

AO 108 (Rev. 06/09) Application for a Warrant to Seize Property Subject to Forfeiture

FILED

UNITED STATES DISTRICT COURT

for the Eastern District of Virginia

2012 JAN 13 P 2:19

In the Matter of the Seizure of)
(Briefly describe the property to be seized))
The Domain Name Megaupload.com)
and Nine Associated Domain Names)

CLERK US DISTRICT COURT ALEXANDRIA, VIRGINIA

Case No. 1:12-sw-34

UNDER SEAL

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Eastern District of Virginia is subject to forfeiture to the United States of America under 18 U.S.C. § 981(a)(1)(C)* (describe the property):

See Attachment A

* Such property is also subject to forfeiture to the United States of America under 18 U.S.C. §§ 982(a)(1), 1963(a), and 2323.

The application is based on these facts:

SEE ATTACHED AFFIDAVIT OF [REDACTED]

[X] Continued on the attached sheet.



Reviewed by AUSA Lindsay Kelly

Printed name and title

Sworn to before me and signed in my presence.

Date: 1/13/2012

[Handwritten signature]

Judge's signature

City and state: Alexandria, Virginia

Honorable Liam O'Grady, U.S. District Judge

Printed name and title

Attachment A

Domain Names:

MEGAWORLD.COM

MAGECLICK.COM

HDMEGAPORN.COM

MEGAVKDEO.COM

MEGAUPLOAD.COM

MEGAROTIC.COM

MEGACLICK.COM

MEGAVIDEO.COM

MEGAVIDEOCLIPS.COM

MEGAPORN.COM

FILED

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

2012 JAN 13 P 2:19

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

In the Matter of the Seizure of:)	
)	1:12SW34
The Domain Name <u>Megaupload.com</u> and Nine)	
Associated Domain Names)	UNDER SEAL

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, [REDACTED], being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. [REDACTED]

[REDACTED]. This affidavit is in connection with an investigation into the activities of KIM DOTCOM (also known as KIM SCHMITZ and KIM TIM JIM VESTOR) ("DOTCOM"), MEGAUPLOAD LIMITED, VESTOR LIMITED, FINN BATATO, JULIUS BENCKO ("BENCKO"), SVEN ECHTERNACH ("ECHTERNACH"), MATHIAS ORTMANN ("ORTMANN"), ANDRUS NOMM, and BRAM VAN DER KOLK ("VAN DER KOLK") (collectively, "DEFENDANTS"), who are believed to be involved in the operation and administration of several websites that reproduce and distribute infringing copies of copyrighted television programs, software, music, and motion pictures.

2. Your affiant is currently assigned to [REDACTED]

[REDACTED], Virginia, where your affiant's duties include the investigation of crimes involving the infringement of intellectual property rights, including violations of Title 18, United States Code, Section 2319 and Title 17, United States Code, Section 506. Your affiant has been employed as a [REDACTED]. Your affiant has directed and participated in investigations involving the use of computers and the Internet to commit

violations of fraud, intrusion, and intellectual property laws, and has received training in these areas. Your affiant has also received training and gained experience in, among other things, interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, intellectual property crimes, and computer-based crimes, computer evidence identification, seizure and processing.

3. Your affiant makes this affidavit in support of the government's application, pursuant to Title 21, United States Code, Section 853(f), Title 18, United States Code, Section 2323, Title 18, United States Code, Section 1963, Title 18, United States Code, Section 982(b)(1), and Title 18, United States Code, Section 981(b)(1) for a warrant to seize following domain names: MEGAWORLD.COM; MAGECLICK.COM; HDMEGAPORN.COM; MEGAVKDEO.COM; MEGAUPLOAD.COM; MEGAROTIC.COM; MEGACLICK.COM; MEGAVIDEO.COM; MEGAVIDEOCLIPS.COM; MEGAPORN.COM (collectively, "Subject Domain Names").

4. The procedure by which the government will seize the Subject Domain Names is described in Attachment A hereto and below.

5. As set forth below, there is probable cause to believe that the Subject Domain Names are subject to seizure and forfeiture as property constituting or derived from proceeds obtained directly or indirectly from, or used or intended to be used to facilitate the commission of criminal copyright infringement (17 U.S.C. § 506; 18 U.S.C. §§ 2319 and 2323); constituting or derived from proceeds traceable to conspiracy to commit criminal copyright infringement (18 U.S.C. §§ 371 and 981; 28 U.S.C. § 2461); involved in or traceable to conspiracy to commit money laundering (18 U.S.C. §§ 982 and 1956(h)); or constituting or derived from proceeds

obtained directly or indirectly from, or acquired or maintained in violation of, conspiracy to commit racketeering (18 U.S.C. §§ 1962, 1963). This affidavit does not set forth all of your affiant's knowledge about this matter, and is intended to provide sufficient information to support probable cause.

TECHNICAL BACKGROUND

6. Based on training and experience and information learned from others, your affiant is familiar with the following terms:

a. **Internet Protocol Address**: An Internet Protocol address ("IP address") is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address. The assignment of IP addresses to computers connected to the Internet is controlled by Internet Service Providers ("ISPs").

b. **Domain Name**: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond to a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

c. **Domain Name System**: The domain name system ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or

subdomain, of the domain on the right. The right-most label conveys the “top-level” domain. For example, the domain name “www.example.com” means that the computer assigned that name is in the “.com” top-level domain, and the “example” second-level domain.

d. Domain Name Registry: DNS servers are computers connected to the Internet that convert, or resolve, domain names into IP addresses. For each top-level domain (such as “.com”), there is a single company, called a “registry,” that determines which second-level domain resolves to which IP address. The registry for the “.com” top-level domain is VeriSign, Inc.

e. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. For example, the registrar used to register the Mageclick.com, Megavkdeo.com, HDMegaporn.com, and Megaworld.com domain names was GoDaddy.com. The individual or business that purchases, or registers, a domain name is called a “registrant.” Registrants control the IP address, and thus the computer, to which their domain name resolves. A registrant may easily move a domain name to another computer anywhere in the world. Typically a registrar will provide a registrant with the ability to change the IP address a particular domain name resolves to through an online interface.

PROBABLE CAUSE FOR SEIZURE AND FORFEITURE

7. In March 2010, [REDACTED] initiated an investigation of a worldwide criminal organization known as the “Mega Conspiracy,” which was believed to be hosting and distributing unauthorized copies of copyrighted works over the Internet. The Mega Conspiracy consists of a series of websites and services, including a video hosting and distribution service

located at the domain Megavideo.com; an adult video hosting service located at the domain Megaporn.com; a file hosting and distribution service located at the domain Megaupload.com; an advertising service associated with its other websites located at the domain Megaclick.com; and a number of associated websites. DEFENDANTS and others are members of the Mega Conspiracy, which has operated since at least September 2005 and is estimated to have caused harm to copyright holders in excess of \$500,000,000 and generated more than \$175,000,000 in revenue.

8. Once a user uploads a file to Megaupload.com, the system provides the user with a specific and unique Uniform Resource Locator (“URL link”) from which the file can be downloaded or viewed. If a video file is uploaded, an individual can use the provided URL link to redirect others to the related website Megavideo.com to view the file via the website’s Flash video player. Users can also embed the Flash video player from Megavideo.com into another website to display the video file there. Megaupload.com supports a vast landscape of websites offering the Megaupload.com-provided URL links to view unauthorized copies of copyrighted motion pictures and television programs that are being hosted on servers controlled by the Mega Conspiracy. Once a video has been viewed, a user also has the ability to download and save the video to his computer.

