IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. KIM DOTCOM, et al., Defendants	The Honorable Liam O'Grady Criminal No. 1:12-CR-3

[PROPOSED] RESPONSE OF DEFENDANT MEGAUPLOAD LTD SUPPORTING AND SUPPLEMENTING THE RENEWED MOTION FOR PROTECTIVE ORDER BY NON-PARTY QTS/CARPATHIA HOSTING, INC. RE MEGAUPLOAD SERVER EVIDENCE

1. Introduction

Defendant Megaupload Ltd. ("Megaupload") (owner of some data at stake herein, legal custodian of third-party data, and named but not served as a criminal defendant in these proceedings) seeks leave of Court to specially appear for the limited exigent purpose of responding to the instant "renewed" motion [D.E. 217-218] that will determine the preservation or destruction of crucial defense evidence stored on servers formerly leased from Carpathia (now "QTS").[1] The Court granted leave to specially appear and oppose the original motion [D.E. 87].

It is well-settled the Due Process Clause "standard of fairness" requires that "criminal defendants be afforded a meaningful opportunity to present a complete defense." *California v. Trombetta*, 467 U.S. 479, 485 (1984). To that end, it is equally well-settled that "the government has a duty to preserve evidence that possesses 'an exculpatory value that was apparent before the evidence was destroyed' where 'the defendant would be unable to obtain comparable evidence by other reasonably available means.'" *United States v. Newsome*, 322 F.3d 328, 334 (4th Cir.

[1] Megaupload reserves all rights regarding the failure of criminal service and to renew its motion to dismiss and nothing herein shall act as a waiver of such rights.

2003) (quoting *Trombetta*, 467 U.S. at 489). In such circumstances, the Government may have a duty "to take affirmative steps to preserve evidence on behalf of criminal defendants," even where the evidence is not already (or not still) in the government's control. *See Trombetta*, 467 U.S. at 486. In this action, Megaupload respectfully submits that the Government has a constitutional duty to preserve the "Carpathia Servers" as potentially exculpatory evidence that "might be expected to play a significant role" in the defense against the crimes alleged in the Superseding Indictment.

Moreover, since the original motion concerning these servers was filed, as discussed below, the Government filed a civil forfeiture action implicating the broad electronically stored information ("ESI") preservation and eDiscovery cooperation mandates of the Federal Rules of Civil Procedure.[2] The duty to preserve and cooperate in ESI preservation to prevent destruction begins not when litigation begins but when it was reasonably anticipated by the Government that it might occur. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003); *The Pension Committee of the University of Montreal Pension Plan, et al. v. Banc of America Securities LLC, et al*., Amended Order, Case No. 05-cv-9016, 2010 U.S. Dist. LEXIS 4546, 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010). The forfeiture civil action in combination with private civil copyright lawsuits related before this court act as an additional and separate basis on which Megaupload requests to be specially heard as an interested party in this proceeding. Megaupload

[2] The civil forfeiture action will continue on regardless of the outcome of the pending appeal and the Megaupload server data will be important evidence from non-infringement to lack of tracing and is vital to the litigants defending their property rights. The Government, which is supposed to be a model litigant, must avoid taking steps to actively interfere with data preservation and avoid destruction of highly relevant ESI. *See, e.g.*, The Sedona Conference® Cooperation Proclamation: Resources For The Judiciary (https://thesedonaconference.org/cooperation-proclamation)

requests preservation of the Megaupload server data, which is important evidence in all the related cases.

A criminal defendant's rights to present evidence, to confront witnesses and to obtain discovery are essential to a fair trial. Forfeiture alleged in this case in the Superseding Indictment [Dkt. 34, ¶¶ 106-116] was adjudged and ordered in Civil Action No.: I: I 4-cv-969, presently on appeal. Civil proceedings impose further requirements on preservation of evidence.

In this novel and complex case, the Government appears determined to prevent defendants from having a fair trial and appears determined to deprive defendants of due process rights protected by the United States Constitution. Distilled to its essence, the Government removed Megaupload's server data from Megaupload's control, will not give it back, and has taken active steps to prevent preservation of the data for use by Megaupload in its own defense.

Non-Party QTS/Carpathia confirms this in their renewed motion. The Government has controlled events for the manifest purpose of seeing such evidence destroyed in a case it has described as one of "the largest criminal copyright cases ever brought by the United States."[3]

Defendants submit that, unless the Court acts to preserve the Megaupload server evidence, the integrity of the criminal case and related proceedings will be irreversibly undermined.

The Court is familiar with the facts. On January 19, 2012, the Government executed search warrants as to Defendants at numerous locations around the world, including at

[3] Press Release, U.S. Department of Justice, Justice Department Charges Leaders of Megaupload with Widespread Online Copyright Infringement (Jan. 19, 2012), http://www.justice.gov/ opa/pr/2012/J anuary/12-crm-07 4.html.

Carpathia's server-hosting facility in the Eastern District of Virginia.[4] On January 27, 2012, the Government informed Megaupload that it had "copied selected Mega Servers and copied selected data from some of the other Mega Servers," without identifying specific data or selection criteria. [D.E. 32]. The Government expressly disclaimed any possession, custody or control over the Mega Servers.[5]

Ensuing events contradicted Government disclaimers of control over the Mega server. On March 20, 2012, Non-party Carpathia Hosting Ltd. filed its Emergency Motion for Protective Order, which is renewed herein. [D.E. 38-39.] On March 30, 2012, Non-party Kyle Goodwin, represented by the Electronic Frontier Foundation, sought to appear to obtain access to files backed up on the Megaupload servers, which he needed because his hard drive had crashed. [D.E. 51-52.] Plaintiffs in related civil suits also appeared. [D.E. 53-55, 80.] The Government opposed Carpathia's Motion. [D.E. 56.] After Megaupload filed papers [D.E. 67], the Government filed a response thereto. [D.E. 76.]

