UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No.	2:21-cv-03056-DSF-PDx	Date	April 19, 2022
Title	*JUUL LABS, INC. v. Andy Chou, et al.*		

Present: The Honorable	PATRICIA DONAHUE, U.S. MAGISTRATE JUDGE

Isabel Martinez	N/A
Deputy Clerk	Court Reporter / Recorder
Attorneys Present for Plaintiff(s):	Attorneys Present for Defendant(s):
N/A	N/A

Proceedings: **(In Chambers) Order Denying Plaintiff's Motion to Compel Inspection of Defendants' Devices [Dkt. No. 179]**

Before the Court is Plaintiff's Motion to Compel Inspection of Defendants' Electronic Devices ("Motion to Compel"). [Dkt. No. 179.] The Court conducted an informal discovery conference and has reviewed all of the parties' submissions in connection with this discovery dispute. [Dkt. Nos. 174, 177, 178, 179, 183, 184.] The Court is familiar with the lengthy history of this and the other discovery disputes in this matter. For the reasons discussed below, the Motion to Compel is denied.

I. Legal Standard

A. ESI Production

Under Rule 34, a party may request that another party produce and permit it to inspect, test, sample and copy electronically stored information ("ESI") that is within the scope of Rule 26(a) "in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form." Fed. R. Civ. P. 34(a)(1). In amending Rule 34 to

Initials of Preparer IM

include ESI, the Advisory Committee noted that "[t]he addition of testing and sampling to Rule 34(a) with regard to documents and electronically stored information is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting and testing such systems." Fed. R. Civ. P. 34 Advisory Comm. Notes, 2006 Amendment; *see also In re Ford Motor Co.*, 345 F.3d 1317 (11th Cir. 2003) ("Rule 34(a) does not give the requesting party the right to conduct the actual search.").

When drafting Joint Rule 26(f) reports, parties must include a discovery plan that states any issues about disclosure, discovery, or preservation of ESI, including the form in which ESI should be produced. Fed. R. Civ. P. 26(f)(3)(C). The form of production could be "native, near-native, imaged as PDF (or more commonly, as TIFFs accompanied by load files containing searchable text and metadata) or in paper (printed out)." *Venture Corp. Ltd. v. Barrett*, 2014 WL 5305574, at *3 (N.D. Cal. 2014). In this matter, the parties' discussion of discovery in the Joint Rule 26(f) Report does not address ESI. [Dkt. No. 67 at 10-11.]

A party propounding requests for production ("RFPs") may specify the form in which ESI should be produced. Fed. R. Civ. P. 34 (b)(1)(C). If the RFPs do not specify a form, then the producing party must produce the documents in the form in which they are "ordinarily maintained or in a reasonably usable form." Fed. R. Civ. P. 34 (b)(2)(E)(ii). Most ESI is ordinarily maintained in the form of native files. Unless otherwise ordered, parties "need not produce the same [ESI] in more than one form." Fed. R. Civ. P. 34(b)(2)(E)(iii). In this matter, Defendants did not object to Plaintiff's request pursuant to Rule 34(b)(1)(C) that the ESI be produced as single-page TIFF images with a load file that includes all available and extractable metadata and text, and Excel files to be produced in native format. [Dkt. No. 141-3 at 20-23.]

Initials of Preparer IM

B. Forensic Examination

District courts have broad discretion in controlling discovery. *See Hallett v. Morgan*, 296 F.3d 732, 751 (9th Cir. 2002). "A forensic examination of an opposing party's computer is considered an extraordinary remedy." *MGA Ent., Inc. v. Nat'l Prod. Ltd.*, 2012 WL 12886446, at *2 n.2 (C.D. Cal. 2012); *SGII, Inc. v. Suon*, 2021 WL 6752324, at 9 (C.D. Cal. 2021) ("Courts in this circuit have been reluctant to grant motions compelling forensic examinations of a party's computers.") (citation omitted). "The burden is on the party seeking to compel discovery to cast doubt on the responding party's assertion that it does not have the requested information." *Gary Friedrich Enters., LLC v. Marvel Enters., Inc.*, 2011 WL 2623458, at *1 (S.D.N.Y. 2011).

