UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

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

DEFENDANT'S MEMORANDUM IN SUPPORT OF OBJECTIONS TO MAGISTRATE JUDGE'S JUNE 25, 2021 ORDER REQUIRING THE CREATION OF MATERIALS FOR PRODUCTION IN DISCOVERY

Pursuant to Fed. R. Civ. P. 72(a), Defendant Tofig Kurbanov ("Mr. Kurbanov") submits his objections to the Magistrate Judge's June 25, 2021 Order granting Plaintiffs' Motion to Compel the Preservation and Production of Web Server Data ("Plaintiffs' Motion"). In support thereof, Mr. Kurbanov states as follows.

Introduction

On June 25, 2021, Magistrate Judge Theresa Carroll Buchanan entered an Order granting Plaintiffs' Motion to Compel the Preservation and Production of Web Server Data requiring the creation and production of materials that do not "exist" and that have never been "stored" as is required for such materials to come within the ambit of Fed. R. Civ. P. 34. Attached hereto as **Exhibit 1** is the Magistrate's Order and attached hereto as **Exhibit 2** is the transcript from the June 25, 2021 hearing before Magistrate Buchanan.

Instead, if the Magistrate's Order is allowed to stand, Mr. Kurbanov, a Russian citizen who manages two websites entirely and exclusively from Russia, will be required to alter the operation of the websites' servers (which are located in Germany) in order to *create* records that he has never before created, maintained, or stored. This is ***not*** a situation in which the Defendant

has deleted electronically stored information – like emails that are routinely stored on a server – after being put on notice of likely litigation, but rather this is a case where the Magistrate's order would require Mr. Kurbanov to alter the manner in which he has operated his servers in order to capture – for the first time and for the sole purpose of creating data for discovery – what is commonly referred to as "ephemeral data." It is important to consider for a moment the ramifications of this Order: as an example, almost all modern telephone calls are transmitted digitally, whether via voice over internet protocol (VOIP) technology or simple digital fiber optic lines. And, just like ephemeral server data, such phone calls create, for a short period of time, computer data that could *theoretically* be stored. Indeed, many VOIP providers offer an option to record calls made or received over VOIP. Nevertheless, a litigant is not required to record all of his or her incoming and outgoing phone calls – where they have never done so before – simply to create for discovery purposes that which is not otherwise "stored." And yet, that is what the effect of the Magistrate's Order will be as it effectively reads the word "stored" out of "electronically stored information" and instead requires the *creation* of stored materials that do not otherwise exist.

Indeed, there is no question but that the Magistrate understood (following argument from counsel) and her order required the creation of new materials that would not otherwise exist. As the Magistrate stated from the bench in allowing Plaintiffs' Motion:

> And it's, yes, creating information, storing information that otherwise would not be stored, but that's essentially what I'm telling the defendant to do here is to turn off or to turn on, rather than turning off auto-delete, they're turning on the preservation of this data in long-term storage rather than our RAM.

Transcript, p. 24.

Additionally, even if there were a legal basis to require the Defendant to create new materials for the purposes of discovery – which clearly there is not – there would certainly be no

justification for an order as broad as allowed by the magistrate: although more than 90% of each of the websites' visitors come from outside the United States (and whose use of the websites is, accordingly, outside of this Court's jurisdiction),[1] the Plaintiffs' requests (which the magistrate allowed) were not limited to data about United States users of the websites, but rather all users globally. In so ordering, the Magistrate ignored concerns about the data privacy laws of the other countries where more than 90% of the websites visitors reside.

But, at its most basic, the Federal Rules of Civil Procedure do not require a party to create data that does not already exist; the server data that the Magistrate has ordered produced has never been stored and, as such, does not "exist," and for that reason alone, the Magistrate's order was contrary to law and should be set aside.