Evidence showed that Megaupload and Carpathia had reached an agreement for Megaupload to purchase the servers from Carpathia for $1,465,500 with payment deferred until final disposition of the criminal case against Megaupload. [D.E. 67, Exhibit C, ¶¶ 1.3, 1.4.] The deal would have given the Megaupload defense team cheap and easy access to the all server

[4] The DOJ seized Megaupload data in the Netherlands at the Leaseweb facility and that data has been destroyed. Megaupload will be further seriously prejudiced if the data at issue is also destroyed because there is no other source for comparable data.

[5] The Government while closely in time actively blocking the "free" transfer of the servers for litigation preservation from Carpathia to Megaupload proclaimed "The Mega Servers are not in the actual or constructive custody or control of the United States, but remain at the premises controlled by, and currently under the control of, Carpathia and Cogent. Should the defendants wish to obtain independent access to the Mega Servers, or coordinate third-party access to data housed on Mega Servers, that issue must be resolved directly with Cogent or Carpathia." [Letter of Department of Justice to Defendants' attorneys quoted in Carpathia's prior Rebuttal Memorandum [Dkt. 70] at 7-8.]

data evidence and would have substantially alleviated evidentiary and due process issues in both the civil and criminal cases. As stated by Carpathia, the agreement was: "a much less expensive alternative than Mega making its own image of the servers. … The government objected to that sale, apparently for the reasons described in its response brief: 'The government … is additionally concerned because it has not seen any detailed plans for appropriately transferring the Carpathia Servers to an entity that demonstrates reasonable and untainted resources for that purpose, provides sufficient safeguards regarding access, successfully deals with the specific concerns of victims, and deals appropriately with the contraband and other illegitimate files on the Carpathia Servers.' (Govt Br. at n. 3). " (Carpathia Rebuttal Memo [D.E. 70 at 7-8] quoting from D.E. 56.)

The Government's stated concerns about safeguards, etc., were not based on fact. Contrary to Government objections, Megaupload wanted the servers to be preserved "under a litigation hold." Defense counsel and consultants would have "exclusive access to the Mega data hosted on the Mega servers" and "[a]ll uses of the data . . . [would] be for purposes of assisting Mega and co-defendants in criminal or civil litigation." Defendants proposed that "consumer access to server content shall be prohibited and allowed only on such terms as shall be ordered by a UnitedStates District Court or agreed to in writing signed by the US Attorney's Office," and that "No electronically stored materials may be materially altered, wiped, deleted, or destroyed in any manner." [D.E. 67, Exhibit D.]

A hearing on the matter was held on April 13, 2012. [D.E. 86, 84, 87.] The Court ordered the parties to meet and confer in front of a magistrate judge and to report in two weeks if the matter was not resolved. [D.E. 87.] Resolution not having been achieved and a new Motion for Return of Property/Pre-Trial having been filed by Non-party Goodwin [D.E. 90-91], a second

hearing was scheduled for June 29, 2012, which led to further briefing. [D.E. 92, 98, 99, 105, 110.]

Thereafter, on October 2, 2012, the Court ruled that "the Court finds that it is unable to reach a conclusion as to this matter without an evidentiary hearing." The Court ordered briefing and stated that: "The Court will consider the parties filings and designate a date for the hearing thereafter." [D.E. 126, see also D.E. 130, extending time for briefing.] Further motions, briefs and documents were filed. [D.E. 131, 133-136, 139-141, 144, 149, 153, 155, 157-158, 161-164, 168-170, 174-189.]

In the meantime on or about February 1st 2013 the Government permitted the Megaupload server data located in the EU at Leaseweb in the Netherlands to be destroyed. Megaupload advised Judge Anderson of the development, see letter of July 3, 2013, attached hereto as Exhibit A, and asked to reconvene the meet and confer meetings ordered by the Court on April 18, 2012 [D.E. 87.] in order to preserve the server data located at Carpathia. The United States declined any meet and confer on data preservation.

On July 29, 2014, the Government filed a civil forfeiture action targeting all the revenues and user conduct arising out of Megaupload's global cloud storage services including revenues arising out of the server data evidence in the Netherlands and revenues arising out of the server data evidence in the United States.

No hearing on the server data preservation matter was scheduled until QTS/Carpathia filed the instant renewal Motion. Defendants again request that the Court intervene and permit the transfer of the Megaupload servers in a manner and method that preserves the integrity of the data such that it can be used in the civil and criminal case and to preserve the integrity of due process.

ARGUMENT

I. As a Matter of Fact, the Government Seized Control of Megaupload's Data in January 2012 and Has Never Relinquished Control. Having Blocked Preservation of the Evidence, the Government Cannot Disclaim Control Under Rule of Criminal Procedure 16.

The evidence shows that, as a matter of practical fact, the Government seized control of the Carpathia Servers and the Megaupload data in January 2012 and has never relinquished control. During prior proceedings, the Government exercised its control power to exclude Megaupload and its counsel from the server data. It is anticipated that the Government will continue to assert such control in opposing this motion.

