UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF KENTUCKY
BOWLING GREEN DIVISION
CIVIL ACTION NO. 1:19-CV-00142-GNS-HBB

N. HARRIS COMPUTER CORPORATION;
COLOSSUS, INC.; AND
INTERACT911 CORPORATION PLAINTIFFS

V.

DSI INVESTMENTS, LLC;
DIGITECH SERVICES, INC.;
DAVID C. OGLES; AND
E-JAIL, LCC DEFENDANTS

MEMORANDUM OPINION & ORDER

BACKGROUND

Before the Court is the motion of the Defendants and non-party Simpson County Detention Center ("SCDC"), pursuant to Fed. R. Civ. P. 45(d), for modification or quashing of a subpoena issued by Plaintiffs to SCDC (DN 62).[1] Plaintiffs have filed a response (DN 66); Defendants and SCDC filed a reply (DN 73); Plaintiffs filed a surreply (DN 77); and Defendants filed a sur-surreply (DN 79).

[1] Plaintiffs have not challenged Defendants' standing to move to quash the subpoena issued to SCDC. The Court observes that motions to quash subpoenas are governed by Rule 45(d)(3). See Black v. Kyle-Reno, No. 1:12-CV-503, 2014 WL 667788, at *1 (S.D. Ohio Feb. 20, 2014). Typically, a party does not have standing to quash or object to a Rule 45 subpoena served on a non-party, unless the party can demonstrate a privilege or other personal right in regard to the requested documents. See, e.g., Sys. Prods. & Solutions, Inc. v. Scramlin, No. 13-CV-14947, 2014 WL 3894385, at *7 (E.D. Mich. Aug. 8, 2014) (addresses standing to quash); Iron Workers' Local Pension Fund v. Watson Wyatt & Co., Nos. 04-CV-40243, 07-CV-12368, 2009 WL 648503, at *6 (E.D. Mich. Mar. 10, 1999) (addresses standing to object). Here, Defendants assert a personal right regarding the information requested from SCDC.

NATURE OF THE CASE

In 2002, Defendant Ogles developed a computer software product called JailTracker, a jail management program for use by detention facilities. Ogles registered the copyright with Defendant Digitech Services. In 2012, the Defendants entered into an Asset Purchase Agreement selling JailTracker to Plaintiffs, which develops and markets computer software programs. Ogles also executed a Confidentiality, Assignment of Inventions, Non-Competition and Non-Solicitation Agreement. Ogles became an employee of Plaintiff Colossus, which was subsequently acquired by Plaintiff Harris Corp. Eventually, Ogles' relationship with Harris Corp. deteriorated, and his employment was terminated on March 26, 2019.

Ogles developed a computer software program called E-Jail, also a jail management program for use by detention facilities. Plaintiffs contend that the Defendants violated the restrictive covenants and infringed their copyright by copying the JailTracker software and using it to create E-Jail. The Defendants assert that E-Jail is a distinctly different product from JailTracker and was created without reliance on JailTracker's programming. Plaintiffs and Defendants also assert other claims against each other, but those are not relevant to the present motion.

MOTION TO MODIFY OR QUASH

SCDC was previously a JailTracker client and served as the real-world application test site for E-Jail. Plaintiffs previously issued a subpoena to SCDC for documents related to E-Jail, JailTracker, and communications between SCDC and the Defendants related to the products. SCDC responded to the subpoena. Plaintiffs subsequently issued a second subpoena to SCDC, which is the subject of the motion. Defendants' motion initially sought broad protection (DN 62).

However, over the course of briefing the motion, the scope of the requests for which protection is sought has been narrowed to three of the requests[2]:

> Request No. 1: Documents regarding the performance, features and functionality of E-Jail.
>
> Request No. 2: Documents regarding any software bugs, complaints or quality concerns of E-Jail.
>
> Request No. 4: Documents regarding the build, install, setup, run and operation of E-Jail.

