IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

UNITED STATES OF AMERICA,	)	
	)	The Honorable Liam O'Grady
Plaintiff,	)	
	)	Case No. 1:12-cr-00003-LO
v.	)	
	)	
KIM DOTCOM, *et al*.	)	
	)	
Defendants.	)	

MOTION OF KYLE GOODWIN TO UNSEAL SEARCH WARRANT MATERIALS & BRIEF IN SUPPORT

I. INTRODUCTION

Movant Kyle Goodwin lost access to his property—largely videos of high school sports events that he creates as his business—when the government executed search warrants for servers that housed his property and completed related seizures of the Megaupload service. That property and Mr. Goodwin's motion to have it returned are the subject of a recent order by this Court requesting briefing on the "suggested format and breadth" of a hearing under Fed. R. Crim. P. 41(g).

Pursuant to Mr. Goodwin's original motion, and in light of the upcoming briefing and decision on that motion, Mr. Goodwin now moves this Court to unseal the search and seizure warrants, applications, and all related judicially-filed material relating to the loss of his data ("warrant materials"), or, in the alternative, to unseal the warrant materials with only minimal redactions. Those materials, and the actions the government took under them, will not only be relevant to any Rule 41(g) inquiry, but will likely include evidence Mr. Goodwin will present as part of his ongoing efforts to have his property returned. The materials will also likely assist

other individuals who have lost access to their property due to the searches and seizure of Megaupload. They will also inform the general public about how the government has used its seizure power in this high-profile case, which has important implications for all users (and providers) of cloud computing services. Finally, because this case was initiated nine months ago and has already been the subject of extensive public litigation here and in New Zealand, the government cannot overcome the presumption in favor of access to judicial records.

II. FACTUAL BACKGROUND

Much of the procedural background, as it applies to Mr. Goodwin, is laid out in his brief in support of Carpathia Hosting's emergency motion and his own motion for return of his property. Dkt. No. 51 at 3-6, Dkt. No. 91. at 2-6. Of particular relevance, on January 19, 2012, this Court unsealed an indictment dated January 5. Indictment, Dkt. No. 1. Presumably pursuant to warrants and orders still under seal, the government seized 18 domain names and executed search warrants, effectively seizing the more than 1,000 servers owned by Carpathia Hosting, which Megaupload had leased and on which it most likely stored its customers' data. Dkt. No. 39 at 5; January 27 Letter from Jay V. Prabhu ("Prabhu Letter"), Dkt. No. 32. Moreover, the government, along with foreign law enforcement in New Zealand and elsewhere, also raided the homes of defendants, none of whom resides in the United States, and seized bank accounts, jewelry, cars, and other valuable goods. Dkt. No. 1 at 66-71**.** The government sought, and received, significant press attention for both the raids and the public indictment.

On January 27, the government filed the Prabhu Letter with this Court, stating that it had completed its execution of the warrants, that it no longer had any right to access Carpathia's servers, and that it no longer exercised control over the data. Dkt. No. 32. Fearing that the government's position meant that his property was to be destroyed, Mr. Goodwin filed a brief in

support of an emergency motion by Carpathia for a protective order surrounding the more than 1,000 servers and, when discussions between the parties fell apart, filed his own motion for return of property. Dkt. No. 51; Dkt. No. 91. The Court has not yet ruled on either motion, but importantly, during the hearing held on Mr. Goodwin's motion for return of property on June 28, 2012, the government conceded that during its discussions with Carpathia, it indicated that the company might incur potential liability if it reengaged the servers leased to Megaupload, even though the government also said it had relinquished control of those servers. According to Carpathia's counsel, after those discussions Carpathia did not reconnect the servers, since "we were not free to turn the servers back on." Carpathia also emphasized that data on the Megaupload servers *is* currently being restrained, since Carpathia cannot do anything with the data. Hearing on Motions at 17:22-18:18, U.S. v. Dotcom, (June 29, 2012) (No. 1:12-cr-3).

The day before the June 29, 2012, hearing before this Court, the High Court in New Zealand issued an order finding that related search warrants executed in New Zealand were invalid, and the resulting searches and seizures illegal. *See* Judgment of Winkelmann J (June 28, 2012) ("New Zealand Ruling"), attached as Exhibit A. Specifically, the New Zealand Court held that, among other things:

> The warrants were expressed to authorise the search for and seizure of very broad categories of items. These categories of times were defined in such a way that they would inevitably capture within them both relevant and irrelevant material. The Police acted on this authorisation. The warrants could not authorise seizure of irrelevant material, and are therefore invalid.