RELEVANT FACTS

Mr. Kurbanov operates the websites flvto.biz and 2conv.com (the "Websites") from his home town of Rostov-on-Don, Russia. Declaration of Tofig Kurbanov, ¶2. The Websites allow visitors to save the audio tracks from online videos to their computers without necessarily saving

[1] *See*, *e.g.*, *Tire Eng'g & Distribution, Ltd. Liab. Co. v. Shandong Linglong Rubber Co.*, 682 F.3d 292, 306 (4th Cir. 2012) ("As a general matter, the Copyright Act is considered to have no extraterritorial reach."); *Nintendo of Am., Inc. v. Aeropower Co.*, 34 F.3d 246, 249 n.5 (4th Cir. 1994) ("[T]he Copyright Act is generally considered to have no extraterritorial application."). *See*, *also*, *Palmer v. Braun*, 376 F.3d 1254, 1258 (11th Cir. 2004) ("Federal copyright law has no extraterritorial effect, and cannot be invoked to secure relief for acts of infringement occurring outside the United States.... Thus, it is only where an infringing act occurs in the United States that the infringement is actionable under the federal Copyright Act, giving the federal courts jurisdiction over the action." (citing *Subafilms, Ltd. v. MGM-Pathe Communications*, 24 F.3d 1088, 1091 (9th Cir. 1994) (en banc))); *Foreign Imported Prods. & Publ., Inc. v. Grupo Indus. Hotelero, S.A.*, 2008 U.S. Dist. LEXIS 108705 (S.D. Fla. Oct. 24, 2008) ("Federal copyright law has no extraterritorial effect, and therefore it is only where an infringing act occurs in the United States that the infringement is actionable under the federal Copyright Act, giving the federal courts jurisdiction over the action.... Stated another way, district courts do not have subject matter jurisdiction over infringing acts that took place 'wholly outside' the United States or 'entirely overseas.'").

the video content as well. The functionality of the Websites is content neutral, and there are substantial non-infringing reasons why users would utilize the Websites. *Id.*, ¶3.

The Websites are currently hosted with a company called Hetzner Online GmbH (hetzner.com). It is Mr. Kurbanov's understanding that Hetzner is a company organized and based in Germany, and that the servers hosting the Websites are physically located in Germany. *Id.*, ¶4.

Only a small minority of the Websites' traffic comes from the United States. During the time period of October 1, 2017, through September 30, 2018, only 5.87% of the users of the 2conv.com Website were from the United States, and only 9.92% of the users from the flvto.biz Website were from the United States. *Id.*, ¶5 and prior Kurbanov Declaration dated October 1, 2018 and filed with this Court as Docket No. 25-1 ¶¶ 38-39.

The web server that hosts the Websites does not maintain logs of server activity such as an access log which saves the time, date, and IP address of each request made to the Websites (the "Access Logs"). *Id.* ¶6. Mr. Kurbanov has not configured the server to create and save Access Logs, in part because doing so would require the use of significant hard drive space to store this information, which is an expense that he does not wish to incur. *Id.* It is also his understanding and belief that saving such Access Logs would cause the Websites to run more slowly. *Id.* Mr. Kurbanov has not, at any time since starting the Websites, created or stored Access Logs. *Id.*

The custom-made Website interface software does not store the URLs of the videos that users enter into the Websites to convert them to audio files. In order for the Website software to store each URL information entered into the Websites by users for conversion, Mr. Kurbanov would have to have to program the Websites' software to store this information, which would

involve significant costs. *Id.*, ¶7. Moreover, Mr. Kurbanov would also incur additional expenses in respect to storing this newly recorded information. *Id.*, ¶8. Mr. Kurbanov estimates that, if the Websites saved every URL that users entered into the Websites it would take up approximately 92.5 gigabytes of storage space each day which translates to about 2.7 terabytes of storage each month. This would result in thousands of dollars a year in storage charges. For example, according to Amazon Web Services ("AWS") server charges, AWS would charge about $4,500 for the first year of storage at this rate. As the storage would continue accumulating, the storage charges would increase by $4,500 each year (to about $9,000 for the second year and $13,500 for the third year, *etc*.) assuming that usage rates of the Websites remained constant. *Id.* It is also Mr. Kurbanov's understanding and belief that saving such URL information would cause the Websites to run more slowly. *Id.*, ¶9. Mr. Kurbanov has not, at any time since starting the Websites, created or stored this URL information. *Id.*

Mr. Kurbanov also values the privacy of the Websites users and believes that keeping and storing Access Logs or storing the records of the URLs that were converted could jeopardize the privacy of the Websites users. *Id.*, ¶12. Storing such information – or providing it to third-parties such as the Plaintiffs could create a host of legal concerns and liabilities in the 200+ countries where the Websites are accessed (each of which has its own data privacy laws). *Id.*

