

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

<hr/>		
TWENTIETH CENTURY FOX FILM CORP., <i>et al.</i>)	
)	
<i>Plaintiffs,</i>)	
)	
v.)	No. 1:14cv362
)	(LO / IDD)
MEGAUPLOAD LIMITED, <i>et al.</i> ,)	
)	
<i>Defendants.</i>)	
<hr/>		

**RESPONSE OF DEFENDANT MEGAUPLOAD LTD.
TO PLAINTIFFS’ MOTION FOR ENTRY OF PRESERVATION ORDER**

Defendant Megaupload Limited (“Megaupload”) hereby responds to *Plaintiffs’ Motion for Entry of Preservation Order* (Dkt. Nos. 61-64). Megaupload agrees that the Court should enter a preservation order in this action and a related private copyright infringement action¹ specifying the agreed upon protocol to retrieve, restore, and preserve the cached data on servers that non-party Cogent Communications, Inc. had leased to Megaupload (“Cogent Servers”). Thus, Megaupload agrees to certain paragraphs of the proposed preservation order submitted by Plaintiff (Dkt. No. 61-1). As explained below, however, paragraphs 5 and 8 of the proposed order should not be adopted by the Court. Although written to sound neutral, paragraphs 5 and 8 tread on Megaupload’s rights and impair its ability to access and use that digital evidence in defense of the civil and criminal cases—essentially they enjoin Megaupload from access to this data without any extraordinary showing having been made. Instead, those paragraphs should be edited, and a new paragraph 9 governing Megaupload’s access should be added. A proposed form of order is submitted herewith.

¹ *Warner Music Group Corp. v. Megaupload, Ltd.*, No. 1:14cv374-LO/IDD (E.D. Va. filed Apr. 10, 2014). Those Plaintiffs also seek a preservation order. (*Id.*, Dkt. No. 53.)

BACKGROUND AND RELATED PROCEEDINGS

The Criminal Action: Megaupload and the other defendants in this civil action have been indicted for criminal copyright infringement. *United States v. Kim Dotcom, et al.*, No. 1:12-cr-00003-LO (E.D. Va. filed Jan. 5, 2012) (“*Criminal Action*”).² The government’s theory is that Megaupload allegedly used cloud-storage websites and numerous servers to “reproduce[] and distribute[] copies of popular copyrighted content over the Internet without [the owner’s] authorization” while earning money from cloud users’ subscription fees and third-party advertising. (*Id.*, Doc. 34, *Superseding Indictment* ¶¶ 2-8.) The criminal charges and the claims asserted in this civil action (brought by alleged crime victims) allege similar underlying activities, and attempt to hold Megaupload civilly and criminally liable for the alleged infringing acts of the users. Megaupload contends that the criminal charges and civil claims lack merit.

The Servers and the Data: The primary servers allegedly used by Megaupload in the United States are the so-called “Carpathia Servers” and the Cogent Servers (which together the government calls the “Mega Servers”). In January 2012, the Government executed search warrants as to Defendants at numerous locations around the world, including at Carpathia’s server-hosting facility in Virginia and at Cogent’s facility in the District of Columbia.³ 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 the specific servers, the specific data, or the selection criteria. (*Criminal Action*, Dkt. No. 32, AUSA

² The Court may take judicial notice of court records and pleadings in related criminal cases. *See Colonial Penn Ins. Co. v. Coil*, 887 F.2d 1236, 1239-40 (4th Cir. 1989).

³ The DOJ also seized selected Megaupload data in the Netherlands at the Leaseweb facility, but the original data has been destroyed. Megaupload will be further seriously prejudiced if the data on the Cogent Servers also is destroyed because there is no other source for comparable data.

Prabhu Letter (Jan. 27, 2012).) At that time, the Government expressly disclaimed any “custody or control” over the Carpathia and Cogent servers:

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.”

(*Id.*) Yet, thereafter, Megaupload’s access to the data on those servers has been anything but an issue that Megaupload could resolve “directly with Cogent or Carpathia.”