Defendants and SCDC indicate that SCDC has email and text messages relating to E-Jail that could be considered responsive to the Requests. While SCDC has already produced email and text messages through March 26, 2020, it has not produced those generated subsequent to that date. Defendants also indicate that there have been modifications to E-Jail, and Plaintiffs have not been given access to any versions other than the "original" version. The Defendants and SCDC assert a number of grounds upon which the information is not subject to disclosure.

1. March 26, 2020 as the cutoff for discoverable documents.

Ogles' employment with the Plaintiffs terminated on March 26, 2019. Defendants point to the 2012 agreement, which restricted Ogles from marketing or selling a competing product to a JailTracker customer for a year after the end of his employment. That prohibition, Defendants contend, expired on March 26, 2020 and any efforts Ogles made to market or sell E-Jail since then "is none of Plaintiffs' business" (DN 73, p. 5). The current subpoena, Defendants contend, is nothing more than an effort to "keep tabs on what their competitor is doing" (Id.).

Plaintiffs contend that the Defendants ignore the full scope of the claims they have asserted. Responsive documents generated after March 26, 2020 are relevant, they argue, to the intellectual

[2] In its Reply (DN 73), Defendants and SCDC indicated that SCDC does not have, or has already produced, documents responsive to six of the nine requests set out in the current subpoena, leaving only three in contention.

property aspect of the case and whether Defendants have misappropriated trade secrets or breached contractual confidentiality obligations or copyrights. Plaintiffs assert that documents produced in discovery suggest that Defendants used proprietary information to develop E-Jail and have continued to use that information after Mach 26, 2020.

2. Whether Plaintiffs have a legitimate basis upon which to seek the information.

Plaintiffs have retained an expert to review the E-Jail programming code to determine if it evidences copyright infringement, misappropriation of trade secrets, or other misuse of confidential information in comparison with JailTracker. In that regard, Plaintiffs state that their expert's review of the materials produced thus far in the case suggest "several significant differences in the version of the E-Jail software that was produced to Plaintiffs and the versions presented in the development history" (DN 66, p.7). Plaintiffs contend the information conflicts with the Defendants' representation that there were no other versions of the E-Jail software. Plaintiffs requests seek information revealing the full scope of the E-Jail product development. In support of their argument that the requested information about E-Jail is relevant, the Plaintiffs have submitted a lengthy affidavit from their expert witness, Monty G. Meyers (DN 68). In his affidavit, Mr. Meyers testifies that his review of the data thus far produced by the Defendants "strongly suggest that Defendants have produced an imposter version of the software or at least a version that does not match the history of the project and likely was not the software used by and developed with its primary and earliest client, Simpson County" (DN 68, p. 8).

Defendants argue that Plaintiffs' suspicions are unfounded and offer an explanation for why the software code might appear atypical. They note that the software was developed in collaboration with a software developer in India using an existing open-source software platform widely available to the general public and without a formal "version" progression. Once a jail begins to utilize the software, modules are customized to meet the particular jail's needs or preferences. Thus, differences may exist in the software to the extent it has been customized or enhanced at the request of a particular jail. What Defendants provided to Plaintiffs is the "basic E-Jail," which they produced by copying it onto a virtual server and giving Plaintiffs log-in credentials with full user and root access. This "basic E-Jail," Plaintiffs assert, "is precisely the software that would have been provided to a jail that became a customer at that time" (DN 73, p. 7). Plaintiffs have not been provided any customizations or enhancements that a particular jail may have requested. Defendants further contend that the true motivation behind Plaintiffs' requests is to obtain confidential information about Defendants' research and the needs and preferences of Defendants' clients regarding jail management software.

3. Whether Plaintiffs must make a heightened showing of need in order to be entitled to the discovery and whether the current protective order provides sufficient protection.

Defendants characterize the litigation as "a large, multinational conglomerate" against "an individual entrepreneur from Glasgow, Kentucky, and several small companies that he wholly owns" (DN 73, p. 9). In such cases of dispute between two direct competitors involving trade secrets, Defendants contend that caselaw mandates a higher showing of need in order to be entitled to the discovery, and discovery must be narrowly tailored to the need. To this end, Defendants point to Plaintiffs' expert's affidavit as devoid of any substantial factual basis for Plaintiffs' copyright infringement claim. While Defendants recognize that a protective order has been put in place, they maintain that the higher showing of need and narrow tailoring of the request is required, nonetheless.

