
IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF UTAH

JAMES SEAVER and DEBORAH
SEAVER, as parents and heirs of G.S.,
deceased,

Plaintiffs,

v.

The ESTATE of ALEXANDRE
CAZES, deceased, a citizen of
Canada, formerly doing business as
ALPHABAY; THE TOR PROJECT,
INC. aka THE ONION ROUTER, a
Massachusetts non-profit corporation;
CHINA POSTAL EXPRESS &
LOGISTICS COMPANY aka CHINA
POST aka CHINA COURIER
SERVICES CORPORATION, a
Chinese corporate or governmental
entity; and EMS COOPERATIVE dba
EXPRESS MAIL SERVICE, a foreign
entity,

Defendants.

**MEMORANDUM DECISION AND
ORDER**

Case No. 2:18-cv-712-DB

District Judge Dee Benson

Before the court is a Motion to Dismiss filed by Defendant The Tor Project, Inc. (“Tor”). (Dkt. No. 13.) The Motion has been fully briefed by the parties, and the court has considered the facts and arguments set forth in those filings. Pursuant to civil rule 7-1(f) of the United States District Court for the District of Utah Rules of Practice, the Court elects to determine the motion on the basis of the written memoranda and finds that oral argument would not be helpful or necessary. DUCivR 7-1(f).

Facts

This action arises from the death of G.S., a 13 year-old boy, caused by ingesting the illicit drug U-47700. (Complaint, Dkt. No. 2, ¶¶ 9, 10.) The parents of G.S. have brought suit against the website that sold the drug to G.S., the service provider that created the network through which G.S. was able to access the website on the dark web (Tor), and the mail service that sent the drug to G.S. (*Id.* ¶¶ 14, 15, 24, 25.) Plaintiffs have brought claims for strict products liability, negligence, abnormally dangerous activity, and civil conspiracy. (*See id.*)

Tor is a Massachusetts corporation with its principle place of business in Norton, Massachusetts. (*Id.* ¶ 3.) Tor provides software for enabling anonymous communication and transactions on the internet. (Dkt. No. 13.) To use the Tor Browser, an individual must visit Tor's website to download the software. (*Id.*) When downloaded, installed, and used by an end-user such as G.S., the Tor Browser automatically starts Tor background processes and routes Internet traffic through the Tor network, which relays traffic through a worldwide network. (*Id.*) The Tor network provides security to a user's location and Internet usage to anyone conducting network surveillance or traffic analysis. (*Id.*)

The Tor Browser operates through a group of volunteer-operated servers whose users employ the Tor network by connecting through a series of virtual tunnels, or relays, rather than making a direct connection. (Dkt. No. 16.) Tor estimates, on average, between 350,000 and 400,000 directly connecting users in the United States over the past three months. (*Id.*) Information regarding the location of these users and relays is not publicly available. (*Id.*) Via its website, Tor invites users to run a relay in order to help the network grow. (*Id.*)

Discussion

Personal Jurisdiction

Tor first moves to dismiss Plaintiff's Complaint on the grounds that the court does not have personal jurisdiction over Tor. When, as in this case, a court considers a motion to dismiss "on the basis of the complaint and affidavits," a plaintiff must "only make a *prima facie* showing of personal jurisdiction." *Dudnikov v. Chalk & Vermilion Fine Arts, Inc.*, 514 F.3d 1063, 1070 (10th Cir. 2008). The plaintiff may make this *prima facie* showing by demonstrating by affidavit or other written materials, facts that if true would support jurisdiction over the defendant. *OMI Holdings, Inc. v. Royal Ins. Co.*, 149 F.3d 1086, 1091 (10th Cir. 1998). "[A]ny factual disputes in the parties' affidavits must be resolved in plaintiffs' favor." *Dudnikov*, 514 F.3d at 1070. In order to defeat the plaintiff's *prima facie* showing of personal jurisdiction, the moving defendant must present a compelling case demonstrating "that the presence of some other considerations would render jurisdiction unreasonable." *OMI Holdings*, 149 F.3d at 1091 (quoting *Burger King Corp. v. Rudzewicz*, 471 U.S. 462, 477 (1985)).

To obtain personal jurisdiction over a nonresident defendant in a diversity action, a plaintiff must show (1) that jurisdiction is legitimate under the laws of the forum state, and (2) that the exercise of jurisdiction does not offend the due process clause of the Fourteenth Amendment. *Soma Medical Int'l v. Standard Chartered Bank*, 196 F.3d 1292, 1295 (10th Cir. 1999).

Utah law expressly states that the Utah state long arm statute must be interpreted broadly "so as to assert jurisdiction over nonresident defendants to the fullest extent permitted by the due process clause of the Fourteenth Amendment to the United States Constitution." Utah Code §

78B-3-201; *see also Starways, Inc. v. Curry*, 980 F.2d 204, 206 (Utah 1999) (“We have held that the Utah long-arm statute ‘must be extended to the fullest extent allowed by due process of law.’”) (quoting *Synergetics v. Marathon Ranching Co.*, 701 F.2d 1106, 1110 (Utah 1985)). Because the Utah long-arm statute confers the maximum jurisdiction permissible consistent with the Due Process Clause, the court proceeds to determine whether the exercise of personal jurisdiction over Defendants meets federal due process standards.