A. Due Process Considerations

It is well-settled the Due Process Clause "standard of fairness" requires that "criminal defendants be afforded a meaningful opportunity to present a complete defense." *California v. Trombetta*, 467 U.S. 479, 485 (1984). To that end, it is equally well-settled that "the government has a duty to preserve evidence that possesses 'an exculpatory value that was apparent before the evidence was destroyed' where 'the defendant would be unable to obtain comparable evidence by other reasonably available means.'" *United States v. Newsome*, 322 F.3d 328, 334 (4th Cir. 2003) (quoting *Trombetta*, 467 U.S. at 489). The test for a duty to preserve evidence is whether the "evidence that might be expected to play a significant role in the suspect's defense." *Trombetta*, 467 U.S. at 488. To meet this standard of constitutional "materiality" the evidence "must both possess an exculpatory value that was apparent before the evidence was destroyed, and be of such a nature that the defendant would be unable to obtain comparable evidence by other reasonably available means." *Id*. at 489. In such circumstances, the Government may have a duty "to take affirmative steps to preserve evidence on behalf of criminal defendants," even where the evidence is not already (or still) in the government's control. *See id*. at 486. In this

action, Megaupload respectfully submits that the Government has a constitutional duty to preserve the Carpathia Servers as potentially exculpatory evidence that "might be expected to play a significant role" in the defense against the crimes alleged in the Superseding Indictment.

This case contrasts with *Newsome*, in which the Government's failure to seize certain evidence, and its subsequent destruction, did not arise to a constitutional violation. In *Newsome*, the defendants were convicted of illegally cutting down certain protected trees in a National Forest. Federal investigators found logs from the protected trees at three local lumber mills. The logs were photographed, and slabs (or "cookies") of each log were taken and preserved and used as evidence. The full logs were not seized by the federal investigators, however, and the logs were later milled into veneer by the lumber mills. The defendants contended that the government's failure to seize and preserve the full logs constituted spoliation that violated their Due Process rights.

The Fourth Circuit rejected that contention because the defendants had access to the photographs, the cookies (which were representative samples of the trees and logs), mill records, and mill employees, all of which was deemed to constitute "comparable evidence" that was reasonably available to defendants. *Newsome*, 322 F.3d at 334. The Government makes a similar argument in this case, arguing that it took control of the Carpathia Servers only temporarily pursuant to a search warrant and obtained certain samples of the data, which it will preserve, but it disclaims any duty to seize and preserve the entirety of the data on those servers. [D.E. 56 & 82.] That reasoning is fallacious in the circumstances of this action because the samples obtained are not representative of all the data on those servers—only data that (apparently) is consistent with the Government's theory. Having seized control of the Carpathia Servers in order to forensically copy certain portions of the data, the Government has triggered

its duty to preserve the remaining data because it "might be significant" to the defense in this action, and "comparable evidence" cannot be obtained by reasonably available alternative means. Each datum is unique, and unlike the cookies taken in *Newsome*, the government's seizure of a portion of the data from the Carpathia Servers is not a representative sample of the entire data set.

Furthermore, apart from the Due Process Clause basis for requiring the government to preserve the Carpathia Servers, the Court has "inherent discretionary power to issue orders in aid of [its] jurisdiction." *Orbe v. True*, 201 F. Supp. 2d 671, 676 (E.D. Va. 2002). "And, such an order may extend, 'under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate … the proper administration of justice." *Id*. (quoting *United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977)). Such an order to preserve evidence related to the defendant's case cannot be open-ended, but must describe the proposed evidence with particularity—which is satisfied here, of course, because the evidence is the data on the Carpathia Servers.

As alleged in the Superseding Indictment, the data on the Carpathia Servers would be a critical source of evidence to prove or disprove guilt [*e.g*., D.E. 34, ¶ 5; ¶¶ 25-26 (describing how content was uploaded to or downloaded from "servers," including Carpathia Servers]. This source of evidence came under the control of the Government, who made selected copies of it, but since then the Government has tried to disclaim any responsibility for seizing and preserving this data. Respectfully, as pointed out by the Supreme Court, assessing the importance of lost evidence is extraordinarily difficult. *Trombetta*, 467 U.S. at 487 ("Whenever potentially exculpatory evidence is permanently lost, courts face the treacherous task of divining the import of materials whose contents are unknown and, very often, disputed. … Moreover, fashioning

remedies for the illegal destruction of evidence can pose troubling choices.") (citation omitted). Thus, it is much easier to preserve this evidence now than to try to fashion evidentiary remedies later.

B. Rule 16 Considerations

While the Government contends that Rule 16 is irrelevant because the case has not proceeded to the discovery phase, yet [*e.g.*, D.E. 56 at 4-5]. That misses the point. In light ot the Government's duties during the discovery phase, the Government is not permitted to allow the destruction of the evidence beforehand.

Rule 16(a)(1)(E) of the Federal Rules of Criminal Procedure provides that, "[u]pon a defendant's request, the government must permit the defendant to inspect . . . tangible objects, buildings or places . . . if the item is within the government's possession, custody, or control and: (i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant." Megaupload respectfully submits that the Carpathia Servers are now in the Government's control, and must be preserved for later production under Rule 16.

1. Control of the evidence by the Government.

As to the issue of "possession, custody or control" of the Megaupload data, the court in *United States v. Stein*, 486 F.3d 350 (2d Cir. 2007) reviewed the history of the phrase in Civil Rule 34, Criminal Rule 16 and Civil Rule 45 and concluded that a uniform construction was appropriate. 488 F.3d at 361. At 361-362, the *Stein* court reviewed numerous authorities:

One noted commentator aptly summarized the scope of the obligation:

> "Legal ownership of the requested documents or things is not determinative, nor is actual possession necessary if the party has control of the items. Control has been defined to include 'the legal right to obtain the documents requested upon demand.' The term 'control' is broadly construed." [footnote: 7 MOORE'S FEDERAL PRACTICE §

> 34.14[2][b], at 34-63 to 34-64 (3d ed. 2006) (footnotes omitted); numerous supporting citations omitted.]
>
> These principles have been applied in a wide variety of situations. …

Stein also quoted from *United States v. Kilroy*, 523 F. Supp. 206, 215 (E.D. Wis. 1981) where the court found that the Government had constructive control over evidentiary documents because it was cooperating with defendant's former employer.