New Zealand Ruling at ¶144(b). The New Zealand Court also found:

> If the warrants had been adequately specific as to offence and scope of search, it may still have been appropriate for the issuing Judge to impose conditions. Conditions could have addressed the offsite sorting process, which was inevitable for the items taken away from the search sites. The conditions could have provided for the cloning of hard drives, the

> extraction of relevant material and the return to the plaintiffs of the original hard drives, or their clones.

Id. at ¶144(c).

The New Zealand Court also expressed grave concerns with the New Zealand authorities' lack of attention to the rights of third parties whose property may be affected by the seizures. *Id.* at ¶ 24 ("the applicants for the warrants did not set out proposed conditions as to how to deal with the property of third parties or other irrelevant items."). Likewise, the warrants failed to account for irrelevant evidence that would also be swept up in the broad searches and seizures. *Id.* at ¶ 56 (the "broadly drawn" categories in the warrants "would most likely store some irrelevant material, probably a large volume of irrelevant material, since the warrants were to be executed at domestic properties.").

Finally, the New Zealand Court was not convinced by the New Zealand authorities' argument that the sheer breadth of data made imposing limiting conditions on the warrants unfeasible, and specifically called out the U.S. authorities on whose behalf the seizure was done, holding that the "purpose of … sorting is to extract the relevant from the irrelevant, and it seems to me inevitable that the FBI should have been able to assist with that." *Id.* at ¶ 75.

Since the time the New Zealand court issued its ruling, the searches and seizures of Megaupload's property in that country have come under additional attack. Specifically, New Zealand Prime Minister John Key recently publicly apologized to Kim Dotcom for what he admits was illegal spying on Mr. Dotcom and others.[1] The details of the government's

[1] Adam Bennett and Claire Trevett, *PM Apologizes to Dotcom over "Basic Errors"*, NEW ZEALAND HERALD, Sept. 27, 2012 (available at http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10836884).

surveillance of Mr. Dotcom and other defendants in this case are now the subject of multiple public inquiries in New Zealand.[2]

III. LEGAL ANALYSIS

A. The Common Law Right Of Access Establishes A Presumption In Favor Of Access To Judicial Records And Documents.

The press and the public have a common law right of access to judicial documents. *Nixon v. Warner Communications, Inc.*, 435 U.S. 589 (1978). The "common law presumption in favor of access attaches to all 'judicial records and documents.'" *Stone v. Univ. of Md. Med. Sys. Corp.,* 855 F.2d 178, 180 (4th Cir. 1998) (Wilkonson, J.); *Va. Dept. of State Police v. Wash. Post,* 386 F 3d. 567, 575 (4th Cir. 2004). The Fourth Circuit has held that warrant affidavits fall squarely within this definition. *Balt. Sun Co. v. Goetz,* 886 F.2d 60, 64-65 (4th Cir.1989)

The Fourth Circuit has also specifically noted that the public's interest in access "may be magnified" "[i]n the context of the criminal justice system":

> Society has an understandable interest not only in the administration of criminal trials, but also in law enforcement systems and how well they work. The public has legitimate concerns about methods and techniques of police investigation: for example, whether they are outmoded or effective, and whether they are unnecessarily brutal or instead cognizant of suspects' rights.

Wash. Post Co. v. Hughes (In re Application & Affidavit for a Search Warrant), 923 F.2d 324, 330-31 (4th Cir. 1991). Put simply, the right of access is "fundamental to a democratic state." *United States v. Mitchell*, 551 F.2d 1252, 1258 (D.C. Cir. 1976), *rev'd on other grounds sub nom. Nixon v. Warner Communications*, 435 U.S. 589 (1978).

---

[2] *PM Doesn't Back Further Inquiries into Dotcom Spying*, RADIO NEW ZEALAND (Sept. 28, 2012), http://www.radionz.co.nz/news/political/116849/pm-doesn't-back-further-inquiries-into-dotcom-spying.

Openness in criminal cases "enhances both … basic fairness … and the appearance of fairness so essential to public confidence in the system," *Press-Enter. Co. v. Superior Court of California,* 464 U.S. 501, 508 (1984) (*Press-Enter. I*), as well as increasing the likelihood that the warrants issued in these types of cases involving seizures of digital third-party data are not overbroad, *Nixon,* 435 U.S. at 598. This is a particularly important point in criminal cases concerning cloud computing, where the norms for the scope of seizures are still being developed even as an ever-increasing percentage of personal and business activities are conducted online each year. In 2008, for instance, 69% of American Internet users had used a cloud computing service, either storing data online or using a web-based software application.[3]

