UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

UMG RECORDINGS, INC., *et al.*, *Plaintiffs*, v. KURBANOV, *et al.*, *Defendants*.	Case No. 1:18-cv-00957-CMH-TCB

MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION TO COMPEL DEFENDANT TO PRESERVE AND PRODUCE SERVER DATA

Plaintiffs respectfully request that the Court order Defendant Tofig Kurbanov ("Defendant") to preserve and produce computer server data from Defendant's websites. This is core evidence that will demonstrate the rampant infringement taking place by virtue of Defendant's illegal stream-ripping activities that are the subject of this lawsuit. This motion does not ask Defendant to create new data. Defendant contends that the requested server data does not exist, but Defendant confuses whether the data is *created* in the normal course with whether Defendant *retains* the data in the normal course. The data obviously exists—it is generated as Defendant's websites receive, process, and respond to user requests for stream-ripping and downloading—and Plaintiffs simply ask that Defendant preserve and produce it.[1]

BACKGROUND

A. Case Overview

Plaintiffs are record companies that create, produce, distribute, and license the vast majority of all legitimate commercial sound recordings in the United States. Complaint, ECF

[1] Plaintiffs reserve all rights with respect to Defendant's prior failure to preserve server data.

No. 1, ¶ 1. Defendant owns and operates www.FLVTO.biz and www.2conv.com (collectively, "Defendant's Websites")—music piracy websites that engage in and facilitate copyright infringement at a staggering scale. *Id.* These websites provide users an unlawful "stream-ripping" service that converts authorized video streams from third-party platforms, such as YouTube, to unauthorized, downloadable audio files. *Id.* ¶ 2. Stream-ripping provides a means for easy, instantaneous, and rampant infringement of copyrighted sound recordings, including those owned by Plaintiffs. *Id.*

Plaintiffs allege that Defendant is directly, contributorily, and vicariously liable for infringement of their copyrighted sound recordings. Plaintiffs also allege that Defendant has circumvented technological protective measures that YouTube implemented to control access to and prevent copying of copyrighted works, in violation of Section 1201 of the Copyright Act.

B. Discovery Requests

Defendant is improperly withholding documents that are responsive to Plaintiffs' Requests for Production Nos. 2, 5–7, 9, 12, 30, and 31. In the ordinary course of operations, Defendant's Websites necessarily generate server data, including data that identifies: (a) the YouTube videos being stream-ripped; (b) the MP3 audio files being copied and distributed; and (c) the geographic locations of the users downloading the audio files. That information is plainly relevant to the core claims and defenses in this case, including the scope and extent of infringement, Defendant's financial benefit from infringement, and Defendant's affirmative defense that Defendant's Websites have significant non-infringing uses.

More specifically, the requests are as follows:

- Request for Production No. 2: Documents sufficient to identify each sound recording that Defendant's Websites converted from a video stream from a Source Site into a downloadable audio file, including the track title, the recording artist, identifying information for the video stream from the Source Site, the URL of the video stream from which Defendant's Websites extracted the audio file, the URL of the downloadable audio file, and the date and time that Defendant's Websites created the audio file.

- Request for Production No. 5: Documents sufficient to identify each sound recording that Users downloaded within the United States using Defendant's Websites, including the track title, the recording artist, identifying information for the video stream from the Source Site, the URL of the video from which Defendant's Websites extracted the audio file, the date and time of the download, and the geographic location (i.e., state) of the User.

- Request for Production No. 6: All server logs or other documents showing the video streams from any Source Site converted into downloadable audio files using Defendant's Websites and any subsequent storage, copying, distribution or other use of the audio files.

- Request for Production No. 7: For each sound recording that Defendant's Websites converted from a video stream from a Source Site into a downloadable audio file, all documents concerning each subsequent use, copying, storage, distribution, or other disposition of the audio file, including the date and time of download of the audio file and the geographic location (i.e., state) of the User.

