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

PLAINTIFFS' MEMORANDUM IN OPPOSITION TO DEFENDANT'S OBJECTIONS TO MAGISTRATE JUDGE BUCHANAN'S DISCOVERY ORDER

TABLE OF CONTENTS

INTRODUCTION 1

LEGAL STANDARD 2

BACKGROUND 3

A. Case Overview 3

B. Defendant's Prior Refusal to Comply with His Discovery Obligations and His Willful Disobedience of This Court's Earlier Order 3

C. Plaintiffs' Motion for Defendant to Preserve and Produce Server Data 5

1. Plaintiffs' Discovery Requests 5

2. Plaintiffs' Motion to Compel the Server Data 6

3. The Hearing, The Order, and Defendant's Objections 7

ARGUMENT 8

A. Defendant Has an Obligation to Preserve Existing Server Data 9

B. The Server Data Is ESI 12

C. Defendant's Privacy Argument Also Fails 15

CONCLUSION 17

INTRODUCTION

Magistrate Judge Buchanan carefully considered the briefing, declarations, and oral argument and then granted Plaintiffs' motion to compel, ordering Defendant Tofig Kurbanov ("Defendant") to preserve and produce server data from Defendant's websites (the "Order"). (ECF No. 105.) The Order is fully supported by the law and the undisputed facts in the record. Defendant's objections to the Order have no merit and fail to meet the high standard for reversing a magistrate judge's discovery order.[1]

The data at issue 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. The server data is essential to the operation of Defendant's websites and identifies: the YouTube videos that are stream-ripped; the MP3 files that are copied and distributed; and the geographic locations of the users downloading the audio files.

Defendant concedes that the data is created in the normal operation of his websites, exists, and can be preserved with the flip of a switch using built-in functionality in his web server software. Defendant further concedes that the data is relevant and that preservation and production of the data does not present an undue burden. Based on these undisputed facts, there is no sound basis to reverse Magistrate Judge Buchanan's Order. Defendant instead challenges the Order by arguing that the data is too "ephemeral" to constitute electronically stored information ("ESI") because it resides in his servers' Random Access Memory ("RAM") but is not permanently stored and by arguing that the Order would require him to create new documents. As explained below, however, Magistrate Judge Buchanan's Order is wholly

[1] Defendant objects to only a portion of the Order. Defendant does not object to the portion of the Order that requires him to obtain copies of the requested web server data accessible in his account at a web analytics service called Yandex Metrica. *See infra* at 6–8.

consistent with settled law. The 2006 Amendments to Federal Rule of Civil Procedure 34 and relevant case law flatly reject Defendant's argument. Defendant simply refuses to accept the definition of ESI under Rule 34, attempting to add a permanency requirement to "electronically stored information."

Defendant further objects to the Order by raising alleged privacy concerns. But Magistrate Judge Buchanan correctly rejected Defendant's privacy concerns, observing that users of Defendant's websites affirmatively consent to the very disclosure that Defendant now protests.

LEGAL STANDARD

The alteration of a magistrate judge's non-dispositive order is "extremely difficult to justify." *White v. Chapman*, No. 1:14cv848(JCC/IDD), 2015 WL 4360329, at *2 (E.D. Va. July 14, 2015) (quoting *Bruce v. Hartford*, 21 F. Supp. 3d 590, 593 (E.D. Va. 2014); 12 Charles Alan Wright, Arthur R. Miller & Richard L. Marcus, Federal Practice and Procedure § 3069 (2d ed. 1997)). Accordingly, a district court modifies a magistrate judge's discovery order only upon finding that it is "clearly erroneous or contrary to law." *Id.* (quoting Fed. R. Civ. P. 72(a)); *see also Jesselson v. Outlet Assocs. of Williamsburg, LP*, 784 F. Supp. 1223, 1228 (E.D. Va. 1991).

A magistrate judge's finding of fact should be affirmed unless the district court "on the entire evidence is left with the definite and firm conviction that a mistake has been committed." *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948); *see also Foodbuy, LLC v. Gregory Packaging, Inc.*, 987 F.3d 102, 113 n.10 (4th Cir. 2021). A magistrate judge's legal finding may be reversed only when the magistrate judge's order "fails to apply or misapplies relevant statutes, case law, or rules of procedure." *Attard Indus. v. U.S. Fire Ins. Co.*, No. 1:10cv121 (AJT/TRJ), 2010 WL 3069799, at *1 (E.D. Va. Aug. 5, 2010) (quoting *DeFazio*

v. Wallis, 459 F. Supp. 2d 159, 163 (E.D.N.Y. 2006)). Questions of law are reviewed de novo under this standard, but "the decisions of a magistrate judge concerning discovery disputes and scheduling should be afforded 'great deference.'" *Malibu Media, LLC v. John Does 1–23*, 878 F. Supp. 2d 628, 629 (E.D. Va. 2012) (quoting *In re Outsidewall Tire Litig.*, 267 F.R.D. 466, 470 (E.D. Va. 2010)).