Plaintiffs disagree that a heightened showing of need is required, but, if it is, they contend they have satisfied the requirement. They point to the affidavit of their expert as establishing a request-by-request basis for why he needs the information. Other factors they cite as supporting their belief that Defendants have misappropriated their proprietary information is that Ogles returned his company electronic devices with reformatted drives, concealing whether any information had been copied; continued modification of the E-Jail software without version control to preserve and differentiate any changes; and the admitted rapidity with which Ogles was able to develop E-Jail. The protective order, Defendants contend, limits disclosure of confidential information to counsel, expert witnesses, and the Court, and, as such, there is no risk the information will be shared with the Plaintiffs in such a way as to encroach upon the Defendants' business operations.

DISCUSSION

A party "may obtain discovery regarding any nonprivileged matter that is relevant to a party's claim or defense." FED. R. CIV. P. 26(b)(1). The discovery must be "proportional to the needs of the case, considering importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues and whether the burden or expense of the proposed discovery outweighs its likely benefit." Id. "Information within this scope of discovery need not be admissible in evidence to be discoverable." Id.

When a party seeks discovery from a non-party, it must demonstrate good cause to justify production. Perez v. Off Duty Police Servs., No. 3:13-CV-935-DJH-LLK, 2015 U.S. Dist. LEXIS 58015, at *3 (W.D. Ky. May 4, 2015). Only after a showing of relevance and good cause does the presumption for enforcement of the subpoena arise. Id.

1. March 26, 2020 as the cutoff for discoverable documents.

While March 26, 2020 may be the date upon which Ogles' contractual limitation on non-competition expired, he would still be prohibited from infringing upon Plaintiffs' intellectual property rights.

2. Whether Plaintiffs have a legitimate basis upon which to seek the information.

The affidavit from Plaintiffs' expert, Myers, details at length the reasons why he believes the documents related to the development of E-Jail postdating the one-year anniversary of Ogles' departure are relevant to his analysis. As to Request No. 1, he indicates that he intends to:

> use the information produced in response to this request to analyze how the Defendants' competing product began and evolved into its currently existing form and how such development may compare with and was potentially influenced by Plaintiffs' software (including source code, machine code, and other related materials and artifacts), IP (including trade secrets), and other confidential and proprietary information.

(DN 68, p. 8).

As earlier noted, Meyers has also expressed an opinion that, based upon the discovery produced thus far, he is suspicious that the code is an "imposter version," and not the actual initial version. His affidavit lists a number of objective factors that cause his suspicion. He asserts that additional information is necessary to ferret out if this is true.

Defendant Ogles counters Meyers' affidavit with his own (DN 73-1), in which he describes the history of how E-Jail was developed using Odoo, an open-source program available to the public, in collaboration with a software development company in India. He further explains that the "development process was very quick" (Id. at p. 3), and SCDC was E-Jail's first customer. "There are no separate versions of E-Jail. Given its short existence and rapid development, we have not yet used version control. However, differences may exist in the software to the extent that it has been customized or enhanced at the request of a particular jail" (Id.). He asserts that what has been made available to the Plaintiffs is the original program, and any subsequent modifications are merely to accommodate the specific requests of the customers.

Ogles has offered a reasonable explanation for why Meyers' might be puzzled by some of the E-Jail code, and this explanation may well persuade the finder of fact. However, Plaintiffs are not required to take the Defendants' word for it that what has been produced is the authentic program and are entitled to test the Defendants' contentions.

Turning to Request No. 2, which deals with documents or communications regarding "software bugs, complaints, or quality concerns," Meyers' affidavit asserts that such information is important when "a new competing product (E-Jail in this case) was being developed for delivery to a customer that recently stopped using a similar product (JailTracker in this case) that may have been copied and/or used as a baseline in order to build the new competing product" (DN 68, p. 12). Meyers also asserts that the information will shed light on the "imposter version" issue. Ogles' affidavit does not address the subpoena requests on a request-by-request basis, rather his explanation of how E-Jail was developed was intended as a blanket response to Meyers' affidavit. Again, Meyers has made a reasonable case for how the requested information could be relevant to his analysis of whether Defendants utilized any of JailTracker's proprietary information in developing E-Jail.