- Request for Production No. 9: Documents sufficient to identify each sound recording that Defendant's Websites copied to computer servers that You own, control, or have access to through any contract, subscription, or other agreement, including the track title, the recording artist, identifying information for the video stream from the Source Site, the URL of the video from which Defendant's Websites extracted the audio file, the date and time that Defendant's Websites copied the sound recording, and the IP address and the geographic location of each computer server from which Defendant's Websites acted in the process.

- Request for Production No. 12: All documents showing, on a yearly and monthly basis, the frequency of converting video streams from a Source Site into downloadable audio files using Defendant's Websites, including lists of the most frequently converted music video streams.

- Request for Production No. 30: All documents concerning the use of location-specific advertising to Users in the United States in connection with Defendant's Websites.

- Request for Production No. 31: All documents concerning the use of data associated with Users, including for location-specific or interest-based advertising, in the United States in connection with Defendant's Websites.

Ex. A, at Nos. 2, 5–7, 9, 12, 30, 31.[2]

In his written objections and responses to these requests, Defendant did not challenge the relevance of this information. Defendant's objections and responses to each of the above-referenced requests read as follows:

- **Objection**: Defendant objects to this Discovery Request as overbroad and unduly burdensome. Defendant objects to this request to the extent that it could be read to require Defendant to create or produce documents that do not otherwise exist or which are not within the Defendant's care, custody, or control. Defendant objects to this inquiry to the extent that it could be read to impose an obligation on Defendant to conduct independent research for Plaintiffs' benefit. Subject to these objections, Defendant responds as follows.

- **Response**: Defendant has no responsive documents or things in his care, custody, or control.

Id.

C. Attempts to Confer

Plaintiffs served their first set of interrogatories and document requests on Defendant on April 7, 2021. (Noyola Decl. ¶ 3). That discovery included Plaintiffs' Request Nos. 2, 5–7, 9, 12, 30, and 31 described above.

When the parties had their Rule 26(f) conference on April 19, 2021, Defendant did not indicate that he was not retaining the data sought in Plaintiffs' discovery requests. *Id.* ¶ 4. Although the Federal Rules of Civil Procedure require the parties to discuss "any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced," Defendant refused to agree to—or even discuss—this

[2] All exhibits are attached to the Declaration of Lucy Grace D. Noyola ("Noyola Decl."), filed contemporaneously with this motion.

topic, deeming it "premature." Fed. R. Civ. P. 26(f)(3)(C); (Noyola Decl. ¶ 4); Proposed Joint Discovery Plan, ECF No. 82, at 4.

During a conferral on May 4, 2021, Defendant indicated for the first time that Defendant did not have server data to produce, without providing additional explanation. (Noyola Decl. ¶ 7). In a series of follow-up emails and calls over ensuing weeks, Plaintiffs requested that Defendant identify the server software he is currently using and that the parties attempt to work through this discovery issue. *Id.* Defendant's counsel stated that Defendant's counsel "are not fact witnesses" and that Defendant would not be disclosing additional information and had no server data to produce. *Id.*

D. <u>The Requested Data</u>

In support of this motion, Plaintiffs are attaching the declaration of Robert W. Schumann. Mr. Schumann has worked in the computer and technology industry for over thirty years. (Schumann Decl. ¶ 3). To aid the Court, Mr. Schumann provides an overview of Defendant's Websites and the related technology, focused on the issues in this motion.[3]

1. Defendant's Websites

Defendant's Websites provide users with the ability to download the audio portions of YouTube videos as audio files. *Id.* ¶ 7. YouTube does not provide a feature to download audio files of its videos. *Id.* YouTube is a streaming service—users can view and listen to music

[3] Mr. Schumann's declaration is not meant as a wholesale examination of Defendant's Websites. For instance, his declaration does not explore how Defendant's Websites circumvent the technological measures that YouTube has implemented to control access to content maintained on its site and to prevent or protect against illicit activities such as stream-ripping.