9. Paragraph 18 of the Indictment, which your affiant has reviewed and believes to be accurate and consistent with the investigation, alleges that, before any video can be viewed on Megavideo.com, the user must view an advertisement. Originally, the Mega Conspiracy had contracted with companies such as adBrite, Inc., Google AdSense, and PartyGaming plc for Internet advertising. Currently, the Mega Conspiracy’s own advertising website,

Megaclick.com, is used to set up advertising campaigns on all the Mega Conspiracy websites.

The high traffic volume on the Mega Conspiracy websites allows the Mega Conspiracy to charge advertisers up-front and at a higher rate than would be achieved by the percentage-per-click methodology used by other popular Internet advertising companies. The popularity of the infringing content on the Mega Conspiracy websites has generated more than \$25 million in online advertising revenues.

10. Paragraph 9 of the Indictment alleges that, in addition to displaying online advertisements, the download pages on Megaupload.com are designed to increase premium subscriptions. All non-premium users are encouraged to buy a premium subscription to decrease wait and download times, which can be at least an hour for popular content (and, for some periods of time, these non-premium users have been ineligible to download files over a certain size). As a result, non-premium users are repeatedly asked by the Mega Conspiracy to pay for more and faster access to content on Megaupload.com.

11. Using an undercover computer, [REDACTED] observed how a visitor may view content hosted on Megaupload.com. For example, on November 20, 2011, [REDACTED] observed the copyrighted motion picture *Zack and Miri Make a Porno*, which was released in 2008 by The Weinstein Company, on the website Megavideo.com. When the file was selected, the URL link redirected to www.megavideo.com/?v=REYCBLNF and a file entitled “[Película] Zack and Miri Make a Porno VOSE” was streamed. The same day, [REDACTED] located the copyrighted motion picture *The Twilight Saga: Breaking Dawn - Part 1* on the website www.peliculasyonkis.com. When selected, the URL link redirected to www.megavideo.com/?s=seriesyonkis&v=

HY01ZGSR, where [REDACTED] viewed a camcorded version of the copyrighted motion picture, which had been released in United States theaters only two days prior, on November 18, 2011.

12. Paragraph 10 of the Indictment alleges that the content available from Megaupload.com is not searchable on the website, which allows the Mega Conspiracy to conceal the scope of its infringement. Instead of hosting a search function on its own site, the Mega Conspiracy business model purposefully relies on thousands of third party “linking” sites, which contain user-generated postings of links created by Megaupload.com (as well as those created by other Mega Conspiracy websites, including Megavideo.com and Megaporn.com). While the Mega Conspiracy may not operate these third party sites, the Mega Conspiracy did provide financial incentives for premium users to post links on linking sites through the “Uploader Rewards” program, which ensured widespread distribution of Megaupload.com links throughout the Internet and an inventory of popular content on servers controlled by the Mega Conspiracy. These linking sites, which are usually well organized, promote and direct users to Mega Conspiracy download pages that allow the reproduction and distribution of infringing copies of copyrighted works.

13. Paragraph 14 of the Indictment alleges that, in contrast to the public who is required to significantly rely on third party indexes, members of the Mega Conspiracy have full access to the listings of actual files that are stored on servers they control (as well as the Megaupload.com- and Megavideo.com- and Megaporn.com-generated links to those files). Conspirators have searched the internal database in order to directly access copyright-infringing content on servers controlled by the Mega Conspiracy.

14. Paragraph 19 of the Indictment alleges that, like Megaupload.com, Megavideo.com conceals many of the infringing copies of popular copyrighted videos that are available on and distributed by the website. Megavideo.com does purport to provide both browse and search functions, but any user's search on Megavideo.com for a full length copyrighted video (which can be downloaded from a Mega Conspiracy-controlled server somewhere in the world) will not produce any results. Similarly, browsing the front page of Megavideo.com does not show any obviously infringing copies of any copyrighted works; instead, the front page contains videos of news stories, user-generated videos, and general Internet videos in a manner substantially similar to Youtube.com. Browsing the most-viewed videos in the Entertainment category on Megavideo.com, however, has at times revealed a number of infringing copies of copyrighted works that are available from Mega Conspiracy-controlled servers and are amongst the most viewed materials being offered.

15. The Mega Conspiracy uses e-mail addresses with the extension @megaupload.com in the operation of the Megaupload.com website. [REDACTED] e-mail account megaupload.support@gmail.com revealed the e-mail address abuse@megaupload.com has received and continues to receive thousands of DMCA infringement notices from copyright holders, including but not limited to Warner Bros. Entertainment Inc., Sony Music Entertainment Inc., and the Business Software Alliance. The e-mails provided notice of the existence of unauthorized copies of copyrighted motion pictures, television shows, software, literature, and music on servers controlled by the Mega Conspiracy. The notice e-mails contained the URL links to the locations on Megaupload.com where the infringing copies of copyrighted works resided. [REDACTED] review of other e-mails has

shown that the Mega Conspiracy operators are willfully violating copyright law by ignoring notices of selected infringing content, and are actually uploading infringing content themselves to Mega Conspiracy websites.

16. Using publicly available software that can detect the IP addresses of data incoming to the undercover computer, [REDACTED] was able to determine that the copyrighted content hosted on Megaupload.com was being downloaded from computers assigned IP addresses held by three commercial Internet hosting service companies: Carpathia Hosting, headquartered in Dulles, Virginia, with datacenters in Ashburn, Virginia, both of which are located in the Eastern District of Virginia; Cogent Communications, headquartered in Washington, D.C., with datacenters in Washington, D.C. and France; and Leaseweb in the Netherlands. Each of these Internet hosting service companies leases high-speed computer server space and Internet connectivity to the public.

17. On or about June 24, 2010, members of the Mega Conspiracy were informed, pursuant to a criminal search warrant from the U.S. District Court for the Eastern District of Virginia, that thirty-nine infringing copies of copyrighted motion pictures were present on their leased servers at Carpathia Hosting, a hosting company headquartered in the Eastern District of Virginia. A member of the Mega Conspiracy informed several of his co-conspirators at that time that he located the named files using internal searches of the Mega Conspiracy's systems. As of November 18, 2011, thirty-six of the thirty-nine infringing copies of copyrighted motion pictures were still being stored on servers controlled by the Mega Conspiracy.

18. In addition to Megaupload.com, Megavideo.com, and Megaclick.com, other websites created and domains owned by the Mega Conspiracy include: Megaworld.com;

Megastuff.co; Megaclicks.co; Megastuff.info; Megaclicks.org; Megaworld.mobi; Megastuff.org; Megaclck.us; Mageclick.com; HDmegaporn.com; Megaporn.com; Megavkdeo.com; Megarotic.com; and Megavideoclips.com. At least two of these additional sites have also hosted infringing copies of copyrighted works. The websites and services, as well as the domains themselves, have been facilitated and promoted by illicit proceeds from the operations of Megaupload.com, Megavideo.com, and Megaclck.com.

THE SUBJECT DOMAIN NAMES

19. [REDACTED] ORTMANN registered three of the Subject Domain Names to registrant MEGAUPLOAD LIMITED ("MUL") as follows:

Megaclck.com, on or around January 4, 2004;

Megaupload.com, on or around March 21, 2005;

Megavideoclips.com, on or around July 24, 2005.

MUL is a registered company in Hong Kong with company registry number 0835149.

MUL has a number of bank accounts in Hong Kong that have been used to facilitate the operations of the Mega Conspiracy. Until August 2011, DOTCOM held the title of Chief Executive Officer of MUL and owned, through VESTOR LIMITED, approximately 68% of the shares of MUL. The remaining shares of MUL are owned by ORTMANN, BENCKO, VAN DER KOLK, ECHTERNACH, and a 1% investor in Hong Kong. Since August 2011, DOTCOM has held the title of Chief Innovation Officer of MUL.