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 ¶ 1, ECF No. 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. Defendant's Prior Refusal to Comply with His Discovery Obligations and His Willful Disobedience of This Court's Earlier Order

Defendant's objections to Magistrate Judge Buchanan's Order are merely the latest installment in his strategy of stonewalling and trying to run out the clock on Plaintiffs' time to

fully develop their case. Discovery began on April 1, 2021, and it is set to close on August 13, 2021. On April 7, 2021, Plaintiffs promptly served Defendant with interrogatories and document requests. In response to some of the interrogatories, Defendant refused to answer, invoking the Fifth Amendment right against self-incrimination. (ECF No. 99-3 (Interrog. Nos. 1–3, 8, 10).)

Separately, Defendant initially produced some documents, but then stopped altogether. As a result, on May 26, 2021, Plaintiffs filed a motion to compel Defendant to produce: (1) documents Defendant had initially agreed, but then refused, to produce; (2) documents Defendant claimed do not exist but undoubtedly must exist; and (3) unredacted versions of documents Defendant produced with improper redactions. (ECF No. 91.) The document requests at issue sought information that 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 users use his Sites for non-infringing uses. Defendant's improper redactions were an attempt to conceal relevant information about the identities of those involved in the illegal scheme, the nature and extent of the illicit profits, and the money trail.

Following a hearing on June 4, 2021, the Court granted Plaintiffs' motion in its entirety, ordering Defendant to produce and un-redact documents by June 11, 2021, and directing Plaintiffs to seek their fees and costs associated with the motion. (ECF No. 97.) The Court advised Defendant that his failure to comply with the order could result in the entry of sanctions, including default judgment. (*Id.*)

Defendant disobeyed the Court's order. He did not produce or un-redact the documents by June 11 nor thereafter. Defendant's counsel has acknowledged that Defendant understands what the Court has ordered but refuses to comply with the June 4 Order. (ECF No. 101.) On

June 25, 2021, the Court again warned Defendant of the consequences of his non-compliance. (Hr'g Tr. 27:14–28:09, ECF No. 108-2.) Plaintiffs intend to seek sanctions.

C. Plaintiffs' Motion for Defendant to Preserve and Produce Server Data

1. Plaintiffs' Discovery Requests

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.

When the parties had their Rule 26(f) conference on April 19, 2021, Defendant did not indicate that he was not retaining the server data sought in Plaintiffs' discovery requests. 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 topic, deeming it "premature." Fed. R. Civ. P. 26(f)(3)(C); (Noyola Decl. ¶ 4, ECF No. 99-1); (Proposed Joint Discovery Plan at 4, ECF No. 82).

During a conferral on May 4, 2021, Defendant indicated for the first time, and without explanation, that Defendant did not have server data to produce. (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.*)

2. Plaintiffs' Motion to Compel the Server Data

On June 16, 2021, Plaintiffs filed a motion to compel Defendant to preserve and produce web server data. (ECF No. 98.) Plaintiffs explained in their memorandum in support of the motion that the issue before the Court is whether Defendant will flip a switch on his *web server* software so that the data at issue will be saved rather than erased. (Pls.' Mem. at 13–14, ECF No. 99 (attached as "Exhibit A").) As set forth in the declaration of Robert W. Schumann attached to Plaintiffs' motion, the requested preservation of server data can occur locally, on Defendant's web server software using its already built-in functionality. (*Id.*; Schumann Decl. ¶¶ 12–14, ECF No. 99–6 (attached as "Exhibit B").) Logging using web server software is routine among website operators, and something Defendant can do easily. (Pls.' Mem. at 7; Schumann Decl. ¶¶ 12–14). Web server programs, including the one that Defendant appears to be using (Nginx), have built-in functionality for logging the data at issue, rather than letting it erase from the servers' temporary storage. (Pls.' Mem. at 7; Schumann Decl. ¶ 13.) In addition, apart from local logging at the web server level, site operators may engage in remote logging to third-party services such as Google Analytics and Yandex Metrica that provide sophisticated reporting functionality. (Pls.' Mem. at 7; Schumann Decl. ¶ 14.) These services are also referred to as web analytics services. *Id.* Defendant's Websites use Yandex Metrica to record each "convert" request and each "MP3 download" request. (Pls.' Mem. at 8; Schumann Decl. ¶¶ 16–18.)