videos on YouTube while they are connected to the internet, but the transmission of those videos does not provide users with a permanent copy of the music videos for offline access. *Id.*

Each video on YouTube has a unique watch-page Uniform Resource Locator ("URL"), which is the address of the video's page on YouTube. *Id.* ¶ 8. To use one of Defendant's Websites, a user (1) pastes the watch-page URL of a desired video into a blank text box on the home page, (2) checks a box to indicate agreement to the terms of use, and then (3) clicks on a "convert" button. *Id.* The final step above takes the user to a new page that, after a matter of seconds, presents a link to download from Defendant's Website an MP3 audio file of the audio portions of the desired video. *Id.* When the user clicks on the download link, the MP3 audio file downloads from the server of Defendant's Websites to the user's computer. *Id.*

2. The Client-Server Model

Websites, including Defendant's Websites, use what is known as the client-server model. *Id.* ¶ 9. In the client-server model, a client makes requests to a server, and the server sends responses. *Id.* The client is the computer (or internet-access device such as a smartphone or tablet) of a user of Defendant's Website. *Id.* Specifically, the client is web browser software, such as Google Chrome, Apple Safari, or Microsoft Edge running on the user's computer. *Id.* The computers underlying the Website are the servers. *Id.* They are known as web servers because they are designed to respond to requests from web browsers. *Id.* The most widely used web server programs include Apache, Nginx, and Microsoft IIS. *Id.*

When the user visits the home page of Defendant's Websites, this visit consists of a request made by the user's web browser (the client) to the web server of Defendant's Websites over the internet. *Id.* ¶ 10. Each request is in effect a message that includes the external Internet Protocol ("IP") address of the user's computer and the URL of the resource, such as a webpage or file, that the user wishes to retrieve. *Id.* The server processes the request and sends the appropriate resource to the browser. *Id.*

A web server receives each request via a network connection and necessarily maintains the request in temporary memory known as Random Access Memory ("RAM") during the processing of the request. *Id.* ¶ 11. RAM is distinct from permanent storage, such as that on a hard drive, in that the contents of RAM are lost if the server is turned off. *Id.*

3. The Common Preservation of Server Data

Website operators commonly configure their web servers to maintain logs of server activity for a variety of reasons, including the detection of errors, detection of abuse, analysis of which site features are most popular with users, and audits of traffic volumes for determining advertising revenue. *Id.* ¶ 12. Web servers maintain these logs on permanent storage media, such as hard drives, that are attached or otherwise local to the web servers. *Id.* These media are permanent in the sense that they retain their data even when powered off. *Id.* Web servers may be configured to store logs indefinitely or for a certain period such as 30 days, after which they are deleted from the storage medium. *Id.*

The popular web server programs mentioned above, and other comparable ones, include functionality for logging each request and the fact and nature of the response to each request (but not the full response itself). *Id.* ¶ 13. Site operators may supplement local logging with remote logging to third-party services such as Google Analytics and Yandex Metrica that provide sophisticated reporting functionality. *Id.* ¶ 14. These services are also referred to as web analytics services. *Id.* A website operator using a remote logging service defines, via the program code of their website, precisely which events should be remotely logged. *Id.*

4. Defendant's Server Data

In general, it is impossible for an outsider in the position of a user, with no administrative access to the website's web server, to determine whether a website is engaging in local logging. *Id.* ¶ 15. The nature of the remote logging services, however, is that their use is easily apparent, even to an outsider, because each logged event results in a distinct and visible interaction between the user's browser and the remote logging service. *Id.*

As described above, ordinary use of Defendant's Websites involves the click of a "convert" button and the subsequent click of a link to download an MP3 audio file. *Id.* ¶ 16. Each of these events generates distinct requests from a user's browser to Defendant's Websites that are of the sort that would be recorded by web server software with logging activated. *Id.*