20. [REDACTED] ORTMANN registered the Megavideo.com domain on or around November 13, 2000, to registrant "Megavideo Limited" in Hong Kong. [REDACTED]

[REDACTED] on or about May 20, 2006, DOTCOM registered the company Megavideo Limited in Hong Kong with company registry number 1046619. The company director is listed as KIM TIM JIM VESTOR (a known alias of DOTCOM), and Megamedia Limited is listed as the sole shareholder. Documents [REDACTED] [REDACTED] for Megamedia Limited list KIM TIM JIM VESTOR as the company director, and VESTOR LIMITED as the sole shareholder.

21. [REDACTED] ORTMANN registered the Megarotic.com domain on or around February 9, 2006, to registrant "Megarotic Limited." Megarotic Limited shares an address and telephone number with Megavideo Limited. Moreover,

[REDACTED]
[REDACTED], on or about May 20, 2006, DOTCOM registered the company Megarotic Limited in Hong Kong with company registry number 1046616. The company director is listed as DOTCOM, and Megamedia Limited is listed as the sole shareholder.

22. A search of publicly available WHOIS domain name registration records revealed that the Megaporn.com domain was registered on or about November 9, 1999. The registrant was listed as "Megarotic Limited" in Hong Kong, with the same address and telephone number listed for the Megarotic.com domain.

23. [REDACTED] the HDMegaporn.com domain was registered on or about June 18, 2010, under shopper ID 39841112 with login name "megamanager." The name of the customer is listed as "Administrator" of Megamedia Ltd. in Hong Kong. The

customer's contact information lists the same address and telephone number as listed for the Megarotic.com and Megaporn.com domains. However, the registrant of the HDMegaporn.com domain concealed his name and contact information from public view through the use of a domain registration privacy service called Domains by Proxy, Inc.

24. [REDACTED] the Megaworld.com domain was registered on or about March 28, 2000. The registrant and account holder was indicated to be Megamedia Ltd, in Hong Kong.

25. [REDACTED] the Mageclick.com domain was registered on or about November 29, 2010. The registrant and account holder was indicated to be "Domain Administrator" at Megamedia Ltd, in Hong Kong.

26. [REDACTED]
[REDACTED] on or about May 20, 2006, DOTCOM registered the company Megamedia Limited in Hong Kong with company registry number 1046613. The company director is listed as KIM TIM JIM VESTOR (a known alias of DOTCOM), with Finland passport no. [REDACTED], and VESTOR LIMITED is listed as the sole shareholder.

27. [REDACTED] the Megavkdeo.com domain was registered on or about December 31, 2008, by ECHTERNACH, using a company name and e-mail address known to be associated with ECHTERNACH.

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

28. Title 18, United States Code, Section 2323(a)(1)(A) and (B) and 2323(b) provide, in relevant part, that any property used, or intended to be used to commit or facilitate criminal

copyright infringement, or constituting or derived from proceeds obtained directly or indirectly from the commission of criminal copyright infringement, are subject to both civil and criminal forfeiture. Title 18, United States Code, Section 2323(b)(2) authorizes the use of procedures set forth in Title 21, United States Code, Section 853 for the seizure of property subject to criminal forfeiture.

29. Title 18, United States Code, Sections 981(a)(1) and 982(a)(1) provide that a defendant who is convicted of money laundering shall forfeit to the United States “any property involved in the offense, or any property traceable to such property. Title 18, United States Code, Section 982(b)(1) authorizes the use of procedures set forth in Title 21, United States Code, Section 853 for the seizure of property subject to criminal forfeiture.

30. Where there is probable cause to believe that the property to be seized is subject to forfeiture and that an order pursuant to Title 21, United States Code, Section 853(e) may not be sufficient to assure its availability for forfeiture, a district court may issue a warrant authorizing the seizure of such property. 21 U.S.C. § 853(f). Section 853(f) provides that:

The Government may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant. If the court determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that an order under subsection (e) may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property.

A seizure warrant issued under Title 21, United States Code, Section 853(f) has nationwide scope. 21 U.S.C. § 853(l).

31. In addition, Title 18, United States Code, Section 1963(a) provides that any defendant who is convicted of racketeering activity shall forfeit to the United States any property constituting, or derived from, any proceeds which the person obtained, directly or indirectly, from the racketeering activity. Title 18, United States Code, Section 1963(d)(1) provides that:

Upon application of the United States, the court may enter a restraining order or injunction, require the execution of a satisfactory performance bond, or take any other action to preserve the availability of property described in subsection (a) for forfeiture under this section—

(A) upon the filing of an indictment or information charging a violation of section 1962 of this chapter and alleging that the property with respect to which the order is sought would, in the event of conviction, be subject to forfeiture under this section

A seizure warrant issued under Title 21, United States Code, Section 1963(d) has nationwide scope. 18 U.S.C. § 1963(j).

32. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the Subject Domain Names for forfeiture. By seizing the Subject Domain Names and redirecting them to another website, the United States will prevent supporters of the Mega Conspiracy or third parties from redirecting the Subject Domain Names to servers elsewhere in the world, and thus using them to commit additional crimes. Furthermore, seizure of the Subject Domain Names will prevent visitors from continuing to access the websites located at the Subject Domain Names.

33. Title 18, United States Code, Section 2319(a)(2) provides that the procedures set forth in Chapter 46 of Title 18 (18 U.S.C. § 981, et seq.) shall extend to civil forfeitures under Section 2323(a). Title 18, United States Code, Section 981(b)(1) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause. Title 18, United

States Code, Section 981(b)(3) permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed and may be executed in any district in which the property is found.

34. As set forth above, there is probable cause to believe that the Subject Domain Names are subject to both civil and criminal forfeiture because they were used in the commission of criminal copyright infringement, conspiracy to commit criminal copyright infringement, conspiracy to commit racketeering, and conspiracy to commit money laundering.

SEIZURE PROCEDURE

35. As detailed in Attachment A, upon execution of the seizure warrant, the registry for the top-level domain shall be directed to restrain and lock the Subject Domain Names pending transfer of all right, title, and interest in the Subject Domain Names to the United States upon completion of forfeiture proceedings, to ensure that changes to the Subject Domain Names cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI.

36. In addition, upon seizure of the Subject Domain Names, the registry for the top-level domain will be directed to point the Subject Domain Names to IP addresses controlled by the United States, which will display a web page providing public notice of the website seizure.

37. The domain name registrars also maintain certain records relating to the owner of each domain name for which it is the top-level registry, including the Subject Domain Names (the "Domain Name Records"). Certain of these records are available to the public through a "Whois" lookup through a web browser, among other means. At the time the Subject Domain Names are seized, the registrars will be directed to change the "Technical Contact" and

“Administrative Contact” fields of the Domain Name Records for the Subject Domain Names to contact information relating to FBI to reflect the fact that the Subject Domain Names have been seized; and to change the name server fields of the Domain Name Records to effect the forgoing changes. All other fields will be changed so that they do not reflect any individual or entity.

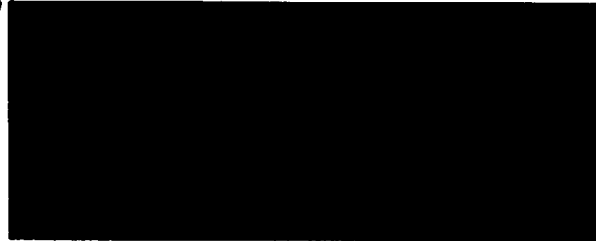
38. Upon completion of forfeiture proceedings, all Domain Name Records for the Subject Domain Names maintained by the top-level registry and the domain name registrars will be changed to reflect the transfer of ownership to the United States.