Importantly, Carpathia confirmed that it owns only the servers, but has no interest in the data: “Carpathia does not own and cannot access the data, nor does it have any interest in the data stored on” its servers; rather “its interests are solely in the physical hardware itself.” (*Criminal Action*, Dkt. No. 39 at 2.) Similarly, Cogent claims no interest in the cached data, only the servers on which the data are stored. As the Internet service provider (“ISP”), however, Megaupload has a statutory interest in the data (and its users have ownership and privacy interests in the data that has been stored).⁴ Similarly, as a defendant in pending civil and criminal cases, it has an interest in accessing this digital evidence to disprove the claims and charges. Yet, Megaupload has not yet had a clear path to the data on either set of servers.⁵

When Megaupload tried to acquire the Carpathia Servers so as to gain access to the data, the Government objected to block the sale. (*Criminal Action*, Dkt. No. 39 at 3.) And the government continues to object to Megaupload’s acquisition of those servers *and* access to the

⁴ Megaupload’s statutory *interest* in this data as the ISP, as well as its statutory *duty* as the ISP to ensure the privacy of this data under the Stored Communications Act, have been explained in a brief previously filed in this action. (Dkt. No. 48, ¶ 8.) A copy of that brief will be submitted to chambers with this response.

⁵ Megaupload did have limited access to the Carpathia Servers in 2012 for a forensic analysis, not for digital evidence collection or assessment.

data thereon. (*Criminal Action*, Dkt. No. 223 at 4-5 & n.3.) While again disclaiming any “custody or control” over the Cogent Servers, the government also has objected to Megaupload’s access to the data cached on the Cogent Servers—baldly asserting that it contains “contraband” that cannot be turned over to counsel for Megaupload. (AUSA Prabhu’s Letter to Magistrate Judge Anderson, June 23, 2016.)⁶ Accordingly, despite claiming that ownership of and access to the data is a private matter between Megaupload, Carpathia, and Cogent, all three have been handcuffed by the government’s objections—the servers and data supposedly are not “in custody,” but neither are they “free to go.”⁷

ARGUMENT

Neither the government nor any party in the civil cases has filed a motion to enjoin Megaupload or preclude Megaload’s access to this data. Obviously, to obtain such extraordinary relief, the movant would have to make a substantial and detailed showing. None has been made. Yet, the government, merely by making bald assertions, and the Plaintiffs, through drafting legerdemain in the proposed preservation order, seek to bar Megaupload’s access to its own data. That is grossly unfair.

To be sure, Megaupload agrees that a preservation order is warranted. In extraordinary circumstances, like those now present, and prior to active discovery in a civil case, the Court has “inherent authority” to issue a “preservation order” that specific procedures be adopted to preserve specific evidence. *See The Pueblo of Laguna v. United States*, 60 Fed. Cl. 133, 135 (2004) (“courts have held that they have the inherent power to order that evidence be preserved and have, for good cause, required that specific procedures be adopted to ensure such

⁶ This letter was not publicly filed by the government, and so Megaupload will not file it now; however, Megaupload will deliver a copy to chambers with this brief.

⁷ The injustice of the government’s self-contradictory positions is explained in Megaupload’s prior brief (Dkt. No. 54), a copy of which will be provided with the chambers copy of this filing.

preservation”). When asked to exercise that inherent authority, however, the Court must act “with restraint and discretion,” and must require that the party “seeking a preservation order demonstrate that it is necessary and not unduly burdensome.” *Id.* at 137-38 (citations omitted). To meet this test, “the proponent ordinarily must show that absent a court order, there is significant risk that relevant evidence will be lost or destroyed—a burden often met by demonstrating that the [possessing] party has lost or destroyed evidence in the past or has inadequate retention procedures in place. More than that, the proponent must show that the particular steps to be adopted will be effective, but not overbroad—the court will neither lightly exercise its inherent power to protect evidence nor indulge in an exercise in futility.” *Id.* at 138 (citations omitted). Megaupload agrees that there is a “significant risk that relevant evidence will be lost or destroyed,” and that ample grounds for a preservation order exist; however, Megaupload disputes certain terms of the preservation order proposed by Plaintiff.