Request No. 4 inquires into documents that describe the build, installation, running, or operation of E-Jail. Meyers again links this information to determining the genuine nature of the software provided by the Defendants. "This requested category primarily represents the instructions and setup parameters that help ensure I build, install, access and use the produced software as expected/intended" (DN 68, p. 16). Moreover, "in cases such as this where I am conducting a "side by side" comparison of different competing software systems and their capabilities/functions, the build, installation, and setup materials and instructions in many instances also provide details and information related to or reflecting similarities or carry-overs that may reflect the use of one system to define and develop the other system or provide a head-start in the development process" (Id. at p. 17). Again, Meyers has made a reasonable case for how the requested information could be relevant to his analysis of whether Defendants utilized any of JailTracker's proprietary information in developing E-Jail.

3. Whether Plaintiffs must make a heightened showing of need in order to be entitled to the discovery and whether the current protective order provides sufficient protection.

Defendants contend that Plaintiffs should be held to a higher standard of demonstrating need for the information, given the nature of the case. As the Eastern District of Kentucky observed:

> Discovery issues in cases involving trade secrets present unique difficulties, as courts must balance one party's legitimate interest in maintaining the secrecy of valuable information with the other party's need to establish a claim or defense. These concerns carry greater significance in cases such as this where one party fears the disclosure of trade secrets to a competitor, as courts recognize 'that such disclosure to a competitor is more harmful than disclosure to a noncompetitor.'

Alltech, Inc. v. Carter, No. 5:08-CV-00325-KKC, 2009 U.S. Dist. LEXIS 150828, at *3 (E.D. Ky. July 8, 2009) (citations omitted).

FED. R. CIV. P. 26 provides courts with tools to address these concerns, including the ability to require that "a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way." RULE 26(c)(1)(G). A protective order is already in place which specifies limits on the manner in which such information is to be revealed. The current iteration of the order is at DN 44, which was entered by agreement of the parties on May 27, 2020. The order establishes three categories of information subject to protection. Matters designated as "Confidential Information" would be subject to limited dissemination and only reviewed by outside and in-house counsel for a party, no more than two party representatives, legal support staff, and non-party employee retained experts. "Highly Confidential Information" and "Source Code" would be subject to a higher restriction in that it could not be shared with party representatives. Moreover, the protective order extends to material produced by third parties in response to any discovery request (DN 44, p. 1, ¶ 1). Defendants can therefore designate information produced by SCDC as "Highly Confidential," in which case it could only be seen by the Plaintiffs' attorneys and retained expert, who would be prohibited from sharing the information or allowing it to be used for "any business, competitive, commercial or any other purpose whatsoever" (Id. at p. 3, ¶6). See Osborn v. Griffin, No. 11-89-WOB-CJS, 2013 U.S. Dist. LEXIS 201060, at *23-25 (E.D. Ky. July 17, 2013) (Confirming that protective order which included material produced by third-party was subject to confidentiality designation by party). In opposition to the sufficiency of the protective order, the Defendants argue that, in a case involving "a large established company" and a "startup competitor," any disclosure, even under a protective order, "carries a great risk of harm to the defendant and should only be required if the plaintiff meets the heightened standard . . ." (DN 73, p. 13). But other than a generalized concern, Defendants have not articulated a specific reason why the protective order will not operate as intended. "In order to permit parties to proceed with litigation concerning confidential information, protective orders, such as the one entered in this case, must be respected by the parties and thus are presumed by courts to be effective. Otherwise, many complex cases, particularly patent cases, would be impossible to prosecute or defend." Corning Inc. v. SRU Biosystems, LLC, 223 F.R.D. 191, 195 (D. Del. 2004).