A “court may exercise personal jurisdiction over a nonresident defendant only so long as there exist ‘minimum contacts’ between the defendant and the forum state.” *World Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 291 (1980) (quoting *International Shoe*, 326 U.S. at 316). The minimum contacts standard can be met in two ways. First, a court may assert specific personal jurisdiction over a nonresident defendant where “the defendant has ‘purposefully directed’ his activities at residents of the forum, and the litigation results from alleged injuries that arise out of or are related to those activities.” *Burger King*, 471 U.S. at 472. Where no nexus exists between the forum-related activity and the injury sustained, the court may nevertheless exercise general jurisdiction over the defendant when the defendant’s contacts are “so pervasive that personal jurisdiction is conferred by the ‘continuous and systematic’ nature of the defendant’s in-state activities.” *OMI Holdings*, 149 F.3d at 1090-91. Contacts sufficient to establish general jurisdiction must “approximate physical presence in the state.” *Shrader v. Biddinger*, 633 F.3d 1235, 1243 (10th Cir. 2011)(internal citation omitted).

The court is presented with a unique issue here, because the very essence of Tor’s business is privacy and anonymity. Tor’s network relies on volunteers who download its product nationwide to operate effectively, but the court does not have before it specific data about those

users or the exact number of users in Utah. However, as Plaintiff observed, given the volume of users Tor claims to have, the number of Tor users in Utah is likely to be between 3,000 and 4,000 each day. (Dkt. No. 16.)

The Tenth Circuit has often applied a “sliding-scale” test to determine whether minimum contacts exist to support personal jurisdiction over an internet-based business. With respect to “interactive Web sites where a user can exchange information with the host computer[,]...the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site.” *Shrader v. Biddinger*, 633 F.3d 1235, 1242 n.5 (10th Cir. 2011).

Tor is a uniquely interactive and commercial website. In order to use the service, a user must download the Tor browser. Many Tor users actually become part of the service by accepting Tor’s invitation to run a relay in order to help the network grow. Tor also enables a large set of commercial transactions on the dark web that would otherwise not be possible. Plaintiff has set forth substantial evidence to support the assumption that many of these transactions and relays are occurring in Utah on a daily basis. The court finds that Plaintiff has provided sufficient evidence to set forth a prima facie showing that Tor maintains continuous and systematic contacts in the state of Utah so as to satisfy the general jurisdiction standard. The court also finds that the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

Communications Decency Act

The court nevertheless finds that dismissal is appropriate because Plaintiff’s claims are barred by the Communications Decency Act, 47 U.S.C. § 230 (the “CDA”). The CDA provides

that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” 47 U.S.C.

§230(c)(1). The CDA further provides that “[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.” *Id.* §

230(e)(3). Through these provisions, the CDA “creates a federal immunity to any state law cause of action that would hold computer service providers liable for information originating with a third party.” *Ben Ezra, Weinstein, & Co. v. Am. Online Inc.*, 206 F.3d 980, 984–85 (10th Cir. 2000).

In order to qualify for immunity under the CDA, a defendant must show that 1) it is an “interactive computer service”; 2) its actions as a “publisher or speaker” form the basis for liability; and 3) “another information content provider” provided the information that forms the basis for liability. *Silver v. Quora, Inc.*, 666 F. App'x 727, 729 (10th Cir. 2016). The purpose of this immunity is to “facilitate the use and development of the Internet by providing certain services an immunity from civil liability arising from content provided by others.” *F.T.C. v. Accusearch Inc.*, 570 F.3d 1187, 1195 (10th Cir. 2009).

First, Tor qualifies as an interactive computer service. An “interactive computer service” is “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet....” 47 U.S.C. §230(f)(2). Tor fits this definition squarely because it enables computer access by multiple users to computer servers via its Tor Browser.

Second, Plaintiff seeks to hold Tor liable for information regarding the illicit drug U-47700 that G.S. was able to access through the Tor Browser. In other words, Plaintiff seeks to treat Tor as the “publisher or speaker” of third party information—“a result [the CDA] specifically proscribes.” *Ben Ezra, Weinstein, & Co., Inc. v. Am. Online Inc.*, 206 F.3d 980, 986 (10th Cir. 2000).

Third, the content that provides the basis for liability here—information regarding U-47700 and the ability to purchase it on the dark web—was not created by Tor. Rather, a third party provided the information and G.S. accessed it through use of the Tor Browser. “A service provider must ‘specifically encourage[] development of what is offensive about the content’ to be ‘responsible’ for the development of offensive content. *Silver*, 666 F. App’x at 729–30 (quoting *Accusearch*, 570 F.3d at 1199). Plaintiff has not alleged that Tor played any part in the creation of the content accessed by G.S.

All of Plaintiff’s claims are state law causes of action that would hold Tor, an internet service provider, liable for information originating with a third party. Those claims are barred by the CDA. Accordingly, Plaintiff’s claims against Tor are dismissed.

Conclusion

For the foregoing reasons, Tor's Motion to Dismiss is GRANTED and Plaintiff's Complaint against Tor is hereby DISMISSED pursuant to the Communications Decency Act, 47 U.S.C. § 230.

DATED this 20th day of May, 2019.

BY THE COURT:

A handwritten signature in black ink that reads "Dee Benson". The signature is written in a cursive style with a long horizontal stroke at the end.

Dee Benson
United States District Judge