CONCLUSION

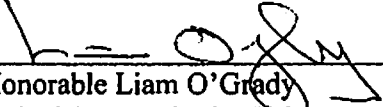
39. Based on the information contained in the Indictment and this affidavit there is probable cause to believe that the Subject Domain Names are subject to seizure and forfeiture as property constituting or derived from proceeds obtained directly or indirectly from, or used or intended to be used to facilitate, the commission of criminal copyright infringement (17 U.S.C. § 506; 18 U.S.C. §§ 2319 and 2323); constituting or derived from proceeds traceable to conspiracy to commit criminal copyright infringement (18 U.S.C. §§ 371 and 981; 28 U.S.C. § 2461); involved in or traceable to the conspiracy to commit money laundering (18 U.S.C. §§ 982 and 1956(h)); or constituting or derived from proceeds obtained directly or indirectly from, or acquired in maintained in violation of, a conspiracy to commit racketeering (18 U.S.C. §§ 1962 and 1963).

Accordingly, it is requested that a seizure warrant be issued for the Subject Domain Names.

FURTHER THIS AFFIANT SAYETH NOT



Subscribed to and sworn before me on this 13th day of January, 2012.



Honorable Liam O'Grady
United States District Judge

Submitted by Lindsay A. Kelly and Jay V. Prabhu
Assistant United States Attorneys

ATTACHMENT A

I. Seizure Procedure

A. The seizure warrant will be presented in person or transmitted via facsimile or email to personnel of the domain name registry listed in Section II (“Subject Registry”) and the domain name registrars listed in Section III (“Subject Registrars”) who will be directed, for the domain name listed in Section IV (“Subject Domain Names”) for which it serves as the top-level domain registry, to make any changes necessary to restrain and lock the Subject Domain Names pending transfer of all rights, title, and interest in the Subject Domain Names to the United States upon completion of forfeiture proceedings.

B. Upon seizure of the Subject Domain Names, the Subject Registry shall take all steps necessary to restrain and lock the domain at the registry level to ensure that changes to the Subject Domain Names cannot be made absent a court order or, if forfeited to the United States government, without prior consultation with FBI.

C. The Subject Registry shall point the Subject Domain Names to [REDACTED] and [REDACTED] at which the Government will display a web page with the following notice:

This domain name associated with the website Megaupload.com has been seized pursuant to an order issued by the U.S. District Court for the Eastern District of Virginia.

*An indictment has been returned by a grand jury in Alexandria, Virginia, charging several individuals and entities allegedly involved in the operation of Megaupload.com and related websites with the following federal crimes:
Conspiracy to Commit Racketeering (18 U.S.C. § 1962(d)),
Conspiracy to Commit Copyright Infringement (18 U.S.C. § 371),
Conspiracy to Commit Money Laundering (18 U.S.C. § 1956(h)), and
Criminal Copyright Infringement (18 U.S.C. §§ 2, 2319; 17 U.S.C. § 506).*

The case is being prosecuted by the U.S. Attorney's Office for the Eastern District of Virginia and the U.S. Department of Justice's Computer Crime and Intellectual Property Section.

D. Upon seizure of the Subject Domain Names, the Subject Registrars shall modify any records, databases, tables, or documents that are used by the Subject Registrars to identify the owner of the Subject Domain Names to reflect the seizure of the Subject Domain Names. These changes relate to the following records, if they exist:

1. The "Technical Contact" and "Administrative Contact" fields will reflect the following information:
 - a) Name: Federal Bureau of Investigation
 - b) Address: 935 Pennsylvania Ave
Washington, DC 20535
 - c) Country: USA
 - d) Telephone: 202-324-3000
 - e) Email: IPR@ic.fbi.gov
2. Any remaining fields will be changed so they do not reflect any individual or entity.

II. Subject Registry

VeriSign, Inc.
21355 Ridgetop Circle
Dulles, VA 20166

III. Subject Registrars

GoDaddy.com
14455 N. Hayden Rd., Ste. 226
Scottsdale, AZ 85260

Dotster, Inc.
8100 NE Parkway Drive, Suite 300
Vancouver, WA 98662

IV. Subject Domain Names

MEGAWORLD.COM

MAGECLICK.COM

HDMEGAPORN.COM

MEGAVKDEO.COM

MEGAUPLOAD.COM

MEGAROTIC.COM

MEGACLICK.COM

MEGAVIDEO.COM

MEGAVIDEOCLIPS.COM

MEGAPORN.COM

AO 109 (Rev. 12/09) Warrant to Seize Property Subject to Forfeiture

FILED

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

2012 JAN 13 P 2:19

In the Matter of the Seizure of
(Briefly describe the property to be seized)
The Domain Name Megaupload.com
and Nine Associated Domain Names

)
)
)
)
)

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

Case No. 1:12-sw-34

UNDER SEAL

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the Eastern District of Virginia be seized as being subject to forfeiture to the United States of America. The property is described as follows:

See Attachment A

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property on or before 1-27-2012
(not to exceed 14 days)

in the daytime – 6:00 a.m. to 10:00 p.m.

at any time in the day or night, as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to

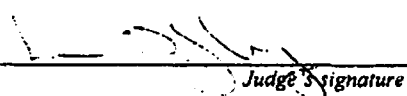
Honorable Liam O'Grady, U.S. District Judge

(name)

I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) for _____ days (not to exceed 30).

until, the facts justifying, the later specific date of _____

Date and time issued: 1/13/2012


Judge's signature

City and state: Alexandria, Virginia

The Honorable Liam O'Grady, U.S. District Judge

Printed name and title

FILED

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

In the Matter of the Seizure of:)
Case No. 1:12-sw- 34)
The Domain Name Megaupload.com and)
Nine Associated Domain Names) UNDER SEAL

2012 JAN 13 P 2:19
CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

**GOVERNMENT'S MOTION TO SEAL SEIZURE WARRANT
PURSUANT TO LOCAL RULE 49(B)**


The United States, through undersigned counsel, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, now asks for an Order to Seal the seizure warrant, the application for seizure warrant, and the affidavit in support of the seizure warrant, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal these documents.

I. REASONS FOR SEALING (See Local Rule 49(B)(1))

1. The Indictment, and arrest warrants, charging nine defendants with various crimes stemming from their involvement in a worldwide criminal enterprise related to Megaupload.com is under seal. [REDACTED]

2. While it is anticipated that the Indictment will be unsealed shortly after this seizure warrant is served, premature disclosure of the specific details of this criminal case [REDACTED]

[REDACTED]



3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. THE GOVERNING LAW (See Local Rule 49(B)(2))

4. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. Media General Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4th Cir. 2005); In re Washington Post Company v. Hughes, 923 F.2d 324, 326 (4th Cir. 1991). “But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is ‘essential to preserve higher values’ and ‘narrowly tailored to serve that interest.’” Media General Operations, 417 F.3d at 429 (citations omitted); see also In re Knight Pub. Co., 743 F.2d 231, 235 (4th Cir. 1984) (“[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public’s right of access is outweighed by competing interests”). Sealing search and seizure warrants and their accompanying affidavits and application is within the discretionary powers of a judicial officer where, among other things, an “‘affidavit contain[s] sensitive details of an ongoing investigation’ and it is ‘clear and apparent from the affidavits that any disclosure of the information there would hamper’ th[e] ongoing investigation.” Media General Operations 417 F.3d at 430 (citations omitted); see also In re Search Warrant for Matter of Eye Care Physicians of America, 100 F.3d 514, 518 (7th Cir. 1996).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. Ashcraft v. Conoco, Inc., 218 F.3d 288, 302 (4th Cir. 2000).