In his opposition, Defendant conceded that the data at issue "does exist." (Opp'n at 13, ECF No. 102.) Defendant did not argue that the requested data lacked relevance. Nor could Defendant make that argument, as the requested data concerns core issues of liability and

damages, and his discovery objections did not contest relevance. (ECF No. 99-2 (Req. Nos. 2, 5–7, 9, 12, 30, 31).) Defendant also conceded a lack of any undue burden, indicating that compliance could cost only up to a few thousand dollars. (Pls.' Reply at 6, ECF No. 103 (attached as "Exhibit C").)

Instead, Defendant attempted to confuse matters by discussing his custom-made *website* software—which is distinct from the standard web server software that underlies it—and what is allegedly involved with re-programming that website software. (Kurbanov Decl. ¶¶ 7–9, ECF No. 102-1; Opp'n at 1, 4.) Defendant further attempted to confuse matters by making assertions about his alleged practices concerning storage of stream-ripped *audio files*. (*Id.* ¶¶ 10–11; Opp'n at 5.) However, Defendant's allegations about his website software, his German web host, and the audio files themselves were irrelevant. Plaintiffs instead sought Defendant's preservation and production of *web server data*, using his *web server* software. Plaintiffs also requested that Defendant log into his Yandex account to run reports that provide the data stored at Yandex.

Accordingly, Defendant did not dispute that: (a) the server data at issue exists; (b) Defendant uses Nginx web server software—which has built-in logging functionality that can preserve the server data; and (c) Defendant already engages in remote logging via Yandex Metrica.

3. The Hearing, The Order, and Defendant's Objections

At the June 25, 2021 hearing before Magistrate Judge Buchanan, Defendant conceded that the data is created in the normal operation of his websites. (Hr'g Tr. 19:18–21:18.) Defendant further conceded that the data is relevant and preservation and production of the data does not present an undue burden. (*Id.* at 19:9–11, 20:17–24, 23:10–11; *see also id.* at 19:21 ("Yes, it's a matter of flipping a switch . . . .").)

After considering the parties' written submissions and oral argument, Magistrate Judge Buchanan granted Plaintiffs' second motion to compel. (ECF No. 105.) The Order included two requirements. First, the Order required Defendant to change the settings on his web server software to preserve the requested web server data beginning no later than July 2, 2021, and then to produce that data to Plaintiffs on a weekly basis beginning on July 9, 2021. (Hr'g Tr. 29:24–25, 30:23–24.) Second, the Order required Defendant to log into his account at Yandex and produce reports with the requested data stored at Yandex by July 6, 2021. (*Id.* at 29:24–30:03.) Defendant's objections presently before the Court challenge only the former, not the latter. As of this filing, Defendant has not produced any Yandex data as required by the Order.

Late in the day on Friday, July 2, 2021, Defendant filed objections to Magistrate Judge Buchanan's Order, noticing a hearing for Friday, July 9, 2021. (ECF Nos. 107–09.) Despite Defendant's continued obfuscation, he again admits that the data at issue does exist, at least until it is erased. (Obj. Mem. at 11 ("Ultimately, though, it is undisputed that the server data Plaintiff seeks to have preserved and produced does not now 'exist,' nor has it ever 'existed' in a stored form (*other than as transitory, ephemeral data*)." (emphasis added)); *id.* at 12 ("[I]t is true that, for a brief duration of time, the data with which such files could be created does exist . . . .").) Defendant's substantive objections repeat the same arguments that Magistrate Judge Buchanan rejected. (*Compare* Obj. Mem., *with* Opp'n.)

ARGUMENT

Magistrate Judge Buchanan correctly determined that the requested web server data is ESI and that Defendant's privacy concerns did not preclude the Court from requiring that Defendant preserve and produce the data.