It is Mr. Kurbanov's understanding that since the Websites are operated from Russia, the Russian authorities might have the right to seize and inspect the Websites' business records, which would include Access Logs and/or URL records if the Websites were to maintain them. *Id.*, ¶13. Mr. Kurbanov reasonably fears that if any of the Websites' users were to have downloaded what Russia considers to be dissident material, or material that the Russian

government otherwise finds objectionable, that the Russian government could locate a Website user and possibly subject that user to an unfavorable and unfair criminal or civil proceeding. *Id.*

Similarly, although the Websites retain the *right* to log information such as IP addresses they do not actually do so in part because doing so might violate the various data privacy laws of countries from which the users access the Websites. *Id.*, ¶14. For example, the websites servers are located in Germany. It is Mr. Kurbanov's understanding that, under German law, a user's IP address is generally considered personal information which cannot be shared without the user's permission and, even then, only if the user has specifically consented to the specific disclosures. *Id.* Although does not have personal knowledge of all of the privacy laws in the countries from which his users come, he assumes that each of the other 200+ countries from which the Websites are accessed have their own rules about how such data is to be handled *if it is stored and maintained. Id.* Trying to comply with the laws of each of those countries would be unrealistic, which is another reason why Mr. Kurbanov does not store such data. *Id.*

Finally, Mr. Kurbanov believes that, if users knew that information about their requests and usage of the Websites was logged and saved, and could possibly be accessed by governments, it could discourage users from using the Websites and decrease the popularity and profitability of the Websites. *Id.*, ¶15.

THE REQUESTS AT ISSUE

In their Motion, Plaintiffs sought to compel Mr. Kurbanov to create, preserve, and produce two kinds of ephemeral server data concerning the websites' global users, which he has never previously created or stored: (a) logs of the IP addresses and locations of visitors to the websites (which constitutes personally identifiable information under many countries' privacy laws since IP addresses can be used to identify individual users); and (b) logs of URL addresses

entered by the website's users in to the websites' "convert" bar. Specifically, Plaintiffs asked the Court to compel the production of documents in response to requests Nos. 2, 5-7, 9, 12, 30, and 31, which the Magistrate did in a one-line order. Those requests and Defendants' Objections and Responses are set out in the footnote, below[2]

---

[2] **REQUEST 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.
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.

REQUEST 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.
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.

REQUEST 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.
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.

REQUEST 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.
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.

REQUEST 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.
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.

REQUEST 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.
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.

ARGUMENT

I. The Magistrate's Order Was Legal Error Inasmuch As The Rules of Civil Procedure Do Not Require a Party to *Create* Documents for Discovery, Even If The Party Has the Ability to Do So.

While Rule 34 of the Federal Rules of Civil Procedure generally require a party to produce relevant "items in the responding party's possession, custody, or control," by its very terms it limits those items to "documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained…." Fed. R. Civ. P. 34. Courts have routinely held that this production requirement does not extend to the *creation* of documents which do not otherwise exist. *See, e.g., Alexander v. FBI*, 194 F.R.D. 305, 310 (D.D.C. 2000)("Rule 34 only requires a party to produce documents that are already in existence. …A party is not required 'to prepare, or cause to be prepared,' new documents solely

---

REQUEST NO. 30:
All documents concerning the use of location-specific advertising to Users in the United States in connection with Defendant's Websites.
OBJECTION: Defendant objects to this Discovery Request as overbroad and unduly burdensome. Defendant objects inasmuch as this request is not reasonably calculated to lead to the discovery of admissible information. 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. Subject to these objections, Defendant responds as follows.
RESPONSE: Defendant has no responsive documents or things in his care, custody, or control.