> I see no objection to an order requiring the Government, as the defendant asks, to use its "best efforts" to obtain from Standard Oil all of the documents in its possession which came out of the defendant's former office. The Government has 30 days to try to obtain the records. Standard Oil is admittedly not a party to this suit and has no obligation to turn over any of its records to the defendant or to the Government except at trial pursuant to a valid subpoena. Since Standard Oil is cooperating with the Government in the preparation of the case and is making available to the Government for retention in the Government's files any records which Standard Oil has and which the Government wants, however, ***it is not unreasonable to treat the records as being within the Government's control at least to the extent of requiring the Government to request the records on the defendant's behalf and to include them in its files for the defendant's review*** if Standard Oil agrees to make them available to the Government. (Emphasis added.)

A similar result was reached in *United States v. Skedde*, 176 F.R.D. 258, 262 (W.D. Ohio), which also cited *Kilroy* (emphasis added):

> In *United States v. Bryan*, 868 F.2d 1032, 1036 (9th Cir. 1989), the Ninth Circuit stated, in a case involving a request for records of a nationwide investigation of fraudulent tax shelters by a defendant charged with mail fraud in conjunction with a scheme involving such shelters, that "the scope of the government's obligation under Rule 16(a)(1)(C) should turn on the extent to which the prosecutor has knowledge of and access to the documents sought by the defendant in each case." The case was remanded for a hearing to determine whether the defendant had been deprived of discovery of documents "which the prosecution had knowledge of and access to." Id.
> Because ***the records at issue here once were available to the government***, there is greater justification to ***call on it to retrieve them*** than was the case in Kilroy. On the other hand, the records involved in this case appear to be considerably more extensive than the limited category of materials at issue in Kilroy. Nonetheless, it appears appropriate to direct the government to undertake forthwith to retrieve any documents that once were in its possession but remained with LOF and which are 'material to the preparation of the defense' and provide those materials as promptly as reasonably possible to the defendants.

2. Materiality is shown.

Defendants are entitled to discovery of its data on the QTS/Carpathia servers because "(iii) the item was obtained from or belongs to the defendant." Criminal Rule 16(a)(1)(E)(3).

Perhaps more important here, the data is essential to trial preparation and proof on numerous critical issues and is, therefore, material under Criminal Rule 16(a)(1)(E)(1). Such materiality is manifest because the Megaupload server data "will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." *United States v. Stein*, 486 F.3d 350, 357 (2d Cir. 2007), quoting from *United States v. Lloyd*, 301 U.S. App. D.C. 186, 992 F.2d 348, 351 (D.C. Cir. 1993).

The jury will be asked to make decisions on the totality of all the evidence relating to issues of knowledge, intent and willfulness. The whole range of Defendants' operations and user conduct bear on such issues. Defendants have repeatedly articulated legal and factual problems with the Government's case that if not decided as a matter of law in defendants favor will require specific factual determinations. Defendants anticipate requesting special verdict forms with numerous interrogatories that will implicate evidentiary constellations extending over large-scale domains.

Direct criminal infringement requires willful infringement of a valid copyright. 17 U.S.C. § 506(a)(1); *United States v. Teh*, 535 F.3d 511, 517 n.4 (6th Cir. 2008). "Willfulness" under the criminal copyright statute means a "voluntary, intentional violation of a known legal duty." *United States v. Moran*, 757 F. Supp. 1046, 1049 (D. Neb. 1991) (quoting *Cheek v. United States*, 498 U.S. 192 (1991)). Defendant must have acted with knowledge that his conduct was unlawful. *Safeco Insurance Co. of America v. Burr*, 551 U.S. 47, 58 n.9 (2007). See

also 17 U.S.C. § 506(a)(2) ("[E]vidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement of a copyright."); 4 M. Nimmer & D. Nimmer, Copyright, § 15.01[A][2] (2011).

Copyright infringement is assessed on a work-by-work basis. Defendant must have had the specific intent to commit copyright infringement as to each individual work. See, e.g., *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 34 (2d Cir. 2012) (in the more lenient civil context, knowledge level of defendant must be assessed as to each and every file alleged to be part of defendant's mass infringement); *Viacom Int'l Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110, 115-123 (S.D.N.Y. 2013) (ruling that plaintiffs had no "clip-by-clip" evidence to prove knowledge of infringement for any of the 63,060 video clips-in-suit).

Other charges against Defendants appear to allege secondary liability for criminal copyright infringement that Congress has declined to create. *See* Inducing Infringement of Copyrights Act of 2004, S. 2560, 108th Cong. (2003). "Congress has finely calibrated the reach of criminal copyright liability, and therefore, absent clear indication of Congressional intent, the criminal laws of the United States do not reach copyright-related conduct." 4 M. Nimmer & D. Nimmer, Copyright, § 15.05[A], 15-34 (2011). "[I]t is implausible to suppose that Congress intended to combat the problem of copyright infringement by the circuitous route hypothesized by the Government." *Dowling v. United States*, 473 U.S. 207, 220-221 (1985).