A. Defendant Has an Obligation to Preserve Existing Server Data

In contending that the requested server data does not "exist," and thus has never been "stored" as is required to come within the ambit of Federal Rule of Civil Procedure 34, Defendant continues to deliberately confuse whether the data is *created* in the normal course with whether Defendant *retains* the data in the normal course. Magistrate Judge Buchanan understood the distinction and issued the Order, which simply requires Defendant to preserve and produce data that undisputedly exists in the temporary memory (RAM) of Defendant's web servers, rather than let it be erased. The fact that Defendant must take some (minimal) affirmative steps to preserve the server data does not require Defendant to create new evidence.

In support of his objections, Defendant relies in large part on a comment about "creating information" that Magistrate Judge Buchanan made from the bench during the discovery hearing. Defendant asserts "there is no question but that the Magistrate [Judge] understood … [that] her order required the creation of new materials that would not otherwise exist." (Obj. Mem. at 2, ECF No. 108.) But Defendant's claim is demonstrably false. Defendant misrepresents the Magistrate Judge's ruling and takes a snippet of words out of context.

First, Defendant conveniently ignores Magistrate Judge Buchanan's subsequent statements, clarifying the ruling: "He's not actually creating data. The data is there in the RAM memory. . . . So he is not in my mind creating it. He is preserving something that's already there in the RAM memory. He's just going to have to preserve it in a longer-term storage fashion." (Hr'g Tr. 26:16–17, 27:3–6; *see also id.* at 23:16–17 ("The ESI is there. It's just in the RAM. It's not in the permanent storage."); *id.* at 26:19–20 ("He has to preserve it in a longer-term storage – computer storage.").)

Second, when Defendant's counsel argued that "[u]nder federal rules, ESI is only ESI if it's permanently stored. If it's in fleeting RAM, then it's not," Magistrate Judge Buchanan

responded that "it's not different – I don't see how it's fundamentally different from telling somebody to turn off auto-delete." (*Id.* at 23:18–23.) The record is thus clear that Magistrate Judge Buchanan correctly understood that Defendant's web server data exists in his web servers' RAM memory, without requiring Defendant to create new data.

The Magistrate Judge's finding that the server data exists is fully supported by the evidence in the record. In support of their motion, Plaintiffs submitted an *unrebutted* expert declaration from Robert W. Schumann, explaining how the server data at issue is generated and stored on Defendant's servers as Defendant's Websites receive, process, and respond to user requests for stream-ripping and downloading. Mr. Schumann explained how Defendant can preserve the data by changing a setting on Defendant's web server software. Mr. Schumann further explained how Defendant already engages in some form of remote logging, through use of the Yandex Metrica web analytics service.

As Mr. Schumann explains, server data is necessarily 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. (Schumann Decl. ¶¶ 16–17.) 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.

In his opposition, Defendant admitted that the data at issue exists but argued he should not be required to change his regular business practices to preserve the data. (Obj. Mem. at 12.) At the hearing, Defendant's counsel agreed with Plaintiffs' counsel's description of the relevant technology and the existence of—and Defendant's ability to preserve—the server data. (Hr'g Tr. 19:9–23.)

Defendant is not entitled to hide behind his alleged regular business practices 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. These principles are universal, without regard to whether the documents are email, physical paper, or web server data.

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 for not taking those affirmative steps. 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").

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.

B. The Server Data Is ESI

Boiled to its essence, Defendant's position is that the server data is not ESI within the meaning of Federal Rule of Civil Procedure 34 because the data is "ephemeral data" that exists only temporarily unless Defendant takes basic steps to preserve it. (Obj. Mem. at 12; Hr'g Tr. 19:18–23, 21:1–18.) Defendant makes that argument only with respect to the web server data that Plaintiffs sought an order to require him to preserve and produce; Defendant does not

dispute that the data he has already stored at Yandex via remote logging is ESI and must be produced.

There is no merit to Defendant's arguments that the server data at issue is too ephemeral to constitute ESI under Rule 34(a). 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 note 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.* ¶ 2.