6. However, in the specific context of a search and seizure warrant, the Fourth Circuit has cautioned that “the opportunity to object” cannot “arise prior to the entry of a sealing order when a search warrant has not been executed.” Media General Operations, 417 F.3d at 429. “A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant.” Id.; see also Franks v. Delaware, 438 U.S. 154, 169 (1978). Accordingly, “the notice requirement is fulfilled by docketing ‘the order sealing the documents,’ which gives interested parties the opportunity to object after the execution of the search warrants.” Media General Operations, 417 F.3d at 430 (quoting Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989)); see also Local Rule 49(B) (“Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.”).

7. As to the requirement of a court’s consideration of alternatives, the Fourth Circuit counsels that, “[i]f a judicial officer determines that full public access is not appropriate, she ‘must consider alternatives to sealing the documents,’ which may include giving the public access to some of the documents or releasing a redacted version of the documents that are the subject to the government’s motion to seal.” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 66).

8. Finally, regarding the requirement of specific findings, the Fourth Circuit's precedents state that, "in entering a sealing order, a 'judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears creditable,'" Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 65), so long as the ultimate "decision to seal the papers" is "made by the judicial officer," Goetz, 886 F.2d at 65. "Moreover, if appropriate, the government's submission and the [judicial] officer's reason for sealing the documents can be filed under seal." Goetz, 886 F.2d at 65; see also In re Washington Post Co., 807 F.2d 383, 391 (4th Cir. 1986) ("if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal").

III. PERIOD OF TIME GOVERNMENT SEEKS TO HAVE MATTER REMAIN UNDER SEAL (See Local Rule 49(B)(3))

9. Pursuant to Local Rule 49(B)(3), the seizure warrant, the application for a seizure warrant, and the affidavit will remain sealed until the need to maintain the confidentiality of the these documents expires and the United States moves to unseal these documents.

WHEREFORE, the United States respectfully requests that the seizure warrant, application for seizure warrant, affidavit in support of the seizure warrant, and this Motion to Seal and proposed Order be sealed until further Order of the Court. Notwithstanding this request, the United States asks to provide copies as necessary to execute the seizure warrant.

Respectfully submitted,

Neil H. MacBride
United States Attorney

By: 
Lindsay A. Kelly
Assistant United States Attorney

AO 109 (Rev. 12/09) Warrant to Seize Property Subject to Forfeiture

FILED

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

2012 JAN 13 P 2:19

In the Matter of the Seizure of
(Briefly describe the property to be seized)

The Domain Name Megaclick.us

)
)
)
)
)

Case No. 1:12-sw-35

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

UNDER SEAL

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the Eastern District of Virginia be seized as being subject to forfeiture to the United States of America. The property is described as follows:

The Domain Name Megaclick.us

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property on or before Jan 13 2012
(not to exceed 14 days)

in the daytime – 6:00 a.m. to 10:00 p.m.

at any time in the day or night, as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to

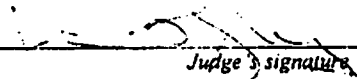
Honorable Liam O'Grady, U.S. District Judge

(name)

I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)* for days *(not to exceed 30)*.

until, the facts justifying, the later specific date of _____.

Date and time issued: 1/13/2012


Judge's signature

City and state: Alexandria, Virginia

The Honorable Liam O'Grady, U.S. District Judge

Printed name and title

AO 108 (Rev. 06/09) Application for a Warrant to Seize Property Subject to Forfeiture

FILED

UNITED STATES DISTRICT COURT

for the Eastern District of Virginia

2012 JAN 13 P 2: 18

CLERK US DISTRICT COURT ALEXANDRIA, VIRGINIA

In the Matter of the Seizure of) (Briefly describe the property to be seized)) The Domain Name Megaclick.us)))

Case No. 1:12-sw-35

UNDER SEAL

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Eastern District of Virginia is subject to forfeiture to the United States of America under 18 U.S.C. § 981(a)(1)(C)* (describe the property):

The Domain Name Megaclick.us

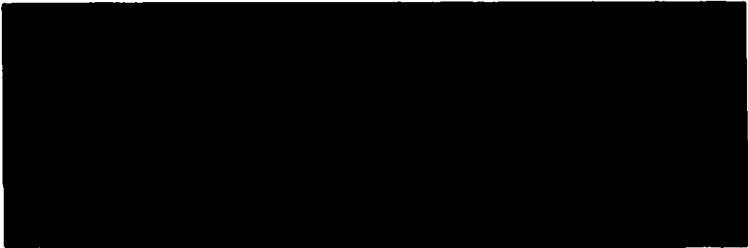
* Such property is also subject to forfeiture to the United States of America under 18 U.S.C. §§ 982(a)(1), 1963(a), and 2323.

The application is based on these facts:

SEE ATTACHED AFFIDAVIT OF [REDACTED]

Continued on the attached sheet.

Reviewed by AUSA Lindsay Kelly



Printed name and title

Sworn to before me and signed in my presence.

Date: 1/13/2012

[Handwritten signature] Judge's signature

City and state: Alexandria, Virginia

Honorable Liam O'Grady, U.S. District Judge

Printed name and title

FILED

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

In the Matter of the Seizure of:

The Domain Name Megaclick.us

)
)
)

1:12SW35

UNDER SEAL

2012 JAN 13 P 2: 18

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, [REDACTED], being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. Your affiant is a [REDACTED]

[REDACTED]. This affidavit is in connection with an investigation into the activities of KIM DOTCOM (also known as KIM SCHMITZ and KIM TIM JIM VESTOR) ("DOTCOM"), MEGAUPLOAD LIMITED, VESTOR LIMITED, FINN BATATO, JULIUS BENCKO ("BENCKO"), SVEN ECHTERNACH ("ECHTERNACH"), MATHIAS ORTMANN ("ORTMANN"), ANDRUS NOMM, and BRAM VAN DER KOLK ("VAN DER KOLK") (collectively, "DEFENDANTS"), who are believed to be involved in the operation and administration of several websites that reproduce and distribute infringing copies of copyrighted television programs, software, music, and motion pictures.

2. Your affiant is currently assigned to [REDACTED]

[REDACTED], where your affiant's duties include the investigation of crimes involving the infringement of intellectual property rights, including violations of Title 18, United States Code, Section 2319 and Title 17, United States Code, Section 506. Your affiant has been employed as a [REDACTED]. Your affiant has directed and participated in investigations involving the use of computers and

the Internet to commit violations of fraud, intrusion, and intellectual property laws, and has received training in these areas. Your affiant has also received training and gained experience in, among other things, interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, intellectual property crimes, and computer-based crimes, computer evidence identification, seizure and processing.

3. Your affiant makes this affidavit in support of the government's application, pursuant to Title 21, United States Code, Section 853(f), Title 18, United States Code, Section 2323, Title 18, United States Code, Section 1963, Title 18, United States Code, Section 982(b)(1), and Title 18, United States Code, Section 981(b)(1) for a warrant to seize the domain name Megaclick.us (hereinafter "Subject Domain Name").

4. The procedure by which the government will seize the Subject Domain Name is described in Attachment A hereto and below.

5. As set forth below, there is probable cause to believe that the Subject Domain Name are subject to seizure and forfeiture as property constituting or derived from proceeds obtained directly or indirectly from, or used or intended to be used to facilitate the commission of criminal copyright infringement (17 U.S.C. § 506; 18 U.S.C. §§ 2319 and 2323); constituting or derived from proceeds traceable to conspiracy to commit criminal copyright infringement (18 U.S.C. §§ 371 and 981; 28 U.S.C. § 2461); involved in or traceable to conspiracy to commit money laundering (18 U.S.C. §§ 982 and 1956(h)); or constituting or derived from proceeds obtained directly or indirectly from, or acquired or maintained in violation of, conspiracy to commit racketeering (18 U.S.C. §§ 1962, 1963).

This affidavit does not set forth all of your affiant's knowledge about this matter, and is intended to provide sufficient information to support probable cause.