Defendants are charged with operating a system that facilitates infringement. But direct infringement requires more than "mere ownership of a machine used by others to make illegal copies"—there "must be actual infringing conduct." *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 549-50 (4th Cir. 2004); *see also ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619, 622 (4th Cir. 2001), quoting H.R. Rep. No. 105-551(I), at 11 (1998)); *Cartoon*

Network LP, LLLP v. CSC Holdings, Inc., 536 F.3d 121, 131-32 (2d Cir. 2008). Conspiracy allegations fail to overcome these defects. Conspiracy is not found in the four corners of the criminal copyright statute and the Government ought not be permitted to add it on under the reasoning in *Dowling* and its progeny.

The Government must prove layers of willfulness, knowledge and intent. The Government fails to properly allege the elements of primary willful copyright infringement by users and without primary willful infringement there can be no secondary willful infringement.

The higher mens rea standard of willfulness is applied to a charge of conspiracy to commit copyright infringement. *Ingram v. United States*, 360 U.S. 672, 678 (1959); *United States v. Brown*, 581 Fed. Appx. 216, 217 (4th Cir. 2014). The Superseding Indictment does not allege an agreement between Defendants and Megaupload users but only among the Defendants themselves. *See United States v. Burgos*, 94 F.3d 849, 860 (4th Cir. 1996) (conspiracy requires "a *specific* agreement to commit a *specific* crime" (internal citation and quotation marks omitted)); *United States v. Gengler*, 2009 WL 5549225, at *8-9 (E.D. Va. Oct. 23, 2009) (conspiracy requires an agreement to violate the law).

The superseding indictment and related documents appear weak on supporting the claims with geo-location data on where data transfers and events occurred and the who, what, when, where, and how of the alleged copyright infringement and automated processes.

Absent an expression of Congressional intent, federal laws do not apply extraterritorially. *Morrison v. National Australia Bank*, 130 S. Ct. 2869 (2010). The Fourth Circuit and numerous sister circuits have confirmed that the Copyright Act does not apply to conduct occurring abroad. *Nintendo of America, Inc. v. Aeropower Co.*, 34 F.3d 246, 249 n.5 (4th Cir. 1994); *Subafilms, Ltd. v. MGM-Pathe Commc'ns Co.*, 24 F.3d 1088, 1095 (9th Cir. 1994) (en banc); *Palmer v.*

Braun, 376 F.3d 1254, 1258 (11th Cir. 2004); *Robert Stigwood Group Ltd. v. O'Reilly*, 530 F.2d 1096, 1101(2d Cir. 1976).

Megaupload wants to show that it provided a legitimate cloud storage site, used by entertainment studios, colleges and government officials for official business. Data on the servers will show that Megaupload maintained strong and effective notice and takedown "safe harbor" policies and practices to curb infringement. Such showings will both defeat prosecution charges that require proof of a "willfulness" mens rea and also raise a defense of "dual use technology" that "is capable of substantial non-infringing uses" and protected in the civil context under *Sony Corp. of America v. Universal City Studios, Inc*., 464 U.S. 417. 439 (1984). Evidence needed for such showings is in the Megaupload server data and not just the portions cherry picked by the Government. From information provided, it appears that the Government has preserved less than 1% of the data on the Megaupload servers. See D.E. 99 at p. 2.

Defendants need access to ***all*** the data for forensic analysis that will show the software code, automated systems, direct delete processes, content servers, and lack of mens rea in Megaupload cloud storage operations, notwithstanding the Government's emphasis on alleged cherry picked infringements. Evidence provided by the Government in extradition proceedings in New Zealand states that Megaupload users had uploaded 206 million total unique files as of January 19, 2012. Of the 14.9 million unique video files stored on servers located within the United States, roughly 42% had never been viewed. Megaupload is entitled to do their own analysis from the raw forensic data.

Log files and databases on the servers may show that copyright owners, their agents or government agents uploaded files alleged to have infringed. Server data will provide geographical locators for alleged infringements and act to provide evidence of extraterritorial

alleged infringements that fail as a matter of law. Server data will show that charges of infringement of particular works are outside of an applicable statute of limitations, are fair use, or otherwise fail on multiple elements.

Indeed, the United States-New Zealand treaty gives a New Zealand the benefit of New Zealand's three year statute of limitations for criminal copyright infringement for the New Zealand accused at s instead of the five years under US law argued by the Government (see Treaty on Extradition between United States and New Zealand, 1970 U.S.T. LEXIS 470; 22 U.S.T. 1.) This will be a point of legal and factual contention at any trial in the United States.

C. The Court Should Exercise Inherent Powers to Preserve Evidence and Protect Due Process Rights of Defendants.

"[A] federal court has the inherent power to order the preservation of evidence in the hands of a party before the Court." *United States v. Salad*, 779 F. Supp. 2d 503, 507 (E.D.Va. 2011) (hereinafter "*Salad*"); *accord Orbe v. True, supra*. The case of *Salad* involved the yacht "Quest," the site of high-seas piracy, hostage-taking and murder. The court ordered the Government to maintain the yacht and make it accessible to defense counsel and experts. In support of the order, *Salad* cited, *inter alia*, *The Pueblo of Laguna v. United States*, 60 Fed. Cl. 133, 135 (Fed. Cl. 2004) for "the inherent powers afforded Article III courts to order the preservation of relevant evidence."

Constitutional rights of criminal defendants include access to exculpatory evidence. *Kyles v. Whitley*, 514 U.S. 419, 432 (1995); *Brady v. Maryland*, 373 U.S. 83 (1963). Access must be given if "favorable evidence could reasonably be taken to put the whole case in such

a different light as to undermine confidence in the verdict." *Kyles*, supra, 514 U.S. at 435 See also *United States v. Bagley*, 473 U.S. 667, 682 (1985); *Brady*, 373 U.S. at 87-88.[6]

The novelties and complexities of this case require the preservation of the Megaupload server evidence. Megaupload has not been served in the criminal case and the court has deferred ruling on the motion to dismiss while noting that failure to serve can become improperly prejudicial at some point in time. Forfeiture rulings for Megaupload and other defendants are on appeal. Similar and perhaps substitutionary data in the Netherlands has been destroyed.