The common law right of access establishes a presumption in favor of access to judicial records and documents. *See Nixon*, 435 U.S. at 602. Once the presumption attaches, as it does here, a court cannot simply seal documents or records indefinitely without considering countervailing factors. Rather, a court must "weigh[] the interests advanced by the parties in light of the public interest and the duty of the courts" to determine whether the documents should be sealed. *Id.* The government bears the burden of "'showing some significant interest that outweighs the presumption'" of access, and, to rebut the presumption, must demonstrate that "'countervailing interests heavily outweigh the public interests in access.'" *Va. Dep't of State Police v. Wash. Post*, 386 F.3d 567, 575 (4th Cir. 2004) (quoting *Rushford v. New Yorker Magazine, Inc.*, 846 F.2d 249, 253 (4th Cir. 1988)).

Nor can the government succeed in keeping the warrant materials sealed on a claim of a general need for secrecy concerning ongoing criminal investigations and law enforcement

[3] John B. Horrigan, *Data Memo, Use of Cloud Computing Applications and Services*, PEW INTERNET AND AMERICAN LIFE PROJECT (September 12, 2008) http://www.pewinternet.org/~/media/Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf.

methods. As the Fourth Circuit noted in *Va. Dep't of State Police*, 386 F.3d at 579, "not every release of information contained in an ongoing criminal investigation file will necessarily affect the integrity of the investigation," so "it is not enough simply to assert" a compelling government interest in the integrity of the investigation "without providing specific underlying reasons for the district court to understand how the integrity of the investigation reasonably could be affected by the release of such information." *See also Balt. Sun*, 886 F.2d at 65-66 (requiring that the sealing of search warrant affidavits be justified by more than just the conclusion that "the public interest in the investigation of crime" outweighs the media's interest in access). The government must demonstrate a specific, narrowly tailored need for sealing. *Id.*

B. Mr. Goodwin Has a Strong Interest in Access to the Warrant Materials.

Mr. Goodwin's strong interest in access to the warrant materials is self-evident. Since January 2012, he has diligently attempted to regain access to his property to which he was denied access without any showing of wrongdoing by him. To that end, he has a pending Rule 41(g) motion for return of property, for which this Court recently requested further briefing. As part of any hearing under Rule 41(g), Mr. Goodwin will need to investigate the government's actions surrounding the searches and seizures that occurred here. *See, e.g., Chaim v. U.S.,* 692 F. Supp.2d 461, 469 (D.N.J. 2010) (under Rule 41(g), courts should consider, among other things, "whether the Government displayed a callous disregard for the constitutional rights of the movant").

Mr. Goodwin's investigation—and proposal for a Rule 41(g) hearing—will be informed by the contents of the warrant materials. For instance, these materials will certainly assist him to learn what steps, if any, the government took to inform the court of the scope of its planned seizure and related execution of search warrants. They would also show any plan provided by the

government or the court in the warrant materials for minimization to protect innocent users before the seizure or to segregate the data after seizure. Federal judges increasingly impose detailed conditions prior to execution of computer searches. Orin S. Kerr, *Ex Ante Regulation of Computer Search & Seizure*, 96 Va. L. Rev. 1241, 1244 (2010). For example, Judge Kozinski in the Ninth Circuit has observed that if the government refuses to forswear the ability to retain or use data that should have been segregated initially, the judge "should order that the seizable and non-seizable data be separated by an independent third party under the supervision of the court, or deny the warrant altogether." *U.S. v. CDT,* 621 F. 3d 1162, 1178 (9th Cir. 2010) (Kozinski, J. concurring). Unsealing will allow Mr. Goodwin, as well as the general public, to learn which, if any, such conditions were undertaken in this case. .

Similarly, under the Fourth Amendment people have a right to be secure in their "papers" and "effects" against unreasonable searches and seizures. A person's "effects" may be the subject of Fourth Amendment protection even where there is no particular privacy or liberty interest. *See Altman v. City of High Point*, 330 F.3d 194 (4th Cir. 2003) (officers' destruction of plaintiffs' dogs constituted seizure under Fourth Amendment). A property seizure occurs when a governmental intrusion meaningfully interferes with an individual's possessory interest. *See U.S. v. Jacobsen*, 466 U.S. 109 (1984); *see generally U.S. v. Mitchell*, 565 F.3d 1347 (11th Cir. 2009) (unreasonable seizure occurred when target's computer hard drive was taken by police and held for 21 days). The Fourth Amendment analysis, in turn, requires the Court to determine whether the seizure was "reasonable." Gaining access to the materials that served as a basis for the government's seizure of his property can assist Mr. Goodwin and other innocent Megaupload users in determining whether the seizure was unreasonable.