Though the Ninth Circuit has not articulated a standard for ordering a forensic examination, district courts across the country have consistently held that "mere suspicion or speculation that an opposing party may be withholding discoverable information is insufficient to support" such an intrusive examination. *Hespe v. City of Chicago*, 2016 WL 7240754, at *4 (N.D. Ill. 2016) (internal quotes and citation omitted); *see also John B. v. Goetz*, 531 F.3d 448, 460 (6th Cir. 2008); *Brady v. Grendene USA, Inc.*, 2015 WL 4523220, at *7-9 (S.D. Cal. 2015); *Powers v. Thomas M. Cooley Law Sch.*, 2006 WL 2711512, at *5 (W.D. Mich. 2006). Thus, a requesting party's desire to confirm the completeness of the responding party's production is insufficient. *In re 3M Combat Arms Earplug Prod. Liab. Litig.*, 2020 WL 6066199, at *3 (N.D. Fla. 2020).

Many courts within the circuit look to whether the party requesting a forensic examination has made a showing that the responding party intentionally destroyed relevant electronic discovery or committed other improper discovery conduct. *See Moser v. Health Ins. Innovations, Inc.*, 2018 WL 6735710, at *5 (S.D.

Cal. 2018); *Sophia & Chloe, Inc. v. Brighton Collectibles, Inc.*, 2013 WL 5212013, at *2 (S.D. Cal. 2013) ("[A]bsent specific, concrete evidence of concealment or destruction of evidence, courts are generally cautious about granting a request for a forensic examination of an adversary's computer."). Of course, the responding party always has a duty to make a reasonable search for any responsive material. *See MGA Ent., Inc.*, 2012 WL 12886446, at *2 (citation omitted); *A. Farber and Partners, Inc. v. Garber*, 234 F.R.D. 186, 189 (C.D. Cal. 2006). Consequently, other courts have considered whether the responding party is competent to reasonably search for and collect responsive data from its devices. *See Belcastro v. United Airlines, Inc.*, 2019 WL 7049914, at *2-3 (N.D. Ill. 2019); *Procaps S.A. v. Patheon, Inc.*, 2014 WL 11498061, at *3 (S.D. Fla. 2014); *Mirbeau of Geneva Lake LLC v. City of Lake Geneva*, 2009 WL 3347101, at *1 (E.D. Wis. 2009) (forensic examination required "[o]nly if the moving party can actually prove that the responding party has concealed information or lacks the expertise necessary to search and retrieve all relevant data . . . .").

In line with the Advisory Committee's Notes to the 2006 Amendment, "compelled forensic imaging is not appropriate in all cases, and courts must consider the significant interests implicated by forensic imaging before ordering such procedures." *John B.*, 531 F.3d at 460. Therefore, a court reviewing a motion to compel the inspection of the non-moving party's devices should ensure that the request is proportional to the needs of the case pursuant to the factors contained in Rule 26. *Motorola Sols., Inc. v. Hytera Commc'ns Corp.*, 365 F. Supp. 3d 916, 924-25 (N.D. Ill. 2019).

II. Background of the Disputes and the Parties' Contentions

On December 3, 2021, following an informal discovery conference, the Court issued an order stating that "[a]s discussed during the hearing, the metadata sought by Plaintiff is relevant and should be produced. The parties are ordered to