In particular, in Plaintiffs’ proposed order, paragraph 5 states

Once the drives and devices have been returned to Cogent’s custody and stored in Cogent’s facility, *no person* (other than Cogent personnel solely for the purpose of ensuring proper maintenance) *shall have access to those drives and devices, or to the data contained on those drives and devices, absent further order from this Court.*

(Dkt. No. 61-1 at 3, ¶ 5 (emphasis added).) That provision, as written, is tantamount to an injunction against Megaupload’s access to the data—barring even access for litigation purposes—without any extraordinary showing by Plaintiffs.

Paragraph 5 should be subject rewritten to be subject to the new paragraph 9 Megaupload proposes, and should read as follows (new language in **bold**):

Subject to paragraph 9 below, once the drives and devices have been returned to Cogent’s custody and stored in Cogent’s facility, no person (other than Cogent personnel solely for the purpose of ensuring proper maintenance) shall have access to those drives and devices, or to the data contained on those drives and devices, absent further order from this Court.

Only with these edits will Megaupload's be able to access this critical data, as needed, in the defense of these cases. Otherwise, Megaupload is enjoined from obtaining access to the data without the Court's permission, which is contrary to law.

Likewise, the second sentence of Plaintiff's paragraph 8 is not a neutral acknowledgment of (i) the indisputable interests of Megaupload, as the ISP, in the cached data on the Cogent Servers, and (ii) the indisputable procedural and constitutional rights of Megaupload as a civil litigant and criminal defendant to have reasonable access to this pivotal digital evidence—which is expected to include significant exculpatory evidence. Instead, that sentence purports to recognize the “position of the United States or any other Party that Megaupload should not be allowed access to such data.” If included as part of a court order, this sentence would mean that Megaupload must overcome some as-yet unproven assertions by the government, or as-yet unasserted objections by some “other Party,” before it can obtain any access to the digital evidence at the very heart of both the criminal and civil actions. That is grossly unfair and unwarranted.

Megaupload submits that the second sentence of paragraph 8 should be stricken. Instead, Megaupload must have reasonable access to this digital evidence and these servers. Megaupload submits that, when appropriate to its defense in the civil and criminal cases, it should be permitted to obtain access to this data, *for litigation purposes only*, simply by giving notice to the government and the civil plaintiffs. The government and the civil plaintiffs may then make any objection they have and can prove; but failing that, Megaupload should have full access to this digital evidence for use in the litigation.

Therefore, Megaupload submits that a new paragraph 9 should be inserted, reading as follows:

9. Megaupload may obtain access to this data, *for litigation purposes only*, by giving notice to the government and the civil plaintiffs, who must make any objection thereto within 14 days of the notice by filing a motion to preclude access. If no such motion is filed, Megaupload may have immediate access; however, if an such a motion is made, it shall be promptly submitted to the Court for decision, and Megaupload may have access only if and as permitted by the Court.

This process protects each party's interests without unduly burdening Megaupload's right to access this pivotal digital evidence, in which it has an interest as the ISP and as a litigant.

CONCLUSION

Megaupload respectfully submits that the Court should not enter Plaintiff's form of order, but should enter the form submitted herewith.

Dated: March 23, 2017

Respectfully submitted,

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

Ira P. Rothken (*pro hac vice*)
Jared R. Smith (*pro hac vice*)
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, Ltd.

CERTIFICATE OF SERVICE

I hereby certify that on March 23, 2017, the foregoing was filed and served electronically by the Court's CM/ECF system upon all registered users:

Kenneth L. Doroshow
JENNER & BLOCK LLP
1099 New York Ave., N.W.
Suite 900
Washington, D.C. 20001
Counsel for Plaintiffs

/s/ Craig C. Reilly
Craig C. Reilly, Esq. (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.