The "convert" request generated by a click of the "convert" button contains the watch-page URL of the video for which the user desires the audio portion. *Id.* ¶ 17. The "MP3 download" request contains the filename of the MP3 file, which, in the case of music, typically contains the name of the artist and the title of the sound recording. *Id.* Server logs for Defendant's Websites (if the server data is preserved in a log) also would indicate the volume of usage by date and geographical region and identify the content being requested for conversion and subsequently downloaded. *Id.*

According to observable responses generated by Defendant's Websites, the web server program in use by Defendant appears to be Nginx. *Id.* ¶ 18. In addition, Defendant's Websites use Yandex Metrica to record each "convert" request and each "MP3 download" request. *Id.*

ARGUMENT

In the ordinary course of operations, Defendant's Websites necessarily generate server data, including data that identifies: (a) the YouTube videos being stream-ripped; (b) the MP3 audio files being copied and distributed; and (c) the geographic locations of the users downloading the audio files. Respectfully, the Court should order Defendant to preserve and produce this key evidence.

A. <u>Defendant Has a Duty to Preserve Existing Server Data</u>

Server data exists by mere operation of the Defendant's Websites. Defendant deliberately confuses the issues by contending that he "has no responsive documents or things in his care, custody, or control" and is not obligated to "create or produce documents that do not otherwise exist." *See supra* p. 4. If Defendant is to be believed, server logs apparently do not exist because Defendant has deliberately chosen not to preserve the server data by retaining it on a server log—even after Plaintiffs expressly asked Defendant to produce the data in the context of this litigation. But, as Mr. Schumann explains, there necessarily ***is*** server data that is created in the normal course of Defendant's stream-ripping operation—including, without limitation, information that identifies the source file URL, the audio track copied and distributed, and the downloader's geographic location. *See supra* p. 8. The problem is that Defendant has configured his server software to turn the logging function off—thus, continually overwriting important data that Plaintiffs explicitly requested in discovery. *See* Ex. A, at Nos. 2, 5–7, 9, 12, 30, 31.

Defendant is not entitled to hide behind his allegedly regular business practices as a means to defeat his preservation obligations. Generally, a party "must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents." *Steves & Sons, Inc. v. JELD-WEN, Inc.*, 327 F.R.D. 96, 108 (E.D. Va. 2018) (quoting *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003)); *In re Ethicon, Inc. Pelvic Repair Sys. Prod. Liab. Litig.*, 299 F.R.D. 502, 518 (S.D.W.

Va. 2014) (same). Further, the advisory committee's notes to Federal Rule of Civil Procedure 37 expressly state that "a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve." Fed. R. Civ. P. 37 advisory committee's notes to 2006 amendment, ¶ 3. Indeed, "in some circumstances, the general duty to preserve may also include deleted data, data in slack spaces, backup tapes, legacy systems, and metadata." *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 524 (D. Md. 2010) (alterations & internal quotation marks omitted).

The fact that Defendant must take some (minimal) affirmative steps to preserve the server data does not require Defendant to create new evidence. It is a bedrock principle that, once a party is required to preserve existing evidence, the party must take affirmative steps to do so. *See*, *e.g*., *R.F.M.A.S., Inc. v. So*, 271 F.R.D. 13, 24 (S.D.N.Y. 2010) (holding that "[t]o fulfill this preservation obligation, a litigant must take affirmative steps to prevent inadvertent spoliation . . . [including] suspending any routine document destruction or other processes involved in the ordinary course of business that might result in the destruction of potentially relevant evidence"); *see also Nacco Materials Handling Grp., Inc. v. Lilly Co.*, 278 F.R.D. 395, 403–04 (W.D. Tenn. 2011) (finding that defendant failed to preserve data concerning access to a secure website when it did not suspend or adjust its routine overwriting and automatic deletion features); *Nat'l Ass'n of Radiation Survivors v. Turnage*, 115 F.R.D. 543, 557–58 (N.D. Cal. 1987) (declaring that "[t]he obligation to retain discoverable materials is an affirmative one"). Indeed, the Federal Rules of Civil Procedure make clear that sanctions may be appropriate. Fed. R. Civ. P. 37(e) (permitting sanctions "[i]f electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery").[4]