REQUEST 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.
OBJECTION: Defendant objects to this Discovery Request as overbroad and unduly burdensome. Defendant objects inasmuch as this request is not reasonably calculated to lead to the discovery of admissible information. 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. Subject to these objections, Defendant responds as follows.
RESPONSE: Defendant has no responsive documents or things in his care, custody, or control.

for their production"); *Rockwell Int'l Corp. v. H. Wolfe Iron & Metal Co.*, 576 F. Supp. 511, 513 (W.D. Pa. 1983)(defendant could not be required to produce a new handwriting exemplar for plaintiff: "a defendant in this civil action, cannot be compelled to create, upon the request of the plaintiff, documentary evidence which is not already in existence in some form. Rule 34 cannot be used to require the adverse party to prepare, or cause to be prepared, a writing to be produced for inspection, but can be used only to require the production of things in existence"); *Gaustad v. Frank*, 2006 U.S. Dist. LEXIS 106877, at *2-4 (E.D. Wis. Mar. 1, 2006)(defendant could not be required to take photographs for plaintiff's use because "Rule 34 only requires a party to produce documents that are already in existence …A party is not required 'to prepare, or cause to be prepared,' new documents solely for their production"); *Soetaert v. Kan. City Coca Cola Bottling Co.*, 16 F.R.D. 1, 2-3 (W.D. Mo. 1954)("Rule 34 cannot be used to require the adverse party to prepare, or cause to be prepared, a writing to be produced for inspection, but can be used only to require the production of things in existence"); *Lamon v. Adams*, 2015 U.S. Dist. LEXIS 53017, at *6 (E.D. Cal. Apr. 22, 2015)("In requiring the production of documents and other tangible things in the responding party's possession, custody, or control, Federal Rule of Civil Procedure 34(a)(1) contemplates only the production of existing items since something that does not exist cannot be possessed, held, or controlled. Rule 34 cannot be used to require the adverse party to prepare, or cause to be prepared, a writing to be produced for inspection, but it can only be used to require the production of things in existence"); *Butler v. Portland Gen. Elec. Co.*, 1990 U.S. Dist. LEXIS 1630, at *2-4 (D. Or. Feb. 9, 1990)("A document is not in the possession, custody or control of a party if it does not exist, and production cannot be required of a document which is not yet in existence"); *Rapalo v. Lopez*, 2014 U.S. Dist. LEXIS 157979, at *7-8 (E.D. Cal. Nov. 7, 2014)("Defendants are not obligated to create in response to a document request. Rule 34

requires parties to produce documents that already exist, but it does not require parties to create new data. …Here, there is no indication that the information already exists in a readily accessible form. Instead, it would require CDCR to compile data by reviewing medical records of individual inmates.")

Despite the longstanding precedent that a party cannot be required to *create* materials for the purpose of discovery, the Magistrate acknowledged that this was precisely what she was ordering be done:

> And it's, yes, creating information, storing information that otherwise would not be stored, but that's essentially what I'm telling the defendant to do here is to turn off or to turn on, rather than turning off auto-delete, they're turning on the preservation of this data in long-term storage rather than our RAM.

Transcript, p. 24.

Recognizing that the Magistrate was specifically ordering the *creation* of materials that would not otherwise exist and that such an order was contrary to the law, Plaintiffs attempted to walk-back the Magistrate's own words, so as to rephrase her order to pretend that the order did not do precisely that which the Magistrate acknowledged it did. *See* Transcript, pp. 26-27.

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). As such, and because Rule 34 does not require the creation of new information for the purpose of discovery, the Magistrate's order requiring the creation and storage of data is legal error and must be set aside.

II. The Magistrate's Order Requiring Mr. Kurbanov to Alter His Long-Standing Server Configuration and Change the Functionality of His Websites Simply to Create Information for Plaintiffs Constitutes Legal Error and Must be Set Aside.

As discussed above, the Magistrate's order will require Mr. Kurbanov to create, preserve, and produce two kinds of ephemeral server data concerning the websites' global users, which he

has never previously stored: (a) logs of the IP addresses and locations of visitors to the websites (which constitutes personally identifiable information under many countries' privacy laws since IP addresses can be used to identify individual users); and (b) logs of URL addresses entered by the website's users in to the websites' "convert" bar. To be clear, Mr. Kurbanov does not store – and has never stored – any of this data.