The Government apparently bases charges of conspiracy on underlying acts of criminal copyright infringement committed by individual users, but there is no evidence of actual agreements with the perpetrators of such crimes. Indeed, such individual agreements would have been unlikely because Defendants had a constant stream of demands on their time and attention while they tried to shape and control a surprisingly successful global cloud storage system as a lawful Online Services Provider. Defendants need the server data to properly portray their wide-ranging worldwide operations and will need access to all the evidence in order to do so.

D. Civil Rules Governing "Electronically Stored Information" Require Preservation of Evidence for the Forfeiture Case.

The duty to preserve evidence "arise[s] not only during [civil] litigation but also extends to that period before the litigation when a party reasonably should know that the

[6] "A prosecution that withholds evidence on demand of an accused which, if made available, would tend to exculpate him or reduce the penalty helps shape a trial that bears heavily on the defendant. That casts the prosecutor in the role of an architect of a proceeding that does not comport with standards of justice, even though, as in the present case, his action is not 'the result of guile,' to use the words of the Court of Appeals."

evidence may be relevant to anticipated litigation." *Silvestri v. General Motors*, 271 F.3d 583, 591 (4th Cir. 2001). Once such duty arises, a party must take reasonable steps to preserve "what it knows, or reasonably should know is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request." *Wm T. Thompson Co. v. General Nutrition Corp.*, 593 F. Supp. 1443 (C.D. Cal. 1984).

As stated in the DOJ's Asset Forfeiture Policy Manual 2013 maintained at http://www.justice.gov/sites/default/files/criminal-afmls/legacy/2014/05/23/policy-manual-2013rev.pdf and accessed on August 23, 2015:

> There is a legal duty to preserve potentially relevant evidence once a party reasonably anticipates litigation, whether the United States is the plaintiff or defendant. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003); Fed. R. Civ. P. 37, Advisory Committee Note, 2006 Amendments, Subdivision (f). Although a litigation hold is the primary method of preservation, reasonableness and good faith are the ultimate standards by which an alleged breach of the duty to preserve is judged. (p. 157.)
> The obligation to preserve evidence arises when a party has notice that evidence is relevant to litigation. (p. 158)
> The advising DOJ attorney should not make the decision to lift a litigation hold until after the time for filing direct appeals in the case (and related or ancillary proceedings) or a petition for a writ of certiorari has passed. (p. 162)

The original Indictment [D.E. 1, ¶¶ 90-99], the search warrants [D.E. 11-16] and the Superseding Indictment, supra, were clearly aimed at forfeiture of all of Megaupload's assets and revenue for alleged criminal copyright infringement. Such claims were necessarily alleged in the broadest possible way, while ignoring the context of new developments in cloud storage industries and difficulties of proof that result from remote geographical locations and from data maintained and organized for technological purposes rather than for legal purposes.

As previously noted, it appears that the Government has preserved less than 1% of the data on the servers. [See D.E. 99 at p. 2.] Manifestly, the 99% that has not been preserved contains "material" evidence as set forth above.

The record reflects the extraordinary importance of this data to Megaupload defendants, to its users and to online communities that need guidance about permissible and impermissible online activities. Indeed, the forfeiture case, whether reversed on appeal or not, due to Mona Dotcom's claims, deal with tracing revenues arising from alleged infringements which cannot be competently done in a fair adversarial manner if the US and EU servers have been discarded. All of Megaupload's servers need data preservation. For example the software code demonstrates a copyright neutral technology. The database servers can show safe harbor compliance. The web servers can show the copyright neutral nature of the interface design. The content servers in combination with other data can show fair use and substantial non-infringing uses and users.

Defendants and Carpathia worked out an arrangement for data preservation that would have protected legitimate ESI usage and litigation hold interests but, in contradiction to the cooperation in data preservation as provided for by law and reasonable practices mandated by courts across the United States the DOJ blocked the agreement and provided no alternative preservation solution. (The Sedona Conference® Cooperation Proclamation: Resources For The Judiciary https://thesedonaconference.org/cooperation-proclamation). The Megaupload server data in the Netherlands was permitted by the DOJ to be destroyed when they knew or should have known that such evidence was highly relevant to the criminal action and the reasonably anticipated civil forfeiture action. Unfair prejudice through loss of important evidence has occurred and will continue to occur unless the court intervenes and will adversely impact defendants in this criminal case, the civil forfeiture case, and in pending civil cases where

defendants are being sued, e.g., by the Motion Picture Association of America (MPAA) and the Recording Industry Association of America (RIAA).

Consequences of loss of evidence are illustrated by *Trigon Ins. Co. v. United States*, 204 F.R.D. 277 (E.D. Va. 2001), where sanctions were imposed on the United States for spoliation.[7] In resisting discovery, the United States argued that documents maintained by its "consultant," Analysis Group/Economics ("AGE"), were not subject to discovery. When that argument was rejected, it was revealed that evidence had been destroyed relating to AGE and experts it retained. The court reiterated policy reasons that are also applicable here (*Id*. at 284-285):

> "the [spoliation] inference stems from the 'common sense observation that a party who has notice that [evidence] is relevant to litigation and who proceeds to destroy [evidence] is more likely to have been threatened by [that evidence] than a party in the same position who does not destroy the [evidence].'" *Anderson v. National Railroad Passenger Corporation*, 866 F. Supp. 937, 945 (E.D. Va. 1994) (quoting N*ation-Wide Check Corp. v. Forest Hills Distributors Inc*., 692 F.2d 214, 218 (1st Cir. 1982)). The destruction of evidence can lead to manifest unfairness and injustice, for it increases the risk of an erroneous decision on the merits of the underlying cause of action and can increase the costs of litigation as parties attempt to reconstruct the destroyed evidence or to develop other evidence that may be less persuasive, less accessible or both.