Courts in other circuits that have faced this very issue have required preservation. For example, the U.S. District Court for the Central District of California held in an internet piracy case that the duty to preserve extends to data, such as a user's IP address, stored temporarily on RAM. *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 447–48 (C.D. Cal. 2007). The court rejected the defendants' argument that "RAM holds data for such a short duration that it is not stored subject to later access and retrieval." *Id.* at 448. Rather, the court declared that the rules of discovery "require[] no greater degree of permanency from a medium than that which makes obtaining the data possible." *Id.* at 447. Notably, the court also highlighted the defendants' ability to control the routing of data through its servers. *Id.* at 453; *accord Arista Recs. LLC v. Usenet.com, Inc.*, 608 F. Supp. 2d 409, 431 (S.D.N.Y. 2009) (rejecting defendants' argument that "they had no duty to preserve the electronic Usage data because of its transitory nature and because it served no business purpose").

Defendant's server data is no different than the data in *Bunnell*. The server data exists, and Plaintiffs simply ask that Defendant be ordered to preserve and produce that data.

[4] Defendant cannot reasonably argue that the server data does not constitute electronically stored information ("ESI") under Federal Rule of Civil Procedure Rule 34(a). The data exists in the RAM of the Defendant's Websites' server. *See supra* p. 7–8. Rule 34(a)(1) "is expansive," "includes any type of information that is stored electronically," and covers information "stored in any medium." Fed. R. Civ. P. 34(a) advisory committee's notes to 2006 amendment, ¶ 2. "Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined." *Id.* ¶ 1. Courts have deemed RAM copies sufficiently fixed. *See*, *e.g.*, *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 446–48 (C.D. Cal. 2007) (ordering defendant to preserve and produce server log data that was temporarily stored in RAM); *see also Quantum Sys. Integrators, Inc. v. Sprint Nextel Corp.*, 338 F. App'x 329, 337 (4th Cir. 2009) (unpublished) (finding that RAM copies are "sufficiently fixed for purposes of copyright infringement").

B. The Court Has Ample Authority

There can be no reasonable dispute as to the Court's authority to enter an order requiring Defendant to preserve the server data going forward and produce it in discovery. Federal Rule of Civil Procedure 16 allows courts to enter orders governing the pretrial course of the action, including: "preservation of electronically stored information," Fed. R. Civ. P. 16(b)(3)(B)(iii); "other appropriate matters," Fed. R. Civ. P. 16(b)(3)(B)(vii); "controlling . . . discovery, including orders affecting disclosures and discovery under Rule 26 and Rules 29 through 37," Fed. R. Civ. P. 16(c)(2)(F); and "adopting special procedures for managing . . . protracted actions," Fed. R. Civ. P. 16(c)(2)(L). In addition, the Court may require preservation of evidence pursuant to its inherent power. *United States v. Salad*, 779 F. Supp. 2d 503, 507 (E.D. Va. 2011) (holding that "a federal court has the inherent power to order the preservation of evidence in the hands of a party before the Court"); *Pueblo of Laguna v. United States*, 60 Fed. Cl. 133, 135 (2004) (observing that "courts have held that they have the inherent power to order that evidence be preserved and have, for good cause, required that specific procedures be adopted to ensure such preservation").