As a starting point, it is important to recognize a crucial flaw in the Magistrate's reasoning. Throughout the hearing (and at Plaintiffs' urging), the Magistrate analogized this case with the more typical situation in which a litigant is required to suspend its normal "document destruction" protocols so as to preserve existing documents for the purposes of discovery. The two are simply not the same. Organizations often have policies by which they regularly purge information that they otherwise store after a set period of time: for example, an organization might dispose of personnel records a number of years after an employee departs a company. Despite such protocols, businesses are generally required to suspend routine *destruction of stored information* to comply with discovery obligations once it becomes reasonably clear that the stored documents are relevant to specific litigation. This is not what the Magistrate's Order does here. Instead, the Magistrate's order requires Mr. Kurbanov to alter the operation of his servers (located in Germany) to *create and store permanent computer files* that were never previously created or stored. While it is true that, for a brief duration of time, the data with which such files could be created does exist (just as the electronic data that makes up a Zoom call exists as it is occurring), most courts and commentators have found that Rule 34 does not reach such ephemeral electronic data, nor can a party be required to start saving such data for discovery *if they had not done so in the past*.

For example, in *Paramount Pictures Corp. v. Replay TV*, 2002 U.S. Dist. LEXIS 28126 (May 30, 2002), the Court faced a similar set of allegations. There, the plaintiff, a collection of movie studios and content producers, alleged, *inter alia*, that the defendant violated their copyrights by creating and distributing a device that allowed users to digitally record television shows (much like TIVO), skip the advertisement in those shows, and send perfect digital copies to others. *See* Paramount Amended Complaint, attached as **Exhibit 3**. In the course of discovery, Plaintiffs sought and obtained from the magistrate an order from the Court requiring the Defendant to preserve data concerning what shows users were recording, as well as what other uses they were making of the shows, such as whether they were sending the shows to others, information that Paramount contended the Defendant already had access to because it was stored on the users' set-top boxes, which were always connected to Defendant's servers. *See* Paramount's Supplemental Memorandum, attached as **Exhibit 4**.

Despite the fact that the information "existed" inasmuch as it was stored at least temporarily on the users' set-top hard drives *which were at all times connected to the Defendants' own servers* and thus available to the Defendants with a click of a button, the Defendant did not collect or store the information at the time of the litigation although (unlike Mr. Kurbanov in this case), it had, at one time, done so. Nevertheless, in reversing the Magistrate's discovery order, the Court held:

> Defendants and amici[3] raise numerous objections to this Order. Generally, they contend that the order requires not that they produce material in discovery but that they create new data; that the order is, therefore, not a discovery order but an impermissible mandatory injunction; that the burdens on defendants and their customers outweigh any benefit to the plaintiffs, and that the order constitutes a serious and unnecessary invasion of ReplayTV4000 users' privacy rights.

[3] The *amici* in the *Paramount* case discussed in detail the privacy concerns of the users of the defendants' recording device (which, like here, could be used for both legal uses or infringing uses). A copy of the amicus brief from *Paramount* is attached hereto as **Exhibit 5.**

> Although each of the issues raises serious questions, which have been very well briefed on all sides, the Court is persuaded to reverse the Magistrate Judge's Order on the grounds that it impermissibly requires defendants to create new data which does not now exist. A party cannot be compelled to create, or cause to be created, new documents solely for their production. Federal Rule of Civil Procedure Rule 34 requires only that a party produce documents that are already in existence. *Alexander v. FBI* (D.D.C. 2000) 194 F.R.D. 305, 310.
>
> …In order to gather information from customers about "what works are copied, stored, viewed with commercials omitted, or distributed to third parties with the ReplayTV4000 [and] when each of those events took place," defendants would be required to undertake a major software development effort, incur substantial expense, and spend approximately four months doing so.
>
> It is evident to the Court, based on Pignon's declaration, that the information sought by plaintiffs is not now and never has been in existence. The Order requiring its production is, therefore, contrary to law.

Paramount Pictures Corp. v. Replay TV, 2002 U.S. Dist. LEXIS 28126, at *8-10 (C.D. Cal. May 30, 2002).

Other courts have similarly held that where electronic data was ephemeral or would otherwise require a litigant to undertake steps to create stored versions of the data that the party had not previously created, that the party could not be compelled to do so. *See, e.g., Louis Vuitton Malletier v. Dooney & Bourke, Inc.*, 2006 U.S. Dist. LEXIS 96796, at *7-8 (S.D.N.Y. Dec. 22, 2006)(refusing to sanction defendant for failing to institute procedure to log chat room transcripts, holding that "This set of circumstances is a far cry from the sort of failure to retain and search for e-mails that has recently been the subject of much judicial scrutiny and the issuance of a new provision in the federal rules of civil procedure governing e-discovery. Indeed, it is more akin to a demand that a party to a litigation install a system to monitor and record phone calls coming in to its office on the hypothesis that some of them may contain relevant information. There is no such requirement, and in this case no indication that defendant acted improperly in this regard"); *Convolve, Inc. v. Compaq Comput. Corp.*, 223 F.R.D. 162, 176-77