C. The Public Interest Has a Weighty Interest in Access Where, as Here, the Sealed Documents are a Matter of Public Concern.

The public also has a strong interest in understanding the government process in executing search warrants on cloud computing servers that contain innocent third-party property.[4] Seizures of domain names, and resulting searches of related servers, are tools the government is using with increasing frequency in criminal copyright enforcement actions. For example, the federal government has reportedly seized more than 800 websites so far under its Operation in our Sites campaign.[5] The government has issued press releases and otherwise sought to publicize its efforts, obviously giving its own perspective on its actions.[6] Legislators, the media, and the public are vigorously debating the very issue of these domain name seizures and related searches, even as a large percentage of Americans continue to use cloud computing services. Access to judicial records would ensure a more accurate and informed public debate, rather than one informed merely by the government's press releases

---

[4] Mr. Goodwin can assert the public's right of access to the sealed materials. "The Supreme Court has made it plain that all persons seeking to inspect and copy judicial records stand on an equal footing, regardless of their motive for inspecting such records." *Leucadia, Inc. v. Applied Extrusino Techs., Inc.* 998 F.2d 157, 167-68 (3rd Circ. 1993).

[5] *See* Michael Berkens, *ICE Seizes 70 More Domains*, THE DOMAINS (July 12, 2012) http://www.thedomains.com/2012/07/12/ice-seizes-70-more-domains/ (discussing seizure of sites allegedl selling counterfeit goods from China); *ICE Seizes 300 More Sites; Can't Have People Watching Super Bowl Ads Without Permission*, TECHDIRT (Feb. 2, 2012, 1:26 PM), http://www.techdirt.com/articles/20120202/12374117639/ice-seizes-300-more-sites-cant-have-people-watching-super-bowl-ads-without-permission.shtml (discussing the seizure of more than 300 domains related to the Super Bowl); *Feds Seize 130+ Domain Names in Mass Crackdown*, TORRENTFREAK (Nov. 25, 2011) (discussing the seizure of more than 130 domains in anticipation of "Cyber Monday," which refers to the Monday after Thanksgiving on which consumers are persuaded to shop online); *Feds seize 82 domains accused of selling counterfeit goods*, ARS TECHNICA (Nov. 29, 2010 12:58 PM), http://arstechnica.com/web/news/2010/11/feds-seize-82-domains-selling-counterfeit-goods.ars (discussing the seizure of 82 domain names by the Department of Justice).

[6] *ICE-led IPR Center Seizes 70 Websites duping consumers into buying counterfeit merchandise*, ICE.GOV (July 12, 2012) http://www.ice.gov/news/releases/1207/120712washington.htm.

When determining whether the presumption of access is overcome, courts must weigh "the interests advanced by the parties in the light of the public interest and the duty of the courts." *Nixon*, 435 U.S. at 602. The public interest weighs particularly heavily in this case because "the public's right to know what the executive branch is about coalesces with the concomitant right of the citizenry to appraise the judicial branch." *F.T.C. v. Standard Fin. Mgmt. Corp.*, 830 F.2d 404, 410 (1st Cir. 1987); *see also Balt. Sun,,* 886 F. 2d at 66 (vacating the sealing of pre-indictment search warrant affidavits on the ground that sealing must be justified by more than just a finding that "the public interest in the investigation of crime" outweighs the media's interest in access).

In this case, providing access to judicial records about the government's searches of Carpathia's servers will help the public understand and meaningfully debate how government agencies are using their existing powers to seize domain names and cloud computing services to enforce copyright law and how the courts are handling their seizure requests. It will assist in the ongoing, robust discussions about whether such powers should be continued or changed. This is because documents concerning the specific legal actions that the government has already undertaken—and the courts' reactions to such actions—will provide an important and currently absent perspective on this matter. The public has a right to know about the legal steps that the government is taking to address this matter of intense national concern and how the courts are responding. Disclosure of the sealed documents would enable the public to evaluate the decisions of their elected officials and to reach their own determinations about the appropriateness of the government's actions.

The public also has a significant interest in ensuring that individuals' constitutional rights are not unnecessarily infringed. *See, e.g., Legend Night Club v. Miller,* 637 F.3d 291, 303 (4th

Cir. 2011) ("upholding constitutional rights is in the public interest") (citing *Giovani Carandolo, Ltd. v. Bason*, 303 F.3d 507, 521(4th Cir. 2002). Thus, the public interest in protecting the constitutional rights of both Mr. Goodwin and the likely millions of other innocent users of Megaupload whose property was seized along with his militates in favor of unsealing.

