UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

VIKEN DETECTION CORPORATION; PETER ROTHSCHILD, Plaintiffs, v. JOHN DOE, Defendant.	No. 19-cv-12034-NMG

MEMORANDUM OF DECISION ON MOTION FOR LEAVE TO ISSUE THIRD PARTY SUBPOENAS

CABELL, U.S.M.J.

Plaintiffs Viken Detection Corporation and one of its principals, Dr. Peter Rothschild, seek an injunction and damages against a John Doe defendant for several instances of alleged unauthorized access of Dr. Rothschild's online Dropbox accounts. These accounts contained trade secrets belonging to the Viken Detection Corporation. They bring their complaint under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, 1030(g), *et seq*., and the Stored Communications Act (SCA), 18 U.S.C. § 2701, 2707(a).

The person or persons responsible for allegedly accessing the accounts are currently only known to the plaintiff by reference to their IP address, a unique alphanumerical label assigned to any device connected to a computer network. The IP addresses of the person(s) responsible for the alleged intrusions were recorded by

Dropbox when the unknown user(s) accessed Dr. Rothschild's accounts. Dropbox has provided these IP addresses to the plaintiffs as well as corresponding dates and times when the accounts were accessed.

The only way the plaintiffs can realistically proceed in this lawsuit against the John Doe defendant(s) is to learn their identity by subpoenaing the Internet Service Provider(s) (ISP) connected to the IP addresses. To this end the plaintiffs have filed a Motion for Leave to Serve Third Party Subpoenas Prior to Rule 26(f) Conference. (D. 2). For the following reasons, the motion will be ALLOWED.

Legal Standard

Allowing the subpoena of third parties prior to the Rule 26(f) conference is allowed under Fed. R. Civ. P. Rule 26(d)(1), where good causes exists. *See*, *e.g.*, *Disc. Video Ctr., Inc.* v. *Does* 1-29, 285 F.R.D. 161, 163 (D. Mass. 2012) (discussing good cause standard for expedited discovery). Properly executed, a subpoena to an ISP to unmask the identity of a John Doe defendant can meet that standard. *See e.g., Kimberlite Corp. v. John Does* 1-20, No. C08-2147 TEH, 2008 WL 2264485, at *1 (N.D. Cal. June 2, 2008) (denying motion to quash ISP subpoenas in CFAA context).

Issuing subpoenas to reveal the identity of the individual behind an IP address is prevalent in litigation surrounding copyright infringement as a result of illegally downloaded media.

See e.g., Patrick Collins, Inc. v. *Does 1-79*, 286 F.R.D. 160, 165 (D. Mass. 2012); *Digital Sin, Inc*. v. *Does* 1-176, 279 F.R.D. 239, 242 (S.D.N.Y. 2012); *Breaking Glass Pictures* v. *Swarm Sharing Hash File SHA1: £973F491D02C1E0220DBC534D8F8EDC15FC53FAEF*, No. CIV. 13-10735-PBS, 2013 WL 2407226, at *1 (D. Mass. May 1, 2013). It also occurs in the context of online defamation. *McMann* v. *Doe*, 460 F. Supp. 2d 259, 261 (D. Mass. 2006).

Given the potential for misuse of subpoenas to unmask otherwise anonymous individuals via their ISP, the sessions in this district have employed, and the plaintiffs invite us to use, the five-factor test enunciated in *Sony Music Entm't Inc. v. Does 1-40*, 326 F. Supp. 2d 556 (S.D.N.Y. 2004). *See, e.g*. *London-Sire Records, Inc*. v. *Doe 1*, 542 F. Supp. 2d 153, 164 (D. Mass. 2008) (applying the *Sony Music* test).

Sony Music lists the factors a judge should consider when deciding whether to issue an identity unmasking ISP subpoena as: (1) a concrete showing of a prima facie claim of actionable harm; (2) specificity of the discovery request; (3) the absence of alternative means to obtain the subpoenaed information; (4) a central need for the subpoenaed information to advance the claim; and (5) the party's expectation of privacy. *Id.*

As set forth in their complaint and memorandum of law (D. 1,3), the plaintiffs have alleged a prima facie case of a violation

of the CFAA and SCA[1], seek only the identifying information of the alleged infringer, have no other means of obtaining this information, cannot proceed without the information, and at this stage sufficiently demonstrate that the John Doe defendant would have no expectation of privacy while committing violations of the CFAA and/or SCA. As such, the subpoenas shall issue subject to the conditions set out below and in the accompanying order.

Instructions Regarding Subpoenas

In accordance with practice in this and other courts, the subpoenas must be served alongside a special notice to the target of the subpoenaed information informing them of a 30-day period in which they may move to quash the subpoena. *See, e.g., Disc. Video Ctr., Inc. v. Does 1-29, 285 F.R.D. 161, 162 (D. Mass. 2012); Kimberlite,* 2008 WL 2264485, at *3 citing *UMG Recordings, Inc.* v. *Does 1-4*, No. 06-0652 SBA (EMC), 2006 WL 1343597, at *3 (N.D. Cal. Mar. 6, 2006)("Given the privacy ... interests that inhere in the records sought, this Court has the authority under the Federal Rules to condition the subpoena on consumer notice and an opportunity to be heard.").

[1] Given that the plaintiffs are proceeding under theories of federal law (CFAA, SCA) and not solely on state claims, the concerns enunciated in *McMann* v. *Doe*, 460 F. Supp. 2d 259, 263 (D. Mass. 2006) do not arise. (ex parte John Doe subpoenas should not issue when plaintiff proceeds in federal court solely on state law claims under diversity jurisdiction because John Doe defendant could be revealed to be citizen of the same state as plaintiff, meaning court acted without jurisdiction).

/s/ Donald L. Cabell_____
DONALD L. CABELL, U.S.M.J.

DATED: October 17, 2019