(S.D.N.Y. 2004)(holding that a defendant in intellectual property case was not required to screen-print or save ephemeral data that it would not otherwise save, deeming such efforts to be "heroic efforts far beyond those consistent with Seagate's regular course of business. To be sure, as part of a litigation hold, a company may be required to cease deleting e-mails, and so disrupt its normal document destruction protocol. But e-mails, at least, normally have some semi-permanent existence. They are transmitted to others, stored in files, and are recoverable as active data until deleted, either deliberately or as a consequence of automatic purging. By contrast, the data at issue here are ephemeral. They exist only until the tuning engineer makes the next adjustment, and then the document changes. No business purpose ever dictated that they be retained, even briefly"); *Williams v. Unitedhealth Grp.*, 2020 U.S. Dist. LEXIS 16906 (D. Kan. Feb. 3, 2020)(finding that defendant did not violate preservation or production obligations by configuring its Cisco Jabber instant messaging system to not retain instant messages); *King v. Catholic Health Initiatives*, 2019 U.S. Dist. LEXIS 211360, at *15-16 (D. Neb. Dec. 9, 2019)(holding that defendant did not have a preservation or production obligation relating to instant messages generated by Microsoft Lync instant messaging system that was configured not to retain instant messages); *Tener v. Cremer*, 89 A.D.3d 75, 80-81 (App. Div. 1st Dept., 2011)("some federal courts have suggested strict limits on the discovery of specific types of data that are typically overwritten or ephemeral. For example, the Seventh Circuit Electronic Discovery Pilot Program has adopted several 'principles' to guide litigants through the discovery of ESI. In particular, principle 2.04 governing the scope of preservation states that certain categories of ESI 'generally are not discoverable in most cases.' …These categories include: …(2) random access memory (RAM) or other ephemeral data…(6) other forms of ESI whose preservation requires extraordinary affirmative measures that are not utilized in the ordinary

course of business"); *Butler v. Portland Gen. Elec. Co.*, 1990 U.S. Dist. LEXIS 1630, at *2-4 (D. Or. Feb. 9, 1990)(denying motion to compel based on defendant's representation that it would have to "create a new computer program in order to produce further information responsive to Request No. 3," holding "As the law does not require a party to prepare or create a document in response to a discovery request, the motion to compel is denied as to Request No. 3.")

Although the Magistrate recognized the difference between ordering a party to suspend a routine practice of destroying data *that already existed and was stored in file that would continue to exist absent the party's destruction policies* and ordering a party to *start creating permanent data logs that would not otherwise exist and which the party had never before created*, she dismissed such a difference as immaterial. It is not. It is precisely the place at which the law draws the line. Obliteration of that line will have consequences not only in this case, but in every case where a litigant ***could*** create materials for discovery purposes if ordered by a court. If the Magistrate's Order were to stand, there is no practical reason why future litigants can't be ordered to start recording every digital phone call or Zoom call.

Indeed, since the rules concerning ESI are only supposed to put electronic information on the same footing as non-electronic information, why stop there? Surely, every (relevant) conversation that a party has is temporarily "stored" in that person's "RAM" (i.e., memory). Why not, then, a "preservation" order that requires a party to immediately transcribe such conversations into a more permanent form so that such transcriptions can be available for production in discovery? By the same reasoning, such an order would not be "creating" new data, simply requiring a party to preserve such data in a more permanent fashion. And, although such an order seems far-fetched, so too does the order entered here which requires a party to create permanent files that he never previously created.