meet and confer in good faith to determine whether that would require a complete re-production by Defendants into TIFF format." [Dkt. No. 123 at 4.] On January 3, 2022, following an informal discovery conference, the Court ordered Defendants to search and produce content responsive to Plaintiff's Requests for Production contained in specified digital devices. [Dkt. No. 129 at 2-3.] On February 24, 2022, the Court issued an Order partially granting Plaintiff's motion to compel that required Defendants to conduct further searches of their digital devices. [Dkt. No. 148 at 5-14.] On March 8, 2022, following an informal discovery conference, the Court issued an order requiring Defendants to provide specified information about its prior WeChat Enterprise Software System and a sworn declaration by March 16 stating: (1) the identity and title of the individual[s] who conducted the searches; (2) if the searches were of digital devices, the qualifications of the individuals who conducted the searches; (3) the devices that were searched, including make/model/serial number; (4) the dates that the searches took place; and (5) the software, protocols, and/or methods used to conduct the searches. [Dkt. No. 150 at 2-3.] The Court also warned Defendants that if they could not adequately search their devices, it might take additional steps including granting Plaintiff's request for a third-party forensic examination. [*Id.* at 3.] The Court noted that the parties disputed whether Defendants should ship devices used by Defendant Chou and six employees from New Jersey and China to California for examination by a forensic expert. [*Id.*]

On March 30, 2022, the Court conducted an informal discovery conference to address Plaintiff's argument that Defendants' ESI production fails to comply with Rule 34 and the Court's orders that Defendants should be compelled to ship specified electronic devices to California for review by a forensic expert. [Dkt. No. 174.] Plaintiff contended that the declarations submitted by Defendants of Zhaofeng Liu and Lynn Lee were deficient and failed to comply with the March 8 Order requiring Defendants to fully detail the searches and qualifications of those who carried out the search for responsive documents. Plaintiff also stated that

through its March 23 deposition of Keyin Ye, an employee of Defendants, Plaintiff learned that Leon Li, an employee at Defendants' New Jersey warehouse, actually carried out the search of the computers located there, not Zhaofeng Liu. Plaintiff argued that Leon Li was not qualified to conduct the searches based on previous representations by Defendants about his responsibilities at the warehouse.

In the Motion to Compel, Plaintiff argues that a forensic examination is necessary because Defendants' collection and production of responsive ESI was inadequate, did not comply with standard eDiscovery methods, did not comply with this Court's orders directing that documents be produced with metadata, and have potentially resulted in the modification and/or loss of relevant data. [Dkt. No. 179 at 4-5.] Plaintiff submitted a protocol to carry out the examination in its proposed order. [*See* Dkt. No. 179-16.][1]

Defendants submitted the Liu and Lee declarations, a portion of Ye's deposition, and a declaration from Carley Barnes, who has 14 years of experience in E-discovery matters. Defendants contend that Plaintiff's complaints of alleged noncompliance with the Court's March 8 Order are based on apparent mischaracterizations and/or misrepresentations of Defendants' declarations and witness testimony. [Dkt. No. 177 at 4.] Barnes declares that he reviewed Liu's declaration and that the methodology used to carry out the searches on Defendants' computing devices, which only utilized the native search features contained in Windows and Macintosh, "comport[ed] with standard methodologies" for locating relevant electronic documents. [Dkt. No. 177-4 at 2.] Barnes concludes that the methodologies used by Liu "comported with the standards utilized by most E-

[1] The proposed order [Dkt. No. 179-6] refers to an attached "Exhibit A" that contains a statement which must be signed by the forensic examiner, however, no such exhibit to the proposed order was filed.

Discovery services providers and would be sufficient to locate active data of electronic documents and messages on native devices." [*Id.*]

Defendants oppose the forensic examination on the grounds that its search for responsive ESI was sufficient and followed industry standards, that it was never ordered to perform a forensic review of its devices, that Plaintiff's mere suspicion of the failure to produce documents does not warrant a forensic examination, and that it would cause a significant burden on Defendants' business operations and potentially violate Chinese law.

Plaintiff identifies five areas in which it contends that Defendants have failed to reasonably search for and produce ESI: (1) WeChat data; (2) Skype data; (3) ESI produced in inaccessible formats; (4) search methodology; and (5) search of devices at Defendants' New Jersey warehouse.