The court further ruled that Trigon could recover its costs and attorney fees associated with the motion, to be determined after trial. (204 F.R.D. 291, n. 11 and referencing text.) Trigon was later awarded fees and expenses in the amount of $ 179,725.70. *Trigon Ins. Co. v. United States*, 234 F. Supp. 2d 592, 595 (E.D.Va. 2002); *see also Aaron v. Kroger L.P.*, 2011 U.S. Dist. LEXIS 111004 (E.D. Va. 2011) ("In the instant case, Kroger was on notice of Plaintiff's request that the evidence be preserved. Kroger also knew or should have known that the video footage — whether or not it showed Plaintiff's actual fall — might later prove relevant,

[7] Spoliation is defined at 204 F.R.D. 284, e.g., "Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation," citing *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 778 (2nd Cir. 1999).

such that preserving the tapes was clearly the more prudent course of action."); *Cytec Carbon Fibers LLC v. Hopkins*, 2012 U.S. Dist. LEXIS 173247 (D.S.C. 2012); *Beaven v. United States DOJ*, 622 F.3d 540 (6th Cir. 2010) (government officials wrongfully disclosed a file folder containing private information and then destroyed the file folder); and *United States v. CBS, Inc.*, 103 F.R.D. 365 (C.D. Cal. 1994) (granting in part non-party movie studios' motion to recover $2,000,000 cost of responding to discovery subpoenas, including costs for personnel for time spent on document production, equipment, supplies, transportation, alterations of facilities to provide work space for the document production, and accountants' fees for time spent responding to subpoenas).

E. The Court Should Refer the Matter to a Magistrate Judge for a Determination of the Most Expeditious and Economical Method of Preservation. The Government Should Be Required to Bear the Cost.

Technological development proceeds at a rapid pace. Servers put into service before January 2012 will have a greatly diminished value in 2015-2016. Transferring the Megaupload data to new servers would require expensive hardware and many hours of labor. Defendants submit that the most likely best use for the servers now being stored by QTS/Carpathia will be as a forensic database that is maintained intact, catalogued and explored. Important materials can be copied for purposes of the parties while the "best evidence" remains unaltered. However, such possibilities are subject to specific facts such as preserving the integrity of sensitive data storage from data loss over time and forensic access that are outside the scope of this motion. Reference to a magistrate judge for ESI cooperation is appropriate.

Defendants do not have assets necessary to preserve the data, to provide access to the data, to transfer the servers to a new storage facility or to compensate QTS/Carpathia for their past storage of the servers. Defendants submit that the costs for these undertakings should be

borne by the Government who manufactured the problem. *United States v. Salad*, supra; *The Pueblo of Laguna*, supra, at 60 Fed. Cl. 140 ("In the court's view, the better course is to reemphasize that documents should not be destroyed and create incentives to ensure that happens. … The Department of the Interior ("DOI") shall move inactive Pueblo of Laguna records from the BIA Southwest Regional Office to the Office of Trust Records ("OTR"), in Albuquerque, New Mexico, at which location said inactive records shall be made available to plaintiff for purposes of inspection."); *Trigon Ins. Co. v. United States*, supra; *United States v. CBS, Inc., supra.*

Conclusion

For the foregoing reasons, defendant Megaupload, Ltd. respectfully requests that the Court grant them leave to specially appear for the limited exigent purpose of responding to the instant motion.

Defendants, like QTS/Carpathia, are frustrated by the exercise of control on the part of the Government that has blocked a simple resolution of issues involved in preservation of the crucial Megaupload server data. Unlike QTS/Carpathia, Defendants' frustration is not grounded in only monetary distress. The Government is burdened with a weak case to present in a criminal trial and it wants to prevent a strong defense. The Government cannot criminally and civilly indict all the revenues arising out of all the global users of the Megaupload cloud storage site in the largest copyright case in history while at the same time cherry picking a sliver evidence to retain for trial and throwing away the rest to manifestly prevent the mounting of a fair defense.

Therefore, defendants ask the Court to protect their rights under Criminal Rule 16 and the other rules and case law cited herein and to exercise its inherent powers in ordering the

preservation of the Megaupload data for the multiple related litigations. Preservation should be carried out by purchase of QTS/Carpathia servers and their transfer to facilities that will provide access to the data for the benefit of defendants' counsel and experts, the Government and others authorized by the Court. The Government should bear the cost of such purchase and preservation. Details should be worked out by reference to a magistrate judge.

Respectfully submitted,

/s/ Craig C. Reilly
Craig C. Reilly
VSB # 20942
111 Oronoco Street
Alexandria, Virginia 22314
TEL (703) 549-5354
FAX (703) 549-5355
Craig.reilly@ccreillylaw.com

Ira P. Rothken
ROTHKEN LAW FIRM
3 Hamilton Landing
Suite 280
Novato, CA 94949
(415) 924-4250
(415) 924-2905 (fax)
ira@techfirm.net

Counsel for Defendant Megaupload Limited

CERTIFICATE OF SERVICE

I hereby certify that on August 24, 2015, the foregoing MOTION OF SPECIALLY APPEARING DEFENDANT AND INTERESTED PARTY MEGAUPLOAD LIMITED TO FILE [PROPOSED] RESPONSE OF DEFENDANT MEGAUPLOAD LTD SUPPORTING AND SUPPLEMENTING THE RENEWED MOTION FOR PROTECTIVE ORDER BY NON-PARTY QTS/CARPATHIA HOSTING, INC. RE MEGAUPLOAD SERVER EVIDENCE, was filed and served electronically by the Court's CM/ECF system upon all registered users.