TECHNICAL BACKGROUND

6. Based on training and experience and information learned from others, your affiant is familiar with the following terms:

a. **Internet Protocol Address**: An Internet Protocol address ("IP address") is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address. The assignment of IP addresses to computers connected to the Internet is controlled by Internet Service Providers ("ISPs").

b. **Domain Name**: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond to a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

c. **Domain Name System**: The domain name system ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the

“top-level” domain. For example, the domain name “www.example.com” means that the computer assigned that name is in the “.com” top-level domain, and the “example” second-level domain.

d. Domain Name Registry: DNS servers are computers connected to the Internet that convert, or resolve, domain names into IP addresses. For each top-level domain (such as “.com”), there is a single company, called a “registry,” that determines which second-level domain resolves to which IP address. The registry for the “.us” top-level domain is Neustar, Inc.

e. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The registrar used to register the Megaclick.us domain name was GoDaddy.com. The individual or business that purchases, or registers, a domain name is called a “registrant.” Registrants control the IP address, and thus the computer, to which their domain name resolves. A registrant may easily move a domain name to another computer anywhere in the world. Typically a registrar will provide a registrant with the ability to change the IP address a particular domain name resolves to through an online interface.

PROBABLE CAUSE FOR SEIZURE AND FORFEITURE

7. In March 2010, [REDACTED] initiated an investigation of a worldwide criminal organization known as the “Mega Conspiracy,” which was believed to be hosting and distributing unauthorized copies of copyrighted works over the Internet. The Mega Conspiracy consists of a series of websites and services, including a video hosting and

distribution service located at the domain Megavideo.com; an adult video hosting service located at the domain Megaporn.com; a file hosting and distribution service located at the domain Megaupload.com; an advertising service associated with its other websites located at the domain Megaclick.com; and a number of associated websites. DEFENDANTS and others are members of the Mega Conspiracy, which has operated since at least September 2005 and is estimated to have caused harm to copyright holders in excess of \$500,000,000 and generated more than \$175,000,000 in revenue.

8. Once a user uploads a file to Megaupload.com, the system provides the user with a specific and unique Uniform Resource Locator (“URL link”) from which the file can be downloaded or viewed. If a video file is uploaded, an individual can use the provided URL link to redirect others to the related website Megavideo.com to view the file via the website’s Flash video player. Users can also embed the Flash video player from Megavideo.com into another website to display the video file there. Megaupload.com supports a vast landscape of websites offering the Megaupload.com-provided URL links to view unauthorized copies of copyrighted motion pictures and television programs that are being hosted on servers controlled by the Mega Conspiracy. Once a video has been viewed, a user also has the ability to download and save the video to his computer.

9. Paragraph 18 of the Indictment, which your affiant has reviewed and believes to be accurate and consistent with the investigation, alleges that, before any video can be viewed on Megavideo.com, the user must view an advertisement. Originally, the Mega Conspiracy had contracted with companies such as adBrite, Inc., Google AdSense, and PartyGaming plc for Internet advertising. Currently, the Mega Conspiracy’s own

advertising website, Megaclick.com, is used to set up advertising campaigns on all the Mega Conspiracy websites. The high traffic volume on the Mega Conspiracy websites allows the Mega Conspiracy to charge advertisers up-front and at a higher rate than would be achieved by the percentage-per-click methodology used by other popular Internet advertising companies. The popularity of the infringing content on the Mega Conspiracy websites has generated more than \$25 million in online advertising revenues.

10. Paragraph 9 of the Indictment alleges that, in addition to displaying online advertisements, the download pages on Megaupload.com are designed to increase premium subscriptions. All non-premium users are encouraged to buy a premium subscription to decrease wait and download times, which can be at least an hour for popular content (and, for some periods of time, these non-premium users have been ineligible to download files over a certain size). As a result, non-premium users are repeatedly asked by the Mega Conspiracy to pay for more and faster access to content on Megaupload.com.

11. Using an undercover computer, [REDACTED] observed how a visitor may view content hosted on Megaupload.com. For example, on November 20, 2011, [REDACTED] observed the copyrighted motion picture *Zack and Miri Make a Porno*, which was released in 2008 by The Weinstein Company, on the website Megavideo.com. When the file was selected, the URL link redirected to www.megavideo.com/?v=REYCBLNF and a file entitled “[Película] Zack and Miri Make a Porno VOSE” was streamed. The same day, [REDACTED] located the copyrighted motion picture *The Twilight Saga: Breaking Dawn - Part 1* on the website www.peliculasyonkis.com. When selected, the URL link redirected to www.megavideo.com/?s=seriesyonkis&v=HY01ZGSR, where [REDACTED] viewed a

camcorderd version of the copyrighted motion picture, which had been released in United States theaters only two days prior, on November 18, 2011.

12. Paragraph 10 of the Indictment alleges that the content available from Megaupload.com is not searchable on the website, which allows the Mega Conspiracy to conceal the scope of its infringement. Instead of hosting a search function on its own site, the Mega Conspiracy business model purposefully relies on thousands of third party “linking” sites, which contain user-generated postings of links created by Megaupload.com (as well as those created by other Mega Conspiracy websites, including Megavideo.com and Megaporn.com). While the Mega Conspiracy may not operate these third party sites, the Mega Conspiracy did provide financial incentives for premium users to post links on linking sites through the “Uploader Rewards” program, which ensured widespread distribution of Megaupload.com links throughout the Internet and an inventory of popular content on servers controlled by the Mega Conspiracy. These linking sites, which are usually well organized, promote and direct users to Mega Conspiracy download pages that allow the reproduction and distribution of infringing copies of copyrighted works.

13. Paragraph 14 of the Indictment alleges that, in contrast to the public who is required to significantly rely on third party indexes, members of the Mega Conspiracy have full access to the listings of actual files that are stored on servers they control (as well as the Megaupload.com- and Megavideo.com- and Megaporn.com-generated links to those files). Conspirators have searched the internal database in order to directly access copyright-infringing content on servers controlled by the Mega Conspiracy.

14. Paragraph 19 of the Indictment alleges that, like Megaupload.com, Megavideo.com conceals many of the infringing copies of popular copyrighted videos that are available on and distributed by the website. Megavideo.com does purport to provide both browse and search functions, but any user's search on Megavideo.com for a full length copyrighted video (which can be downloaded from a Mega Conspiracy-controlled server somewhere in the world) will not produce any results. Similarly, browsing the front page of Megavideo.com does not show any obviously infringing copies of any copyrighted works; instead, the front page contains videos of news stories, user-generated videos, and general Internet videos in a manner substantially similar to Youtube.com. Browsing the most-viewed videos in the Entertainment category on Megavideo.com, however, has at times revealed a number of infringing copies of copyrighted works that are available from Mega Conspiracy-controlled servers and are amongst the most viewed materials being offered.

15. The Mega Conspiracy uses e-mail addresses with the extension @megaupload.com in the operation of the Megaupload.com website. [REDACTED] the e-mail account megaupload.support@gmail.com revealed the e-mail address abuse@megaupload.com has received and continues to receive thousands of DMCA infringement notices from copyright holders, including but not limited to Warner Bros. Entertainment Inc., Sony Music Entertainment Inc., and the Business Software Alliance. The e-mails provided notice of the existence of unauthorized copies of copyrighted motion pictures, television shows, software, literature, and music on servers controlled by the Mega Conspiracy. The notice e-mails contained the URL links to the locations on

Megaupload.com where the infringing copies of copyrighted works resided. [REDACTED] review of other e-mails has shown that the Mega Conspiracy operators are willfully violating copyright law by ignoring notices of selected infringing content, and are actually uploading infringing content themselves to Mega Conspiracy websites.