A. WeChat Data

Plaintiff points to Defendants' production of WeChat messages by cutting and pasting those messages into Word documents, thereby omitting the original messages' metadata, as a particularly egregious example of the insufficient production. Plaintiff submits the declaration of Calvin Weeks, who has 35 years of specialized experience in digital forensics, eDiscovery, cybersecurity, and cyber incident response. [Dkt. No. 179-1 at 2.] Weeks has handled collections, searches and productions of instant messages from different applications, including WeChat, and states that "specialized forensic and eDiscovery software is usually capable of extracting such messages including all metadata and exporting them into a format" that does not have the flaws as presented in Defendants' production. [*Id.* at 6.] Weeks also declares that WeChat data "is a proprietary format and can only be parsed into a proper readable and searchable format using tools that can extract the WeChat data and search it properly, such as the Axiom forensic tool." [*Id.* at 5.]

Weeks identifies three problems with Defendants' approach to the WeChat data. First, Weeks states that none of the image files in the original messages were included in the cut-and-pasted messages, so that some original content was not produced and some messages are thus unintelligible. [*Id.* at 6.] Defendants state that they cut and pasted messages into Word documents "[s]ince Plaintiff objected to the production of screenshots of WeChat." [Dkt. No. 183-1 at 11.] If cutting and pasting failed to include image files, then Defendants are hereby ordered to also provide screenshots of those image files.

Second, Weeks states that "the production [of WeChat data] does not include the original metadata associated with the original messages, e.g. the real author, the data and time a message was sent, received, and read, the contact information for both sender(s) and recipient(s), etc." [Dkt. No. 179-1 at 6.] The declaration of Plaintiff's counsel identifies by Bates number documents that "appear to be WeChat and/or Skype messages that were copied and pasted into Word format documents" which "have metadata with the 'Date Created' and 'Last Date Modified' fields showing the same date, or dates within one of two days of the production date of March 16, 2022, which does not appear to be the original metadata for when those messages were actually first created and last modified." [Dkt. No. 179-2 at 6-7.] Defendants state that "metadata for the messages" are included in both screenshots and cut and pasted versions of WeChat messages. [Dkt. No. 183-1 at 11.] Metadata is data embedded in electronic versions of a document that show, for example, how, when and by whom the document was created, access or modified. *See* The Rutter Group, *Prac. Guide: Fed. Civ. Proc. Before Trial, California and 9th Cir. Editions* § 11:1851:19 (2020). Defendants do not explain how the data embedded in the electronic version of the WeChat messages was incorporated into the screenshots and cut-and-pasted versions that they produced to Plaintiff.

Initials of Preparer IM

On the issue of WeChat data, it appears that the Weeks and Barnes declarations address different points. Barnes states that the production of "native files from WeChat is not possible" [Dkt. No. 177-4 at 3], but does not define or explain what he means by "native files" and does not address whether WeChat data can be extracted in a form that preserves and displays its metadata. Barnes states that as to WeChat, producing "screenshots or versions where the messages are cut and pasted into other documents is typical" [Dkt. No. 177-4 at 3], but does not state whether it is possible to take screenshots of the metadata or otherwise copy and paste it into another document without altering it. Weeks does not discuss native WeChat files. Weeks states that Defendants' production of WeChat messages failed to include "the original metadata associated with original messages" [Dkt. No. 179-1 at 6,] thereby suggesting that WeChat data can be extracted into a form that preserves and displays its metadata. Weeks also states that through the use of forensic tools such as Axiom, WeChat data can be parsed into a format that is readable and searchable. [Dkt. No. 179-1 at 5.]