In their motion, however, Plaintiffs cited *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443 (C.D. Cal. 2007), a case in which a district court found that it appropriate to order a defendant to preserve server data stored temporarily in a computer's RAM for production in discovery. The *Columbia Pictures* decision has been described by some commentators as "controversial" and "dangerous." *See* **Exhibits 6 and 7, respectively.** In a subsequent amicus brief, the Electronic Frontier Foundation, the Center for Democracy & Technology, and Public Knowledge explained the dangers of the *Columbia Pictures* decision this way:

> At least before the Server Log Data Order issued, no litigant would assume that erasing a whiteboard might violate a duty of preservation. Similarly, no court would ask a litigant to record all telephone calls, to videotape all staff meetings, or to outfit every potential witness with a GPS tracking device in order to create a record of their locations at every moment. To be sure, objections based on burden, privacy, and attenuated relevance could be raised in those hypothetical situations. But the more basic point is that discovery simply does not reach such ephemera, even if highly relevant and easily collected (snapping photos of whiteboards is simple; many digital telephone systems can readily be configured to record calls; inexpensive video cameras now have massive storage capabilities; free programs allow one to track location via GPS features built into many modern cell phones). Yet that type of discovery is precisely what the Server Log Data Order contemplates, solely because the electronic equivalent of such ephemeral communications will necessarily involve the creation of a temporary snapshot that could, in theory, be preserved.
>
> … If RAM is ESI, then it follows that an accident of technological fate can have drastic and unexpected results on the scope of discovery in a case. For example, calls made over digital business phone systems, which are commonplace today, or via Voice over Internet Protocol ("VoIP") technology, a method of routing voice signals over the Internet, necessarily pass temporarily through RAM and could be retained through the use of simple software designed to log them. Under the reasoning of the Server Log Data Order, every call made on a digital phone system must be recorded by a party subject to a "litigation hold," while calls made using analog phone systems need not. Similarly, a security system using digital video cameras would create voluminous quantities of ESI, while an analog system would not. Surely a decision about the technology used to implement these sorts of systems should not have these effects. *See FED. R. CIV. P.* 34(a) advisory committee's note (discovery of electronically stored information should "stand[] on equal footing" with traditional discovery).

Exhibit 8, pp. 8-9; 15.

In short, *Columbia Pictures* stands as a "controversial" and "dangerous" outlier case which this Court is not bound by and which it should not follow here. Indeed, as the Electronic Frontier Foundation, the Center for Democracy & Technology point out, Orders such as the one at issue here are a genie that cannot be put back into the bottle once they are let out.

III. The Magistrate's Order Requires Mr. Kurbanov to Choose Between Compliance With the Court's Order, On The One Hand, And Compliance With The Laws of the Countries in Which the Websites Are Accessed, On The Other.

Finally, as noted above, the Magistrate's order requiring Mr. Kurbanov to preserve and produce the data requested by Plaintiffs presents Mr. Kurbanov with a Hobson's choice: he can either comply this Court's order, which would require him to violate the laws of other countries and/or put the Websites' users at risk or he can defy the Magistrate's order and risk a finding of contempt. It is not a position that this Court should force upon a foreign individual who has to contend with the ramifications of such data collection in other countries.

For example, the Websites are operated out of Russia, with servers located in Germany. As Mr. Kurbanov explains in his accompanying declaration, one fear that he has is that, if he were to store and retain the information sought by the Plaintiffs, "the Russian authorities might have the right to seize and inspect the Websites' business records, which would include Access Logs, URL records, and/or audio files, if the Websites were to maintain them. I fear that if any of the Websites' users were to have downloaded what Russia considers to be dissident material, or material that the Russian government otherwise finds objectionable, that the Russian government could locate a Website user and possibly subject that user to an unfavorable and unfair criminal or civil proceeding." Kurbanov Decl., ¶13. This fear is well-justified as, in July of 2018, Russia enacted new laws relating to internet data that could indeed require Mr. Kurbanov to provide Russian authorities with stored data concerning Russian individuals,

particularly those that might be identifiable by IP address. *See* "Yarovaya Law and new data storage requirements for online data distributors," attached hereto as **Exhibit 9.**

Similarly, if Mr. Kurbanov were to comply with the Magistrate's order, he would likely violate the laws of Germany, where the Websites' servers are located. *See*, *e.g.*, "Online Privacy Law: Germany," Library of Congress, attached hereto as **Exhibit 10,** pp. 1, 3 ("Germany generally prohibits the collection and use of personal data unless the law specifically permits this or the data subject has given his or her informed consent. German law also follows the Directives on issues relating to rights and remedies of data subjects, security requirements, restrictions on location data, minimization of data, and safeguards against transmitting personal data to third countries with lesser standards of protection. … There has been much discussion of whether IP addresses are personal data, and the majority opinion considers them to be always personal data when they are fixed IP addresses that identify a specific computer. If they are movable IP addresses that are assigned by the access provider every time the user logs in, then they are personal data only if the service provider has enough information to actually identify the user, which will usually be the case.").