Courts generally apply one of two tests in determining whether to enter a preservation order. Some courts require the party seeking the preservation order to show that it is "necessary and not unduly burdensome," whereas other courts employ a balancing test of three factors:

> 1) the level of concern the court has for the continuing existence and maintenance of the integrity of the evidence in question in the absence of an order directing preservation of the evidence; 2) any irreparable harm likely to result to the party seeking the preservation of evidence absent an order directing preservation; and 3) the capability of an individual, entity, or party to maintain the evidence sought to be preserved, not only as to the evidence's original form, condition or contents, but also the physical, spatial and financial burdens created by ordering evidence preservation.

Compare Pueblo of Laguna, 60 Fed. Cl. at 138, *with Capricorn Power Co. v. Siemens Westinghouse Power Corp.*, 220 F.R.D. 429, 433–34 (W.D. Pa. 2004). The tests are similar to one another, and Plaintiffs meet them both.

C. Preservation Is Warranted

The preservation order is necessary. Absent the order, Defendant will continue to destroy key server data. Defendant's refusal to preserve and produce the data irreparably prejudices Plaintiffs' ability to prepare their case for adjudication.

At all pertinent times, Defendant provides a service for stream-ripping, directed toward distributing infringing music files, most of which are owned by Plaintiffs. The data sought is compelling evidence of Defendant's infringement and other unlawful acts—evidence of the actual usage of Defendant's service. The server data would identify each of Plaintiffs' copyrighted works and how often they have been stream-ripped and infringed, which is key evidence in proving liability and damages. Without the requested order compelling preservation and production, Plaintiffs also will be prejudiced in their ability to rebut conclusively Defendant's affirmative defense alleging that Defendant's Websites have "significant non-infringing uses." Answer, ECF No. 81, at 11. Moreover, the volume of infringement is key evidence because high infringement levels "provide[] the backdrop against which all of [the defendant's] actions must be assessed." *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 454 F. Supp. 2d 966, 985 (C.D. Cal. 2006); *see also Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 929–41 (2005).

The preservation and production of server data does not present an undue burden in this case. Logging is a common activity. In fact, Defendant already engages in some form of remote logging via Yandex Metrica. *See supra* pp. 7–8; *see also* Kurbanov Declaration, ECF No. 25-1,

¶¶ 35–40 (citing use of Yandex Metrica); *UMG Recordings, Inc. v. Kurbanov*, 963 F.3d 344, 355 (4th Cir. 2020) (holding that the court had personal jurisdiction in part because Defendant collected the personal data of users in Virginia and sold the data to advertisers). Defendant can preserve the requested server data merely by enabling the logging function that undoubtedly is already built into his server software. *See supra* p. 7. Defendant can store the server log data on a hard-drive or in the cloud.

Defendant has not come forward under Rule 26(b)(2)(B) to show that the requested information is not accessible because of undue burden or cost. In fact, Defendant would not even allow his counsel to discuss ESI issues with Plaintiffs, including Defendant's Websites' web server software. In any event, Plaintiffs have shown "good cause" for Defendant to be ordered to preserve and produce the data. Fed. R. Civ. P. 26(b)(2)(B). It is important evidence that only Defendant can preserve. To the extent Defendant raises any issues as to the scope of preservation, *e.g.*, the specific information to preserve and produce, the format, the time period, or otherwise, they can be addressed.

CONCLUSION

For the reasons discussed above, Plaintiffs respectfully request that the Court grant the relief requested herein. A proposed Order is attached.

Respectfully submitted,

Dated June 16, 2021

/s/ Scott A. Zebrak
Scott A. Zebrak (VSB No. 38729)
Matthew J. Oppenheim (*pro hac vice*)
Lucy Grace D. Noyola (*pro hac vice*)
Kellyn M. Goler (*pro hac vice*)
OPPENHEIM + ZEBRAK, LLP
4530 Wisconsin Avenue, NW, 5th Floor
Washington, DC 20015
Tel: (202) 480-2999
Fax: (866) 766-1678
scott@oandzlaw.com
matt@oandzlaw.com
lucy@oandzlaw.com
kellyn@oandzlaw.com

Attorneys for Plaintiffs