UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

San Francisco Division

SYNOPSYS, INC.,

Plaintiff,

v.

UBIQUITI NETWORKS, INC., et al.,

Defendants.

Case No. 17-cv-00561-WHO (LB)

ORDER THAT TAIWANESE COMPUTERS ARE NOT PER SE OUTSIDE THE SCOPE OF DISCOVERY

Re: ECF Nos. 99, 105, 109, 110

INTRODUCTION

This lawsuit centers on allegations by plaintiff Synopsys, Inc. ("Synopsys"), a software company, that the defendants (collectively, "Ubiquiti") "pirated" its software by installing it on Ubiquiti's computers and then using counterfeit license keys to run the software without obtaining a valid license. Among other claims, Synopsys alleges that Ubiquiti (1) circumvented technological measures that control access to copyrighted software, in violation of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201(a)(1), and (2) committed fraud in representing to Synopsys that it was interested in entering into a license agreement to obtain Synopsys software when it in fact was planning to use counterfeit license keys. Synopsys issued discovery requests to "forensically inspect" Ubiquiti's computers for evidence to support its claims. Ubiquiti objects to Synopsys's requests.

The parties' discovery dispute involves two issues: (1) relevance and (2) burden. The parties' briefs focus almost entirely on relevance. Ubiquiti's main argument is that all but two of the computers at issue are located outside the United States, the DMCA and U.S. copyright law do not impose liability for activity that occurred outside the United States, and hence the computers outside the United States are not relevant to Synopsys's claims and should be excluded from discovery. Synopsys disagrees with Ubiquiti's factual and legal contentions. As for burden, the court previously instructed the parties to meet and confer on the specifics of an appropriate inspection protocol and, if they were unable to agree on a solution, to submit a joint letter brief with their respective positions on how inspection would work, exactly what would be inspected, and what burdens that inspection might impose.[1] The parties have not reached an agreement or submitted a joint letter brief with this information.[2]

The court held a hearing on January 25, 2018. Because the parties did not raise burden arguments before the hearing, this order does not address burden issues and addresses only the parties' relevance arguments. The court holds that Ubiquiti computers are not per se outside the scope of relevant discovery merely because they are located outside the United States.

STATEMENT

1. Synopsys Claims That Its Data Shows That Ubiquiti Circumvented Its Software's License-Key-Protection System Approximately 39,000 Times

Synopsys is a world leader in semiconductor design software.[3] Ubiquiti develops networking technology and, among other things, designs semiconductor chips for use in its products.[4]

Synopsys alleges that Ubiquiti downloaded Synopsys electronic design automation ("EDA") software onto Ubiquiti computers.[5] Synopsys alleges that its software will not run without a

---

[1] *See* Order – ECF No. 104 at 2, 5–6. Citations refer to material in the Electronic Case File ("ECF"); pinpoint citations are to the ECF-generated page numbers at the top of documents.

[2] *See* Letters – ECF Nos. 111, 114, 117–119.

[3] Joint Case Mgmt. Statement – ECF No. 98 at 2.

[4] *Id.*

[5]

license key and that Ubiquiti has been using counterfeit license keys since at least February 2014 to access and run Synopsys software on its computers without obtaining a valid license.[6]

This software has a built-in feature: according to Synopsys, its software transmits basic information about computers that use counterfeit license keys, such as the computers' MAC addresses, IP addresses, and server host names, back to Synopsys.[7] The parties refer to this transmission as "call-home" or "phone-home" data. Synopsys claims that call-home data here shows that Ubiquiti used counterfeit license keys over 39,000 times to access Synopsys software.[8]

2. Ubiquiti Installed Synopsys Software on Taiwanese Computer Servers, and U.S. Employees Remotely Connected to Those Servers to Run Synopsys Software

Ubiquiti acknowledges that it installed Synopsys software on a "storage array" in Taiwan that is accessed through three computer servers located in Taiwan.[9] Ubiquiti employees can access and run the software by using their local laptops or desktops and remotely connecting to the servers.[10]