Defendants also contend that Plaintiffs have failed to identify with particularity what trade secret was allegedly misappropriated. As such, they further contend Plaintiffs have failed to supply a basis upon which the Court can appropriately narrow discovery and prevent a generalized fishing expedition.

> Parties alleging misappropriation of a trade secret "are normally required first to identify with reasonable particularity the matter which it claims constitutes a trade secret before it will be allowed to compel discovery of its adversary's trade secrets." Dura Global Techs., Inc. v. Magna Donnelly Corp., No. 07-CV-10945-DT, 2008 U.S. Dist. LEXIS 38989, 2008 WL 2064516, at *1 (E.D. Mich. May 14, 2008). Such discovery responses are intended "to give defendants fair notice of the essential details of the trade secret claim so that they can conduct appropriate discovery and file appropriate motions concerning the merits of the claim." Kendall Holdings, Ltd. v. Eden Cryogenics, LLC, No. 2:08- CV-390, 2011 U.S. Dist. LEXIS 92936, 2011 WL 3652696, at *2 (S.D. Ohio Aug. 18, 2011).

Yoe v. Crescent Sock Co., No. 1:15-CV-3-SKL, 2017 U.S. Dist. LEXIS 226421, at *7 (E.D. Tenn. May 25, 2017). The undersigned believes that Plaintiffs have made a sufficiently particularized allegation for purposes of discovery. The two products identified in the Complaint are JailTracker and E-Jail, and the question is whether source code from the former was used in the development of the latter. See (Third Amended Complaint, DN 61, p. 20, ¶120).

4. Plaintiffs' request for sanctions.

Plaintiffs contend that Defendants should be required to pay their legal fees as a sanction for failing to comply with LR 37.1. That Rule mandates that, before filing any motions related to discovery, all counsel must make a good faith effort to resolve the dispute extrajudicially and to include a certification in any discovery that they complied with the rule. Plaintiffs assert that Defendants did not contact them to attempt resolution before filing their motion. In response, the Defendants contend that they did notify the Plaintiffs that they would not oppose production of documents created before March 26, 2020, but indicated that they would oppose those created after that date and "await the Court's determination of their Motion to Quash or Modify" (DN 73 p. 13). The Defendants also note that the subject of the motion is a subpoena issued to a non-party. They argue that SCDC is also a movant, and the Rule does not indicate that it applies to anyone other than the parties to the case.

The undersigned would point out that the Scheduling Order in the case imposes an additional obligation on the parties that, before filing any motions related to discovery, they are to contact the undersigned to schedule a telephonic conference to discuss the issue (DN 72, p. 2, ¶3).

Here the application of the Local Rule and the Scheduling Order are a murky. To the extent that the motion is advanced by the Defendants, they failed to comply with both. However, SCDC, a non-party, is also a movant and neither the Local Rule in question nor the Scheduling Order contemplate an obligation on anyone other than parties to the case. For this reason, the undersigned declines to impose any sanctions, but reminds Defendants of these obligations going forward.[3]

ORDER

WHEREFORE, the motion to quash or modify the subpoena issued to SCDC (DN 62) is **DENIED**. However, the Defendants may designate the documents produced as "Highly Confidential," and they will be subject to the provisions of the Amended Agreed Protective Order (DN 44).

H. Brent Brennenstuhl

H. Brent Brennenstuhl
United States Magistrate Judge

October 13, 2020

Copies: Counsel of Record

[3] The undersigned further questions whether it would be appropriate to award sanctions based upon a request made in a response to a motion. *See* Fed. R. Civ. P. 7(b)(1) ("A request for a court order must be made by motion."); Sullivan v. Farm Bureau Mut. Ins. Co., No. 1:10-CV-909, 2011 U.S. Dist. LEXIS 35817, at *12 n.8 (W.D. Mich. April 1, 2011) ([A] response is not the proper place for a request to the Court.); *see also* EEOC v. Tenpro, Inc., No. 4:12-CV-75-HSM-SKL, 2014 U.S. Dist. LEXIS 190543, at *46-47 (E.D. Tenn. Aug. 29, 2014).