Courts have deemed RAM data sufficiently fixed, both for purposes of constituting ESI and infringement under the Copyright Act. *See*, *e.g.*, *Bunnell*, 245 F.R.D. at 446–48 (ordering defendant to preserve and produce server log data that was temporarily stored in RAM); *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").[2]

Defendant's principal case, *Paramount Pictures Corp. v. Replay TV*, 2002 U.S. Dist. LEXIS 28126 (C.D. Cal. May 30, 2002), is inapposite. *Replay TV* involved a demand for data *on devices at users' locations*, not data that a defendant received, processed, and responded to on its own servers. *Bunnell* rejected the same argument that Defendant now makes regarding *Replay TV*, holding that "because the Server Log Data already exists, is temporarily stored in

[2] *See also Usenet*, 608 F. Supp. 2d at 432 (rejecting defendants' argument that they did not have to preserve and produce "transient electronic data" on their servers); *cf. MAI Sys. Corp. v. Peak Comput., Inc.*, 991 F.2d 511, 518–19 (9th Cir. 1993) (rejecting a defendant's argument that a copy in a computer's RAM is not a copyright violation because it is not sufficiently "fixed" and holding that a copy in RAM can be "perceived, reproduced, or otherwise communicated"); *Stenograph LLC v. Bossard Assocs., Inc.*, 144 F.3d 96, 101–02 (D.C. Cir. 1998) (same).

RAM, and is controlled by defendants, an order requiring defendants to preserve and produce such data is not tantamount to ordering the creation of new data." *Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *6 (C.D. Cal. May 29, 2007).[3]

Defendant's other cases are also of no moment. They are factually inapposite, and none involves a motion to preserve evidence or otherwise precludes production of "ephemeral" data. *See*, *e.g.*, *Louis Vuitton Malletier v. Dooney & Bourke, Inc.*, No. 04 Civ. 5316 RMB MHD, 2006 WL 3851151, at *2 (S.D.N.Y. Dec. 22, 2006) (denying sanctions motion regarding communications in customer relations chat room, where chat room opened after the infringement ceased, it was speculation that the chats had relevant information, and there was not a ready means for retaining the communications); *Convolve, Inc. v. Compaq Comput. Corp.*, 223 F.R.D. 162, 176–77 (S.D.N.Y. 2004) (denying request for sanctions for not preserving data reflecting adjustments by a tuning engineer to a device, including because preservation apparently presented an undue burden, in the form of "heroic efforts"); *Williams v. UnitedHealth Grp.*, No. 2:18-cv-2096, 2020 WL 528604, at *2 (D. Kan. Feb. 3, 2020) (denying a discovery motion regarding instant messages, without addressing the scope of preservation obligations); *King v. Catholic Health Initiatives*, No. 8:18CV326, 2019 WL 6699705, at *4–5 (D. Neb. Dec. 9, 2019) (requiring defendants to supplement their production with emails, not additional instant messages beyond that already produced, in response to request for sanctions); *Butler v. Portland Gen. Elec. Co.*, No. 88-455-FR, 1990 WL 15680, at *1–2 (D. Or. Feb. 9, 1990) (denying motion to compel asking for names and positions held by employees whose wages were included in public filings

[3] Notably, the court in *Replay TV* issued its decision in 2002, well before the 2006 amendments to the Federal Rules of Civil Procedure that explicitly incorporated provisions concerning ESI. Unlike the court in *Bunnell*, the *Replay TV* court did not have the benefit of these new provisions or the advisory committee's accompanying guidance.

where the information had not been compiled and to do so would require creating a new computer program).[4]

Defendant's arguments about the "ramifications" of the Order are misguided. (Obj. Mem. at 2, 16.) This is not the right forum for Defendant to protest the enactment of Rule 34 regarding ESI or the Advisory Committee's guidance. The Order concerns the factual circumstances presently before the Court. Defendant's comparison of the Order to a requiring a defendant to start recording every Zoom, or any other digital, call is inapt. The Order does not require Defendant to preserve and produce the stream-ripped audio files themselves. The Order requires Defendant to preserve and produce data that identifies the stream-ripping transactions.

C. Defendant's Privacy Argument Also Fails

Magistrate Judge Buchanan correctly rejected Defendant's argument that foreign data privacy laws preclude the Court from requiring him to produce data concerning stream-ripping transactions where the users are located outside the United States. (Hr'g Tr. 25:21–25.)

As Plaintiffs explained in their briefing, Defendant has not established that producing the requested data requires him to violate privacy laws or put users of his websites at risk. (Pls.' Reply at 4–5.) In fact, he has not raised any credible arguments toward that end. A party relying on foreign law has the burden of showing that foreign law bars the discovery at issue. *United States v. Vetco*, 691 F.2d 1281, 1289 (9th Cir. 1981). Defendant has failed to make that showing. For this reason alone, Defendant's privacy arguments should be rejected.