Third, Weeks states because the WeChat messages were manually pasted into an editable document, there is "no way to validate the completeness and accuracy" of the production. [Dkt. No 179-1 at 6.] Plaintiff does not identify any specific WeChat messages or message threads produced by Defendants that appear incomplete or inaccurate. However, the history of Defendants' production of the WeChat discovery raises concerns about its completeness and accuracy. At the March 8 discovery conference and in the related joint e-mail of the parties' positions, Defendants stated that they had provided Plaintiff with written confirmation that a new version of WeChat installed in April 2021 had removed all data from chat messages in the previous version of the WeChat software used by Defendants. [Dkt. Nos. 153 at 12-20, 150-1 at 3.] In fact, that written confirmation was a one-page document containing untranslated communications in Chinese between two unidentified parties, one of whom Defendants stated was a customer service representative for the WeChat software vendor. The Court found this

insufficient and ordered Defendants to engage in a meaningful search to determine whether messages were recoverable from the prior version of the software. [Dkt. No. 150 at 2.] Defendants subsequently made multiple attempts to contact the vendor for support and "were finally able to retrieve locally saved data from their old Enterprise WeChat account." [Dkt. No. 177 at 4.] On March 11, Lynn Lee was advised by an Enterprise WeChat agent that she might be able to regain access to locally saved data by using the mobile phone used to create and log into Defendants' old account. Lee did so and was able to produce old WeChat accounts. [Dkt. Nos. 177-5 at 26, 177-6 at 3-4, 177-5 at 32-33.] Defendants undertook these efforts only after Plaintiff complained and the Court found Defendants' efforts to search for and respond to the WeChat discovery requests insufficient.

Having finally retrieved accounts from the prior WeChat software, Defendants state that data from two of the relevant accounts is not available because it was likely deleted. The March 16 Liu declaration submitted by Defendants states that two of the "newly recovered" old WeChat accounts contain no messages, possibly because "the local data files for these two accounts might have been deleted due to the lack of the disk space," as those two accounts "would have displayed messages from the local data files if they exist." [Dkt. No. 177-2 at 4.] This indicates that Defendants may have been able to recover messages had they been adequately preserved. Defendants address this deficiency by explaining that relevant conversations between the two individuals and other employees "likely have already been located and produced" by the keyword searches. [Dkt. Nos. 177 at 9-10, 183-1 at 9.]

B. Skype

Plaintiff states that Defendants' February 1 production of messages from "Celia's" Skype account was a "single file in JSON format" that Plaintiff's eDiscovery vendor was unable to process. [Dkt. No. 179-2 at 5.] Plaintiff also

states that Defendants copied and pasted Skype messages into Word documents. Plaintiff contends that Defendants failed to produce the Skype messages in a reasonably usable format and that the Skype production contained no metadata. [Dkt. Nos. 179 at 9, 179-2 at 6.] The Weeks Declaration does not address specific deficiencies in the Skype production. Defendants' position is that they produced Skype messages "in the standard JSON format according to Microsoft's own instructions for doing so," and that there are a "multitude of commonly used viewers for JSON." [Dkt. No. 183-1 at 11-12.] On this record, the Court cannot conclude that Defendants' production of the Skype messages was inadequate.

C. ESI Produced in Inaccessible Formats

As noted above, Defendants did not object to Plaintiff's request pursuant to Rule 34(b)(1)(C) that the ESI be produced as single-page TIFF images with a load file that includes all available and extractable metadata and text, and Excel files to be produced in native format. [Dkt. No. 141-3 at 20-23.] The declaration of Plaintiff's counsel describes ESI produced by Defendants between November 2021 and March 2022 that fails to comport with Plaintiff's request or is in an unusable format. [Dkt. No. 179-2, ¶¶ 4-19.] For example, according to Plaintiff's counsel, Defendants' March 16 production, done pursuant to Court Order [Dkt. No. 148] contained 366 documents, devoid of metadata, only 79 of which appeared to be distinct documents, and approximately 70 of which contain a "Conversion Error" message and are unusable. [Dkt. No. 179-2, ¶ 17.] The Weeks Declaration alludes to some of these documents, though does not specifically mention any in particular, and states that "many of Defendants' documents have been converted from other formats . . . or appear to be screenshots. When documents are converted in such a way, all associated metadata is removed . . . ." [Dkt. No. 179-1 at 8.] Defendants contend that Plaintiff mischaracterizes the facts. [Dkt. No. 183 at 12-13.] Defendants point to two exhibits which they state show that their March 16

production did contain metadata. However, Defendants' filed pleading does not attach the exhibits. [Dkt. No. 183-1 at 12 n.6.]