Ubiquiti also acknowledges that when its employees remotely access its servers to run Synopsys software, Synopsys's call-home data reports the MAC address and host name of the server (or virtual machines running on the server), not the MAC address or host name of the employee's local computer.[11] Similarly, the call-home data reports the user name of the account profile on the server that the employee uses to remotely log on, not the user name of the account profile the employee has on his local computer.[12] Additionally, Synopsys asserts that the call-home data reports the IP address and the country location of the server, not the IP address or the country location of the end user.[13]

---

[6] *Id.* Ubiquiti disputes that a license key is necessary to run Synopsys software. *Id.*

[7] Joint Letter Br. – ECF No. 99 at 2.

[8] Joint Case Mgmt. Statement – ECF No. 98 at 3; Joint Letter Br. – ECF No. 99 at 4.

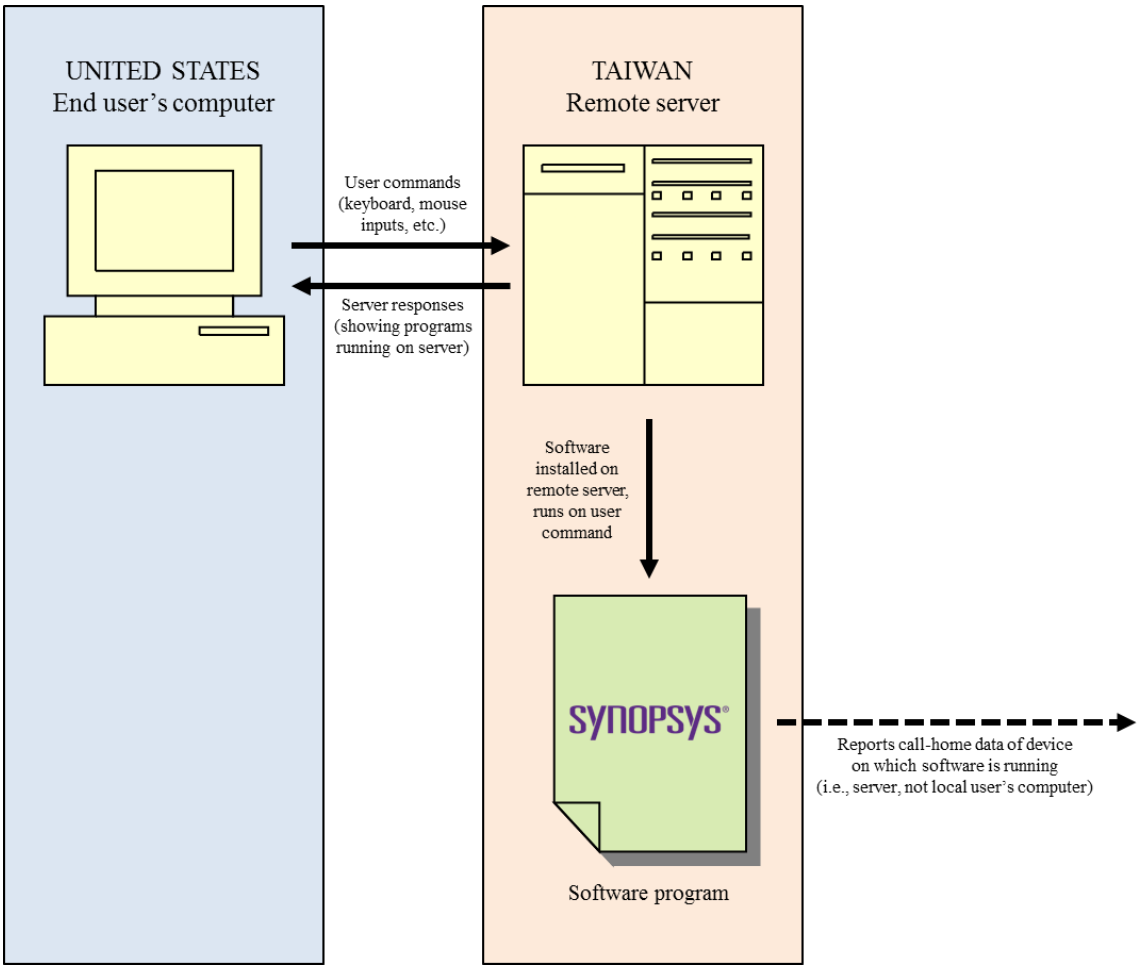
[9] Tsai Decl. – ECF No. 105-5 at 4 (¶ 12).