---

[4] Finally, Defendant cites *Tener v. Cremer*, 89 A.D. 3d 75, 80–81 (N.Y. App. Div. 2011). But that case recognizes that ESI *includes* data such as that in RAM and other ephemeral data. While discovery of RAM data or ephemeral data generally may not be at issue in most cases, the situation before the Court is different. Here, the requested server data is very relevant, and preservation and production of the data do not present an undue burden.

Defendant's privacy arguments fail for several additional reasons. First, the Privacy Policy for Defendant's Websites informs users that the server data at issue may be collected and disclosed.[5] When users affirmatively opt into the click-through agreement before each "convert" request, they assent to Defendant's Terms of Use and its incorporated Privacy Policy.[6] Thus, users have given their consent to collection and disclosure of the data, and they should not expect that their activity on Defendant's Websites is not logged or disclosed. These facts refute Defendant's claim and gave the Court comfort that Defendant's privacy argument was not credible. (Hr'g Tr. 25:21–25.)

Second, Defendant hypothesizes that, if he is required to preserve server data logs, those logs could expose "dissident material" to the Russian government. (Obj. Mem. at 5–6, 18–19.) But this argument is based on nothing more than pure speculation. Defendant offers no basis in

---

[5] "Using the Service. When you access the Service, use the search function, convert files or download files, your IP address, country of origin and other non-personal information about your computer or device (such as web requests, browser type, browser language, referring URL, operating system and date and time of requests) *may be recorded for log file information*, aggregated traffic information and in the event that there is any misappropriation of information and/or content. Usage Information. *We may record information about your usage of the Service such as your search terms, the content you access and download and other statistics*. . . . Disclosure of Information[.] *We may be required to release certain data to comply with legal obligations* or in order to enforce our Terms of Use and other agreements. We may also release certain data to protect the rights, property or safety of us, our users and others. This includes providing information to other companies or organizations like the police or governmental authorities for the purposes of protection against or prosecution of any illegal activity, whether or not it is identified in the Terms of Use." FLVTO.biz, "Privacy Policy," https://www.flvto.biz/en95/policy/ (last visited June 23, 2021); *see also* 2conv.com, "Privacy Policy," https://2conv.com/en80/policy/ (last visited June 23, 2021) (same) (emphasis added).

[6] To convert a file, a user must check a box agreeing that "[b]y using our service you are accepting our Terms of Use." FLVTO.biz, "FLVTO," https://www.flvto.biz/en96/ (last visited June 24, 2021); *see also* 2conv.com, "2conv," https://2conv.com/en81/ (last visited June 24, 2021) (same). The Terms of Use provide in relevant part: "We retain a separate Privacy Policy and your assent to these Terms also signifies your assent to the Privacy Policy." FLVTO.biz, "Terms of Use," https://www.flvto.biz/en96/terms/ (last visited June 24, 2021); 2conv.com, "Terms of Use," https://2conv.com/en81/terms/ (last visited June 24, 2021) (same).

fact to believe that his stream-ripping sites are used for purposes of political dissent. Defendant's speculation is not a substitute for facts.

Third, any privacy concerns can be further mooted by Defendant's redacting the specific IP addresses (or replacing them with unique but anonymous identifiers), while still providing server data identifying: the YouTube videos that are stream-ripped; the MP3 files that are copied and distributed; and the geographic locations of the users that downloaded the audio files. Defendant's only purported privacy concern relates to IP addresses; redactions, combined with identification of the user's geographical location, can readily address that concern.

Finally, Defendant's privacy arguments fall flat for another compelling reason. Apart from any local logging using his web server software, Defendant already is engaged in remote logging with a third-party service Yandex Metrica. Defendant has integrated Yandex into the program code of his websites, capturing and storing data concerning various events, including each "convert" request and each "MP3 download" request. (Pls.' Mem. at 8; Schumann Decl. ¶¶ 16–18). Thus, Defendant's alleged privacy concerns are pretextual.

CONCLUSION

The server data is highly 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 users use his Sites for non-infringing uses. Defendant refuses to produce the data only because he knows that it is highly incriminating. For the reasons discussed above, Magistrate Judge Buchanan's Order is fully supported by the law and the undisputed facts in the record. Plaintiffs respectfully request that the Court affirm the Order.

Respectfully submitted,

Dated July 7, 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 20016
Tel: (202) 480-2999
Fax: (866) 766-1678
scott@oandzlaw.com
matt@oandzlaw.com
lucy@oandzlaw.com
kellyn@oandzlaw.com

Attorneys for Plaintiffs