D. Search Methodology

Plaintiff also raises several issues regarding Defendants' search methodology. Specifically, Weeks explains that Liu failed: (1) to take any steps to maintain the integrity of the data he was analyzing, including creating a forensic mirror image of the device, (2) to describe with specificity the methodology of his search terms, including the syntax or structure and whether Boolean standards were employed, (3) to use more sophisticated search tools commonly used in the industry or to explain why he chose to use only the native search features, (4) to state whether the searches were limited to exact matches, whether query modifiers were used to capture variants of the key words, and whether the searches were limited to English words, and (5) to show that the searches would have captured responsive data in deleted messages whereas industry standard search tools would have captured such data. The Barnes Declaration submitted by Defendants summarily states that "such searches typically utilize the native search features of those messaging platforms to locate relevant messages and documents which are stored on the computer being searched and in the remote server." [Dkt. No. 177-4 at 2-3.]

Plaintiff contends that Defendants' searches failed to comply with the Court's March 8 Order, which Plaintiff interprets as requiring Defendants to conduct a forensic examination of their devices. The Court did not order Defendants to conduct a forensic examination of their devices. Defendants were ordered to provide a sworn declaration that contained information such as the identity of the individuals who conducted the searches, their qualifications, the specific devices that were searched, dates that the searches took place, and the software, protocols, and methods used. [Dkt. No. 150 at 3.] As the Court stated in its order, it might be necessary to order a forensic examination if Defendants were unable to adequately,

i.e. thoroughly, search their own devices. [*Id.*] The objective was to determine from the specifically requested information whether such a search occurred. However, the Court did not equate a forensic examination, complete with creating a mirror image of the device's contents, with an adequate search for and production of responsive material and Plaintiff has not offered any authority suggesting as much.

Plaintiff's other claim, that Defendants failed to use proper search protocols for a forensic search, is also unpersuasive. First, the Court did not order Defendants to conduct a forensic search and second, Plaintiff is unable to point to material it contends has been withheld. The Federal Rules of Civil Procedure impose a duty on parties to undertake a "diligent search and reasonable inquiry in order to adequately respond to requests for production." *Beeman v. Anthem Prescription Mgmt., Inc.*, 2017 WL 5564535, at *4 (C.D. Cal. 2017) (citing *Garcia v. Bana*, 2012 WL 2119157, at *10 (N.D. Cal. 2012); *Choudhuri v. Wells Fargo Bank, N.A.*, 2017 WL 1738034, at *2 (N.D. Cal. 2017)); *see also Moore v. Publicis Groupe*, 287 F.R.D. 182, 188 (S.D.N.Y. 2012) ("[T]he Federal Rules of Civil Procedure do not require perfection."). Though Weeks states in his declaration that aspects of Liu's search fell below eDiscovery standards, it is clear from the explanation of his reasoning that he and Plaintiff have held Defendants to a different and more rigorous standard than what is required by the Federal Rules of Civil Procedure. In short, Plaintiff has not shown that Defendants' search methodology was inadequate based on the declarations ordered on March 8.