16. Using publicly available software that can detect the IP addresses of data incoming to the undercover computer, [REDACTED] was able to determine that the copyrighted content hosted on Megaupload.com was being downloaded from computers assigned IP addresses held by three commercial Internet hosting service companies: Carpathia Hosting, headquartered in Dulles, Virginia, with datacenters in Ashburn, Virginia, both of which are located in the Eastern District of Virginia; Cogent Communications, headquartered in Washington, D.C., with datacenters in Washington, D.C. and France; and Leaseweb in the Netherlands. Each of these Internet hosting service companies leases high-speed computer server space and Internet connectivity to the public.

17. On or about June 24, 2010, members of the Mega Conspiracy were informed, pursuant to a criminal search warrant from the U.S. District Court for the Eastern District of Virginia, that thirty-nine infringing copies of copyrighted motion pictures were present on their leased servers at Carpathia Hosting, a hosting company headquartered in the Eastern District of Virginia. A member of the Mega Conspiracy informed several of his co-conspirators at that time that he located the named files using internal searches of the Mega Conspiracy's systems. As of November 18, 2011, thirty-six of the thirty-nine infringing copies of copyrighted motion pictures were still being stored on servers controlled by the Mega Conspiracy.

18. In addition to Megaupload.com, Megavideo.com, and Megaclick.com, other websites created and domains owned by the Mega Conspiracy include: Megaworld.com; Megastuff.co; Megaclicks.co; Megastuff.info; Megaclicks.org; Megaworld.mobi; Megastuff.org; Megaclick.us; Mageclick.com; HDmegaporn.com; Megaporn.com; Megavkdeo.com; Megarotic.com; and Megavideoclips.com. At least two of these additional sites have also hosted infringing copies of copyrighted works. The websites and services, as well as the domains themselves, have been facilitated and promoted by illicit proceeds from the operations of Megaupload.com, Megavideo.com, and Megaclick.com.

THE SUBJECT DOMAIN

19. [REDACTED] the Megaclick.us domain was registered on or about November 29, 2010. The registrant and account holder was indicated to be "Domain Administrator" at Megamedia Ltd, in Hong Kong. [REDACTED]

[REDACTED] on or about May 20, 2006, DOTCOM registered the company Megamedia Limited in Hong Kong with company registry number 1046613. The company director is listed as KIM TIM JIM VESTOR (a known alias of DOTCOM), with Finland passport no. [REDACTED], and VESTOR LIMITED is listed as the sole shareholder.

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

20. Title 18, United States Code, Section 2323(a)(1)(A) and (B) and 2323(b) provide, in relevant part, that any property used, or intended to be used to commit or facilitate criminal copyright infringement, or constituting or derived from proceeds obtained directly or indirectly from the commission of criminal copyright infringement, are

subject to both civil and criminal forfeiture. Title 18, United States Code, Section 2323(b)(2) authorizes the use of procedures set forth in Title 21, United States Code, Section 853 for the seizure of property subject to criminal forfeiture.

21. Title 18, United States Code, Sections 981(a)(1) and 982(a)(1) provide that a defendant who is convicted of money laundering shall forfeit to the United States “any property involved in the offense, or any property traceable to such property. Title 18, United States Code, Section 982(b)(1) authorizes the use of procedures set forth in Title 21, United States Code, Section 853 for the seizure of property subject to criminal forfeiture.

22. Where there is probable cause to believe that the property to be seized is subject to forfeiture and that an order pursuant to Title 21, United States Code, Section 853(e) may not be sufficient to assure its availability for forfeiture, a district court may issue a warrant authorizing the seizure of such property. 21 U.S.C. § 853(f). Section 853(f) provides that:

The Government may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant. If the court determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that an order under subsection (e) may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property.

A seizure warrant issued under Title 21, United States Code, Section 853(f) has nationwide scope. 21 U.S.C. § 853(l).

23. In addition, Title 18, United States Code, Section 1963(a) provides that any defendant who is convicted of racketeering activity shall forfeit to the United States any

property constituting, or derived from, any proceeds which the person obtained, directly or indirectly, from the racketeering activity. Title 18, United States Code, Section 1963(d)(1) provides that:

Upon application of the United States, the court may enter a restraining order or injunction, require the execution of a satisfactory performance bond, or take any other action to preserve the availability of property described in subsection (a) for forfeiture under this section—

- (A) upon the filing of an indictment or information charging a violation of section 1962 of this chapter and alleging that the property with respect to which the order is sought would, in the event of conviction, be subject to forfeiture under this section

A seizure warrant issued under Title 21, United States Code, Section 1963(d) has nationwide scope. 18 U.S.C. § 1963(j).

24. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the Subject Domain Name for forfeiture. By seizing the Subject Domain Name and redirecting them to another website, the United States will prevent supporters of the Mega Conspiracy or third parties from redirecting the Subject Domain Name to servers elsewhere in the world, and thus using them to commit additional crimes. Furthermore, seizure of the Subject Domain Name will prevent visitors from continuing to access the websites located at the Subject Domain Name.

25. Title 18, United States Code, Section 2319(a)(2) provides that the procedures set forth in Chapter 46 of Title 18 (18 U.S.C. § 981, et seq.) shall extend to civil forfeitures under Section 2323(a). Title 18, United States Code, Section 981(b)(1) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause. Title 18, United States Code, Section 981(b)(3) permits the issuance of a seizure warrant by

a judicial officer in any district in which a forfeiture action against the property may be filed and may be executed in any district in which the property is found.

26. As set forth above, there is probable cause to believe that the Subject Domain Name are subject to both civil and criminal forfeiture because they were used in the commission of criminal copyright infringement, conspiracy to commit criminal copyright infringement, conspiracy to commit racketeering, and conspiracy to commit money laundering.

SEIZURE PROCEDURE

27. As detailed in Attachment A, upon execution of the seizure warrant, the registry for the top-level domain shall be directed to restrain and lock the Subject Domain Name pending transfer of all right, title, and interest in the Subject Domain Name to the United States upon completion of forfeiture proceedings, to ensure that changes to the Subject Domain Name cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI.

28. In addition, upon seizure of the Subject Domain Name, the registry for the top-level domain will be directed to point the Subject Domain Name to IP addresses controlled by the United States, which will display a web page providing public notice of the website seizure.

29. The domain name registrars also maintain certain records relating to the owner of each domain name for which it is the top-level registry, including the Subject Domain Name (the "Domain Name Records"). Certain of these records are available to the public through a "Whois" lookup through a web browser, among other means. At the time

the Subject Domain Name are seized, the registrars will be directed to change the “Technical Contact” and “Administrative Contact” fields of the Domain Name Records for the Subject Domain Name to contact information relating to FBI to reflect the fact that the Subject Domain Name have been seized; and to change the name server fields of the Domain Name Records to effect the forgoing changes. All other fields will be changed so that they do not reflect any individual or entity.

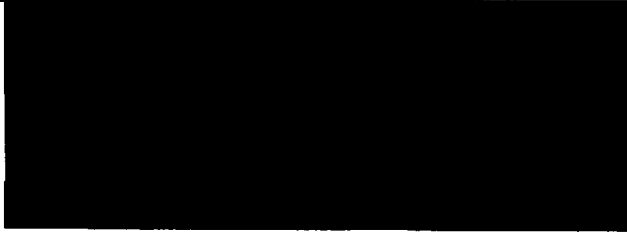
30. Upon completion of forfeiture proceedings, all Domain Name Records for the Subject Domain Name maintained by the top-level registry and the domain name registrars will be changed to reflect the transfer of ownership to the United States.