At the hearing, the Magistrate put aside Russian and German privacy concerns stating that she believed that such concerns were "waived" by the site's users because of the websites' terms of use, which permit the websites to collect information and because Mr. Kurbanov would be acting pursuant to an Order of this Court. Transcript, pp. 15, 25. The concerns cannot, however, be so easily brushed aside. First, with respect to the Russian data collection laws, the websites' Terms of Service were written before Russia enacted its new data protection laws. More to the point, although the Terms of Service may *permit* the Websites to collect such data, it has not in reality done so. And, although it ***may*** be true that the Terms of Service protect the

Websites from legal liability, that would be cold comfort if the Russian government were to use the collected data to target individuals in Russia who have used the Websites. The Magistrate's Order also gave short shrift to the incredibly-stringent German privacy laws described by the Library of Congress in Exhibit 10. According to the Library of Congress, although German law does allow users to consent to the use of their data (including their IP address):

> Consent may be given electronically, provided the data controller ensures that the user of the service declares his consent knowingly and unambiguously, the consent is being recorded, the user may view his consent declaration at any time, and the user may revoke consent at any time with effect for the future.

In addition, it is clear that German Law treats the transmittal of data to a non-EU country such as the United States (which does not have as stringent data protection laws) differently than transmittal of data within the EU:

> On the transmittal of data to other countries, Germany also differentiates between recipient countries that are EU or EEA members and third countries. Transfers to the latter generally require assurances that the third country has an EU-compatible standard of data privacy.

In short, the Terms of Service may not actually provide the Websites with protection in connection with the preservation and production of data as contemplated by the Magistrate's Order.

Similarly, the 200+ other countries which make up more than 90% of the website's users will each have their own data privacy laws which could be implicated by the Magistrate's Order. Mr. Kurbanov should not be put in the position of violating the laws of untold numbers of countries (or the rights of users from those countries) by virtue of an order in a civil case in a country to makes up less than 10% of the traffic to the Websites.

Conclusion

For the reasons stated hereinabove, the Magistrate's Order of June 25, 2021 should be set aside.

Dated: July 2, 2021

Respectfully Submitted:

/s/ Jeffrey H. Geiger
Jeffrey H. Geiger (VSB No. 40163)
SANDS ANDERSON PC
1111 E. Main Street, Suite 2400
Bank of America Plaza
P.O. Box 1998 (23218)
Richmond, Virginia 23218-1998
Telephone: (804) 783-7248
Facsimile: (804) 783-7291
jgeiger@sandsanderson.com

/s/ Valentin Gurvits
Valentin D. Gurvits (*pro hac vice*)
Matthew Shayefar (*pro hac vice*)
BOSTON LAW GROUP, PC
825 Beacon Street, Suite 20
Newton Centre, Massachusetts 02459
Telephone: 617-928-1804
Facsimile: 617-928-1802
vgurvits@bostonlawgroup.com
matt@bostonlawgroup.com

/s/ Evan Fray-Witzer
Evan Fray-Witzer (*pro hac vice*)
CIAMPA FRAY-WITZER, LLP
20 Park Plaza, Suite 505
Boston, Massachusetts 02116
Telephone: 617-426-0000
Facsimile: 617-423-4855
Evan@CFWLegal.com

Attorneys for Defendant

CERTIFICATE OF SERVICE

I hereby certify that on the 2nd day of July, 2021, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will then send a notification of such filing to the following:

Scott A. Zebrak, Esquire
Matthew J. Oppenheim, Esquire
Lucy Grace D. Noyola, Esquire
Kellyn M. Goler, Esquire
Oppenheim + Zebrak, LLP
4530 Wisconsin Avenue, NW, 5th Floor
Washington, DC 20016
Email: scott@oandzlaw.com
matt@oandzlaw.com
lucy@oandzlaw.com
kellyn@oandzlaw.com
Counsel for Plaintiffs

/s/ Jeffrey H. Geiger
Jeffrey H. Geiger