movies in the .tar files).

> Federal Rules Evidence (FRE) 1002, states:
>
> An original writing, recording, or photograph is required in order to prove its content unless these rules or a federal statute provides otherwise.

FRE 1002 aims to guard against incomplete or fraudulent proof by requiring the possessor of an original to produce it, unless it can be shown to have been lost or destroyed through no fault of the proponent. While FRE 1002 has most often been invoked in contract cases, it has also been invoked in cases dealing with copyright infringement when trying to assess the "substantial similarity" of an allegedly infringing work to the original. *See Seiler v. Lucasfilm, Ltd*., 808 F.2d 1316, 1319 (9th Cir. 1987) ("There can be no proof of 'substantial similarity' and thus of copyright infringement unless Seiler's works are juxtaposed with Lucas' and their contents compared.") (applying the best evidence rule in a copyright action); *id*. ("[P]roof of the infringement claim consists of the works alleged to be infringed."); *accord Airframe Sys., Inc. v. L-3 Commc'ns Corp*., 658 F.3d 100, 107 (1st Cir. 2011) ("Having presented no evidence sufficient to prove the content of its registered source code versions, Airframe cannot show that any of its registered works is substantially similar to the allegedly infringing M3 program."); *Gen. Universal Sys., Inc. v. Lee*, 379 F.3d 131, 146 (5th Cir. 2004) (*per curiam*) ("Without providing its own source code for comparison, GUS did not satisfy the requirement that the infringed and infringing work be compared side-by-side.").

Absent evidence of the copyrighted work and the allegedly infringing works, the record is

insufficient to allow appellate review of the jury's verdict. *See, e.g., Olson v. Nat'l Broad. Co.*, 855 F.2d 1446, 1448, 1451 (9th Cir. 1988) (granting JMOL to copyright defendant because no reasonable jury could have found substantial similarity); *cf. Shaw v. Lindheim*, 919 F.2d 1353, 1355 (9th Cir. 1990) ("We have frequently affirmed summary judgment in favor of copyright defendants on the issue of substantial similarity.").

The court in *Seiler* also addressed the issue of the copyright registration stating that while "Section 410(c) makes the copyright certificate prima facie evidence of "the validity of the copyright and of the facts stated in the certificate."…", "None of the statements in the certificate can be of any use therefore until Seiler proves that the reconstructions are the same as the originals. Prima facie evidence of statements in the certificate is irrelevant until that proof has been made.".

During discovery, Huszar requested categories of documents which included the depository copies (Defendant's Requests for Production, Second Requests (No. 19)). DBC did not provide the depository copies. Discovery closed in this case on January 12, 2018, and no depository copy was provided by this date. It was the responsibility of DBC to provide Huszar with a copy of the depository works, since the work was not produced, it is impossible for DBC to lay the foundation for its case, as these documents were not produced in discovery.

DBC may argue that Huszar is required to access the depository directly from the Copyright Office. The problem with this is that DBC has not provided any evidence that this depository copy is the same as the version they allege has been infringed. The DVD/online streaming version are not the original documents. FRE 1002. Since DBC will not have the copyrighted work available for its case in chief, there is nothing for DBC to "compare against" for the purpose of proving infringement. DBC's case fails as a matter of law, and judgment should be entered in favor of Huszar.

C. Results and data regarding infringement from MaverickEye's torrent "monitoring" software are inadmissible

Huszar requested DBC produce a copy of the source code, documentation, test data, etc. that was used to monitor Huszar's IP address. DBC initially objected to this request, but the parties agreed that the code and any other documents related to the code would be produced.

Huszar retained Dr. Kal Toth who looked at the code and produced a report. Dr. Toth is eminently qualified to testify on software verification, validation, and reliability having managed the development of such systems in industry and taught hundreds of students in Portland on industry standards for the development of reliable software. Dr. Toth did a thorough examination of the code and found that it is based on an open source computer program known as "Monotorrent" and "SharpPcap". There is no real evidence in the code where the programs had been modified, nor is there any apparent release history documented in the code. Some of Dr. Toth's observations from his report are:

> ¶5.6 - The reliability of MaverickMonitor cannot be assessed without objective evidence that recommended patches and updates released by the open source development teams, namely, MonoTorrent and SharpPcap, have been applied or installed. Such evidence has not been provided.
>
> ¶5.7 - MaverickMonitor has a large code base of over 140,0000 lines of source code (LOC). This means that the number of latent (undetected) defects could be quite large. There is no evidence of effective testing.
>
> ¶5.11 - No evidence has been provided that adequate testing was conducted during development. Patzer in [3a, Skype Deposition of Michael Patzer, October 13, 2016] confirmed that his team did not test the BitTorrent software to verify that it operated correctly.
>
> **In the absence of verifiable evidence, an objective software professional cannot conclude that MaverickMonitor detects the IP addresses of infringing BitTorrent users correctly, consistently and reliably.**
>
> **(**See *Rockenstein* Decl, Exhibit 1, *Toth* Expert Report**)**

At issue here is whether this Court would admit data created by an untested and unverified computer system. Ultimately, software cannot "testify", only an expert can testify as to what the software produces. The Seventh Circuit looked at this issue and denied admissibility of expert testimony under *Daubert* where all the expert did was "rely" on advertisements about a software product. *Autotech Technology v. Automationdirect.Com*, 471 F.3d 745, 749 (7th Cir. 2006). Bizarrely, DBC's fact and expert witness, Robert Young, testified that he never installed and ran the MaverickMonitor software on any server despite being designated by DBC as its 30(b)(6) designee on software. (See Exhibit 2, Young Deposition, p. 106:15-18). DBC, a company that used software to sue thousands of people, has no idea how this software works.

An expert cannot "create" reliable data from an "unreliable" computer system. Perhaps Maverickmonitor worked 50% of the time. The problem is that we have no idea for this case which side of the coin was up for Huszar, nor does DBC, or MaverickMonitor. It is, technically speaking, simply the equivalent of a random number generator, and as such any data generated from the MaverickMonitor system should be excluded. As such DBC has no data whatsoever to show that Huszar infringed.

CONCLUSION

DBC has sued thousands of people in the United States and many more across the world for the alleged infringements of its movie, *Dallas Buyer's Club*. All of this was done using a flawed and unreliable BitTorrent monitoring system known as MaverickMonitor. If the Court had known this software was of such poor quality and reliability, would they have even allowed early discovery under FRCP 26? That is a question that may never be answered since these motions are

brought *ex-parte* before there is any discovery. However, here Huszar demonstrated with an inspection of the code that MaverickMonitor's claim of "100% accuracy" is a complete fraud.

Huszar respectfully requests this Court grant his motion for summary judgment and deem him the prevailing party.

DATED: February 28, 2018

Respectfully submitted,

STEVENS & LEGAL, LLC

/s/ Michael O. Stevens
Michael O. Stevens, OSB No. 095198
michael@hillsborofirm.com
Attorney for Defendant