[10] *Id.* at 4–5 (¶ 13). Synopsys alleges that Ubiquiti installed Synopsys software on other computers in addition to these three servers as well. Jan. 25, 2018 Hr'g.

[11] *See* Nazarian Decl. – ECF No. 105-1 at 4 (¶¶ 9–11); Tsai Decl. – ECF No. 105-5 at 3–5 (¶¶ 7–13).

[12] *See* Tsai Decl. – ECF No. 105-5 at 5–6 (¶ 17).

[13] Jan. 25, 2018 Hr'g.



Ubiquiti maintains that of the approximately 39,000 alleged circumventions identified in Synopsys's call-home data, only 626 correspond to an IP address originating in the United States.[14] The remaining 38,000 or so call-home entries show an IP address in Taiwan.[15] Synopsys does not dispute these statistics. Ubiquiti then argues that these IP addresses show that "all but 626 of the alleged acts of circumvention took place entirely outside the United States[.]"[16] Synopsys disputes this characterization and argues that if an end user located in the United States remotely connects to a server in Taiwan and then accesses Synopsys software installed on the server, the call-home data would report an IP address originating in Taiwan (the server's IP address), despite

[14] Ubiquiti Br. – ECF No. 105 at 3–4; Taylor Decl. – ECF No. 105-2 at 3 (¶ 6).

[15] Ubiquiti Br. – ECF No. 105 at 4; Taylor Decl. – ECF No. 105-2 at 3 (¶ 6).

[16]

the fact that the end user is located in the United States.[17] It is undisputed that at least one U.S.-based Ubiquiti employee, Ching-Han Tsai (who has also been named as an individual defendant), used Synopsys software and that he did so on at least some occasions by logging in remotely from the United States to Ubiquiti servers in Taiwan.[18] According to Synopsys, on at least some of these occasions, the call-home data reported a Taiwanese IP address, not a U.S. IP address.[19]

ANALYSIS

It is important to recall exactly what is before the court. This is a discovery motion. It is not a dispositive motion on the merits of Synopsys's claims. Synopsys is not limited to admissible evidence and need not prove its claims at this juncture. It must only show that, given its claims, the discovery it requests is (1) relevant and (2) proportional to the needs of this case. *See* Fed. R. Civ. P. 26(b)(1). "Information . . . need not be admissible in evidence to be discoverable." *Id.* In deciding whether the plaintiff has made that showing, the court can consider even inadmissible evidence. *Cf.* Fed. R. Evid. 104. *See generally, e.g.*, *Goes Int'l, AB v. Dodur, Ltd.*, No. 14-cv-05666-LB, 2016 WL 427369, at *2 (N.D. Cal. Feb. 4, 2016).

The parties have not presented specifics as to exactly what a forensic inspection would cover, and hence the court does not rule on the relevance (much less on the proportionality or burden) of any particular forensic artifact that may be on Ubiquiti's computers. The court is not issuing a blanket approval of a forensic inspection. But nor may Ubiquiti assert a blanket claim that its Taiwanese computers are not relevant to Synopsys's claims. As discussed below, Ubiquiti's Taiwanese computers and the forensic artifacts on them may be relevant to the case.

[17] Jan. 25, 2018 Hr'g.

[18] Tsai Decl. – ECF No. 105-5 at 5 (¶¶ 14, 16).

[19] Jan. 25, 2018 Hr'g.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.