E. Search of Devices at Defendants' New Jersey Warehouse and Use of Team Viewer

In his March 16 declaration, Liu testifies that on March 16, he performed keyword searches on specified devices at Defendants' New Jersey warehouse remotely from China using TeamViewer, and he performed searches using search features provided with Microsoft Windows, WeChat and Skype. [Dkt. No. 177-2 at

6-7.] At his March 23 deposition, Keyin Ye, the New Jersey warehouse manager, testified that Leon Li had performed a search of computers at the New Jersey warehouse and that someone from China had also conducted searches of the devices. [Dkt. Nos. 177 at 10-11, 179 at 12-13, 18-19.] The record does not support most of Plaintiff's complaints regarding alleged inconsistencies between Liu's and Ye's testimony. Ye did testify that one damaged laptop was not searched, and Liu's declaration does not mention a damaged laptop. The Weeks Declaration states that with the proper tools and training, a professional could recover data from a damaged device. However, a court-ordered forensic examination of this damaged laptop would not be proportionate in this matter for the reasons described below.

The Weeks Declaration also explains that Liu's use of TeamViewer does not adhere to industry standards for searching computers remotely. [Dkt. No. 179-1 at 6-7.] Plaintiff does not explain why TeamViewer fails to adhere to those standards, nor does Plaintiff show how the use of TeamViewer caused the searches to be inadequate. Plaintiff has not shown that Liu failed to conduct an independent search of the New Jersey devices. Thus, the Court cannot conclude that any search conducted of the New Jersey devices was inadequate on those grounds.

III. Analysis

After a thorough review of the record and the parties' arguments, the Court finds that Plaintiff has not made the showing of proportionality required for the extraordinary remedy of a forensic examination of 13 of Defendants' devices, six of which are located in China, and of three broad categories of devices located in China.

Plaintiff seeks an order that the following devices located in China be shipped to the United States, where Plaintiff's expert would make a forensic image of each

device to be subsequently searched, and the original devices would then be returned to China:

1. Andy Chou/Apple iMac19;
2. Andy Chou/Apple MacBook Pro;
3. Lynn Lee/Apple MacBook Air;
4. Huiyun Wang/Colorful Desktop;
5. Gringer Lou/Colorful Desktop;
6. Andy Chou/Apple iPhone Xs;
7. All other devices used by any of the aforementioned individuals for their work for Defendants;
8. Defendants' devices that have or have ever had WeChat server data; and
9. Defendants' device that houses its [Enterprise Resource Planning ("ERP")] system.

Plaintiff also seeks to have the following devices located at Defendants' business in New Jersey shipped to its forensic expert:

1. 2019/Acer TC-885-UA92 Desktop;
2. 2018/Acer TC-885-UR12 Desktop;
3. 2021/Acer TC-1660-UA92 Desktop;
4. 2021/Acer TC-1660-UA92 Desktop;
5. 2021/Acer TC-1660-UA92 Desktop;
6. 2018/Dell Inspiron Laptop; and
7. 2018/Dell Inspiron Laptop.

[Dkt. No. 179-16.]

First, Plaintiff has not shown that Defendants intentionally destroyed or intentionally concealed relevant ESI, though Plaintiff has shown flaws in Defendants' searches and production of ESI, particularly the WeChat data. However, in light of the broad scope of the remedy sought by Plaintiff and the significant burden it would place on Defendants, the Court finds that Plaintiff has not shown how this requested forensic examination is proportional to the needs of the case. Importantly, the issue of liability in this trademark infringement matter was already settled on summary judgment and only the statutory damages issue remains. [Dkt. No. 103.]

A party may obtain discovery concerning any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case. Fed. R. Civ. P. 26(b)(1). In determining if the proportionality requirement has been met, Rule 26(b)(1) lists the following factors for courts to consider: the importance of the issues at stake in the action; the amount in controversy; the parties' relative access to the 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.* Relevant information need not be admissible to be discoverable. *Id.*

With respect to the flaws in the production of the WeChat data, Defendants have produced to Plaintiff Word documents showing the substance of the WeChat communications as well as the names of the sender and recipient and dates of those communication. Plaintiff does not identify any incomplete messages or content that it has concluded is missing from Defendants' production, and does not explain how such missing content is relevant to statutory damages. Plaintiff states that the metadata is missing, but does not explain the relevance of the metadata of the original messages beyond that it would allow it to determine whether Defendants have completed an adequate search for responsive material.