D. The Government No Longer Has an Interest in Keeping the Search Warrant Materials Under Seal.

As noted above, the law places the burden for continued justification for sealing on the government and it is plain that the government cannot meet that burden. First and foremost, the seizure and its targets are no secret, the indictment has issued, and the government itself has publicly stated, in a letter filed with this Court, that the "United States has completed execution of its search warrants" and "has no continuing right to access" the Carpathia servers in question. Prabhu Letter at 1. Moreover, the government also stated that it had "the understanding that the hosting companies [including Carpathia] may begin deleting the contents of the servers." *Id.* Thus, the government has finished with its searches and seizures, and its investigation has been made public through the issuance of the public indictment.

With the very public indictment, seizures and arrests of the principals of Megaupload, there can no longer be any need for secrecy based on fears of alerting the targets or potential witnesses, or the possible destruction of evidence or fleeing the jurisdiction. In addition, details of the searches and seizures in New Zealand have already been released publicly and are being debated internationally in the media. Thus, the government has no reasonable investigative basis for keeping the search warrant materials covering the servers in question under seal.

Moreover, the recent New Zealand Ruling signals numerous insufficiencies with the search warrants in that country, leaving open the reasonable question of whether similar infirmities exist in their U.S. counterparts. This is especially true because law enforcement

agencies in New Zealand and the United States were working together "informally" before the United States even requested any official assistance from New Zealand. New Zealand Ruling at ¶ 12. Given what appears to be the two governments' close-working (and "informal") relationship, Mr. Goodwin has even more reason to be concerned about potential infirmities in the search warrant materials whose execution led directly to the deprivation of his property.[7]

Finally, any legitimate government interests that exist can be accommodated through redactions or continued sealing on a document-by-document basis. Because the right to access is such a fundamental one, courts must first "consider less drastic alternatives to sealing," and may not seal documents completely or hide the very existence of a docket if it is possible to accommodate the government's interests by redacting specific information. *Stone*, 855 F.2d at 181; *see also Balt. Sun*, 886 F.2d at 66 (requiring that the judicial officer consider alternatives to sealing documents, such as "disclosing some of the documents or giving access to a redacted version"); *Moussaoui*, 65 F. App'x at 889 ("[S]ealing an entire document is inappropriate when selective redaction will adequately protect the interests involved"). In addition, before any motion to seal may be granted, notice must be provided to the public and must ordinarily be docketed "reasonably in advance of deciding the issue" to give the public an opportunity to object. *Stone*, 855 F.2d at 181; *see also* Civil L.R. 5; Crim. L.R. 49.

[7] It is likewise conceivable that the content of the warrants would provide detail about *how* the servers were searched and what was done with the data on them. This kind of information may help Mr. Goodwin and others like him understand the best way to actually retrieve their property.

IV. CONCLUSION

Because the government does not have a compelling interest in keeping the sealed documents under seal and cannot demonstrate that any interest heavily outweighs the public's interest in access, the documents should be unsealed and made publicly accessible.

For the reasons set forth above, Mr. Goodwin respectfully requests that the Court grant his motion to unseal the warrant materials in their entirety, or, in the alternative, to unseal the warrant materials with only minimal redactions.

Dated: October 22, 2012

Respectfully submitted,

/s/

John S. Davis
WILLIAMS MULLEN
200 So. 10th St.
Richmond, VA 23218
Telephone: (804) 420-6296
Facsimile: (804) 420-6507
Email: jsdavis@williamsmullen.com

Julie P. Samuels
Corynne McSherry
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
Email: julie@eff.org

Abraham D. Sofaer
THE HOOVER INSTITUTION
Stanford University
434 Galvez Mall
Stanford, CA 94305-6010
Telephone: (650) 723-1754
Email: asofaer@stanford.edu

Attorneys for Interested Party Kyle Goodwin

CERTIFICATE OF SERVICE

I hereby certify that on October 22, 2012, the foregoing was filed and served electronically by the Court's CM/ECF system upon all registered users, upon the following:

Jay V. Prabhu
Chief, Cybercrime Unit
Assistant United States Attorney
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314

Ed McNicholas
Sidley Austin LLP
1501 K Street, NW
Washington, DC 20005

Counsel to Megaupload Limited

Ira Rothken
Rothken Law Firm
3 Hamilton Landing, Suite 280
Novato, CA 94949

Counsel to Megaupload Limited

Stephen Fabrizio
Jenner & Block
1099 New York Avenue, NW
Suite 900
Washington, DC 20001

Counsel to Motion Picture Association of America

I declare under penalty of perjury that the foregoing is true and correct.

Dated: October 22, 2012

/s/
John S. Davis