/s/ Craig C. Reilly
Craig C. Reilly
VSB # 20942
111 Oronoco Street
Alexandria, Virginia 22314
TEL (703) 549-5354
FAX (703) 549-5355
Craig.reilly@ccreillylaw.com
Counsel for Defendant Megaupload Ltd.

quinn emanuel trial lawyers | washington, dc
1299 Pennsylvania Avenue NW, Suite 825, Washington, District of Columbia 20004-2400 | TEL: (202) 538-8000 FAX: (202) 538-8100

WRITER'S DIRECT DIAL NO.
(202) 538-8120

WRITER'S INTERNET ADDRESS
williamburck@quinnemanuel.com

July 3, 2013

The Honorable John F. Anderson
United States Magistrate Judge
United States District Court for the Eastern District of Virginia
Albert V. Bryan U.S. Courthouse
401 Courthouse Square
Alexandria, VA 22314

Re: *United States v. Kim Dotcom, et al., Case No. 1:12-cr-3*

Dear Judge Anderson:

We are writing to alert the Court to the recent revelation that on February 1, 2013, LeaseWeb deleted all data from 630 servers previously leased to Megaupload in the Netherlands.[1] This wholesale destruction of millions of Megaupload users' personal files was in direct contravention of Megaupload's and Electronic Frontier Foundation's ("EFF") repeated requests to LeaseWeb for data preservation pending resolution of the U.S. criminal case. Specifically, in a letter dated April 3, 2012, EFF wrote to Leaseweb "to formally request that [LeaseWeb] preserve that material both for purposes of contemplated future litigation and as a matter of obligation and courtesy to the innocent individuals whose materials have unfortunately been swept up into this case." EFF's letter further requested "that anyone with access to our client's materials, or evidence potentially relevant to an action filed on behalf of our client or other similarly situated third parties, immediately institute a litigation hold that covers all reasonably potentially relevant evidence, e.g., the complete set of data on servers used by Megaupload." Similarly, on March 1, 2012, Megaupload asked LeaseWeb to confirm "that it will preserve the Megaupload data," noting that "this request is supported by multiple

[1] Further information regarding LeaseWeb's deletion of server data is available at http://torrentfreak.com/leaseweb-wipes-all-megaupload-user-data-dotcom-outraged-130619/ and http://torrentfreak.com/dotcom-reveals-megaupload-data-massacre-emails-plans-to-sue-leaseweb-130626/.

EXHIBIT A

axiomatic reasons including that it is relevant evidence in a pending criminal case in the US, potential civil case(s), and destruction of such data will interfere with the possible return of such data to consumers."[2]

In addition to destroying petabytes of Megaupload user data, Leaseweb's actions have impaired our clients' defense, as the servers contained vast amounts of potentially exculpatory evidence directly relevant to the U.S. criminal case. While LeaseWeb's deletion of relevant evidence in the face of explicit preservation requests is inexcusable, the United States is equally culpable. The Government was plainly on notice of the need to preserve the LeaseWeb servers.[3] As Megaupload has long maintained, by freezing the Defendants' assets and denying Defendants access to or possession of the servers, the Government has exercised *de facto* control over the servers and is therefore in constructive possession of them. Under *Brady v. Maryland*, 373 U.S. 83 (1963) and its progeny, the Government had an affirmative duty to ensure the preservation of the LeaseWeb servers and the exculpatory evidence they may have contained. The Government failed to do so.

The destruction of the LeaseWeb servers demonstrates the urgent need to reach a workable solution for data preservation as soon as possible, lest the 1,103 servers currently in Carpathia Hosting's possession meet the same fate. We therefore respectfully urge the Court to reconvene the interested stakeholders and renew negotiations as quickly as the Court's schedule permits.

Sincerely,

William Burck /s/ — Ira Rothken /s/

William A. Burck
Quinn Emanuel Urquhart & Sullivan, LLP

Ira P. Rothken
The Rothken Law Firm

Enclosures

---

[2] Copies of the EFF and Megaupload letters are enclosed for the Court's reference.

[3] *See, e.g.,* April 3, 2012 Letter from EFF to LeaseWeb (Dkt. 57); Megaupload's Response to Emergency Motion for Protective Order by Carpathia Hosting, Inc. (Dkt. 67-1), at 7 n.4 ("Like Carpathia, Leaseweb is refusing to continue to maintain the servers as of April 13 absent appropriate compensation. Megaupload would hope to use its assets upon release by the Court to ensure preservation on that front as well."); April 18, 2012 Letter from Megaupload to Jay V. Prabhu, at 2 ("Because a similar problem exists with servers currently maintained by Leaseweb in the Netherlands, we hope and envision that the ultimate solution for preservation of the servers held by Carpathia can likewise be applied to those in Leaseweb's possession."). A copy of the April 18, 2012 letter is enclosed for your reference.

EXHIBIT A

cc: The Honorable Liam O'Grady, United States District Judge
Jay V. Prabhu, Assistant United States Attorney, counsel for the United States
Marc J. Zwillinger, counsel for Carpathia Hosting, Inc.
Julie P. Samuels, counsel for Kyle Goodwin
Paul M. Smith & Julie M. Carpenter, counsel for Motion Picture Association of America
W. Clifton Holmes, counsel for Valcom, Inc. and Microhits, Inc.

EXHIBIT A