Initials of Preparer IM

Second, Plaintiff's request is not limited to a singular cell phone or laptop, but rather, multiple devices belonging to Defendant Chou, computing devices from an entire company warehouse, and a device which houses Defendant's ERP system. Despite requesting such a broad search of these various devices, Plaintiff does not argue the specific relevance of any individual device, including what may be found on that device, and does not show that any single device is "intricately related to the very basis of the lawsuit." *See Memry Corp. v. Kentucky Oil Technology, N.V.*, 2007 WL 832937, at *3 (N.D. Cal. 2007) (reviewing cases where the use of the devices at issue themselves lead to injury complained of in the lawsuit). Even in its efforts to search the damaged laptop located in New Jersey, Plaintiff makes no showing of information relevant to statutory damages that it seeks from that specific device or what it believes has been improperly withheld. Its various arguments related to missing documents or altered/removed metadata rest on speculation that responsive material exists and may be relevant to the remaining issue.

Third, despite Plaintiff's contention that the forensic imaging would be quick and the devices would immediately be returned by overnight shipping, there is a high risk for disruption to Defendants' business. Defendants state that even the use of overnight shipping, with potential delays due to pandemic lockdowns and customs, could deprive them of the devices for more than two weeks. Defendants also assert that shipping devices containing their customers' personal information from China would violate China's Data Security Law, which Defendants state prohibits providing any data stored in China to any foreign judicial or law enforcement agency without the prior approval of the relevant PRC authorities. [Dkt. No. 183-1 at 14-15.] Though this latter issue is not dispositive, along with the other factors cited by Defendants, it demonstrates the burden of the proposed discovery.

Initials of Preparer IM

Finally, the evidence presented on the sufficiency of production of the non-WeChat/Skype documents is not persuasive to find for any party. The parties' declarations aver contradictory conclusions and the Court is not in a position to sift through the thousands of pages produced to determine what constitutes a separate document, the accessibility of said document, and whether the related metadata is sufficient.

In conclusion, without a showing that outweighs Defendants' burden, Plaintiff's request is no more than an attempt to confirm the search already performed by Defendants and sworn to in a declaration that complies with the Court's March 8 order. Because Plaintiff does not show this extraordinary remedy is proportional to the needs of the case, its request for a forensic examination cannot be granted.

IV. Order

For all of the reasons set forth above, the Motion to Compel is denied.

In light of the flaws in Defendants' ESI production, and the conflicting information provided by the parties, the Court orders as follows:

1. WeChat Data

Defendants state that the "'to', 'from' and 'time/date'" data is included in both screenshots and cut and pasted version of WeChat messages. [Dkt. No. 183-1 at 11.] The Court concludes that the data to which Defendants refer is the data for the original WeChat message, not the metadata for the Word document produced to Plaintiff. Defendants' and Plaintiff's counsel are ordered to jointly review Defendants' production of WeChat messages to verify that the "'to', 'from' and 'time/date'" data is included in the screenshots which were cut and pasted into the production of Word documents.

2. Other ESI

As discussed above, the parties provided the Court with conflicting facts regarding the format and accessibility of ESI produced by Defendants between November 2021 and March 2022. On this record, the Court cannot make factual findings. The parties are ordered to further meet and confer **in good faith** with respect to the ESI produced by Defendants between November 2021 and March 2022. If, after that meet-and-confer, Plaintiff maintains that any of this ESI produced by Defendants is not in a reasonably usable form, the parties are ordered to meet jointly with a forensic examiner, with costs to be borne by Plaintiff, no later than April 27, 2022, to review the material that Plaintiff contends is not in a reasonably usable form. If the forensic examiner is unable to access the material in a reasonably usable form, then Defendants will re-produce the ESI in a readily usable format within two business days of the joint meeting with the forensic examiner.

IT IS SO ORDERED.

Initials of Preparer IM