CONCLUSION

31. Based on the information contained in the Indictment and this affidavit there is probable cause to believe that the Subject Domain Name are subject to seizure and forfeiture as property constituting or derived from proceeds obtained directly or indirectly from, or used or intended to be used to facilitate, the commission of criminal copyright infringement (17 U.S.C. § 506; 18 U.S.C. §§ 2319 and 2323); constituting or derived from proceeds traceable to conspiracy to commit criminal copyright infringement (18 U.S.C. §§ 371 and 981; 28 U.S.C. § 2461); involved in or traceable to the conspiracy to commit money laundering (18 U.S.C. §§ 982 and 1956(h)); or constituting or derived from proceeds obtained directly or indirectly from, or acquired in maintained in violation of, a conspiracy to commit racketeering (18 U.S.C. §§ 1962 and 1963).

Accordingly, it is requested that a seizure warrant be issued for the Subject Domain
Name.

FURTHER THIS AFFIANT SAYETH NOT



Subscribed to and sworn before me on this 13th day of January, 2012.

Honorable Liam O'Grady
United States District Judge

Submitted by Lindsay A. Kelly and Jay V. Prabhu
Assistant United States Attorneys

ATTACHMENT A

I. Seizure Procedure

A. The seizure warrant will be presented in person or transmitted via facsimile or email to personnel of the domain name registry listed in Section II ("Subject Registry") and the domain name registrars listed in Section III ("Subject Registrars") who will be directed, for the domain name listed in Section IV ("Subject Domain Name") for which it serves as the top-level domain registry, to make any changes necessary to restrain and lock the Subject Domain Name pending transfer of all rights, title, and interest in the Subject Domain Name to the United States upon completion of forfeiture proceedings.

B. Upon seizure of the Subject Domain Name, the Subject Registry shall take all steps necessary to restrain and lock the domain at the registry level to ensure that changes to the Subject Domain Name cannot be made absent a court order or, if forfeited to the United States government, without prior consultation with FBI.

C. The Subject Registry shall point the Subject Domain Name to [REDACTED] and [REDACTED] at which the Government will display a web page with the following notice:

This domain name associated with the website Megaupload.com has been seized pursuant to an order issued by the U.S. District Court for the Eastern District of Virginia.

An indictment has been returned by a grand jury in Alexandria, Virginia, charging several individuals and entities allegedly involved in the operation of Megaupload.com and related websites with the following federal crimes: Conspiracy to Commit Racketeering (18 U.S.C. § 1962(d)), Conspiracy to Commit Copyright Infringement (18 U.S.C. § 371), Conspiracy to Commit Money Laundering (18 U.S.C. § 1956(h)), and Criminal Copyright Infringement (18 U.S.C. §§ 2, 2319; 17 U.S.C. § 506).

The case is being prosecuted by the U.S. Attorney's Office for the Eastern District of Virginia and the U.S. Department of Justice's Computer Crime and Intellectual Property Section.

D. Upon seizure of the Subject Domain Name, the Subject Registrars shall modify any records, databases, tables, or documents that are used by the Subject Registrars to identify the owner of the Subject Domain Name to reflect the seizure of the Subject Domain Name. These changes relate to the following records, if they exist:

1. The "Technical Contact" and "Administrative Contact" fields will reflect the following information:
 - a) Name: Federal Bureau of Investigation
 - b) Address: 935 Pennsylvania Ave
Washington, DC 20535
 - c) Country: USA
 - d) Telephone: 202-324-3000
 - e) Email: IPR@ic.fbi.gov
2. Any remaining fields will be changed so they do not reflect any individual or entity.

II. Subject Registry

Neustar Legal Compliance
46000 Center Oak Plaza
Sterling, VA 20166

III. Subject Registrar

GoDaddy.com
14455 N. Hayden Rd., Ste. 226
Scottsdale, AZ 85260

IV. Subject Domain Name

Megaclick.us

FILED

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

2012 JAN 13 P 2:19

In the Matter of the Seizure of:) Case No. 1:12-sw-36
The Domain Name Megaclick.us) UNDER SEAL
CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

**GOVERNMENT'S MOTION TO SEAL SEIZURE WARRANT
PURSUANT TO LOCAL RULE 49(B)**

The United States, through undersigned counsel, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, now asks for an Order to Seal the seizure warrant, the application for seizure warrant, and the affidavit in support of the seizure warrant, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal these documents.

I. REASONS FOR SEALING (See Local Rule 49(B)(1))

1. The Indictment, and arrest warrants, charging nine defendants with various crimes stemming from their involvement in a worldwide criminal enterprise related to Megaupload.com is under seal. [REDACTED]

2. While it is anticipated that the Indictment will be unsealed shortly after this seizure warrant is served, premature disclosure of the specific details of this criminal case [REDACTED]

[REDACTED]

3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. THE GOVERNING LAW (See Local Rule 49(B)(2))

4. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. Media General Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4th Cir. 2005); In re Washington Post Company v. Hughes, 923 F.2d 324, 326 (4th Cir. 1991). “But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is ‘essential to preserve higher values’ and ‘narrowly tailored to serve that interest.’” Media General Operations, 417 F.3d at 429 (citations omitted); see also In re Knight Pub. Co., 743 F.2d 231, 235 (4th Cir. 1984) (“[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public’s right of access is outweighed by competing interests”). Sealing search and seizure warrants and their accompanying affidavits and application is within the discretionary powers of a judicial officer where, among other things, an “‘affidavit contain[s] sensitive details of an ongoing investigation’ and it is ‘clear and apparent from the affidavits that any disclosure of the information there would hamper’ th[e] ongoing investigation.” Media General Operations 417 F.3d at 430 (citations omitted); see also In re Search Warrant for Matter of Eye Care Physicians of America, 100 F.3d 514, 518 (7th Cir. 1996).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable

opportunity to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. Ashcraft v. Conoco, Inc., 218 F.3d 288, 302 (4th Cir. 2000).

6. However, in the specific context of a search and seizure warrant, the Fourth Circuit has cautioned that “the opportunity to object” cannot “arise prior to the entry of a sealing order when a search warrant has not been executed.” Media General Operations, 417 F.3d at 429. “A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant.” Id.; see also Franks v. Delaware, 438 U.S. 154, 169 (1978). Accordingly, “the notice requirement is fulfilled by docketing ‘the order sealing the documents,’ which gives interested parties the opportunity to object after the execution of the search warrants.” Media General Operations, 417 F.3d at 430 (quoting Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989)); see also Local Rule 49(B) (“Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.”).

7. As to the requirement of a court’s consideration of alternatives, the Fourth Circuit counsels that, “[i]f a judicial officer determines that full public access is not appropriate, she ‘must consider alternatives to sealing the documents,’ which may include giving the public access to some of the documents or releasing a redacted version of the documents that are the subject to the government’s motion to seal.” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 66).

8. Finally, regarding the requirement of specific findings, the Fourth Circuit’s precedents state that, “in entering a sealing order, a ‘judicial officer may explicitly adopt the

facts that the government presents to justify sealing when the evidence appears creditable,” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 65), so long as the ultimate “decision to seal the papers “ is “made by the judicial officer,” Goetz, 886 F.2d at 65. “Moreover, if appropriate, the government’s submission and the [judicial] officer’s reason for sealing the documents can be filed under seal.” Goetz, 886 F.2d at 65; see also In re Washington Post Co., 807 F.2d 383, 391 (4th Cir. 1986) (“if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal”).

III. PERIOD OF TIME GOVERNMENT SEEKS TO HAVE MATTER REMAIN UNDER SEAL (See Local Rule 49(B)(3))

9. Pursuant to Local Rule 49(B)(3), the seizure warrant, the application for a seizure warrant, and the affidavit will remain sealed until the need to maintain the confidentiality of the these documents expires and the United States moves to unseal these documents.

WHEREFORE, the United States respectfully requests that the seizure warrant, application for seizure warrant, affidavit in support of the seizure warrant, and this Motion to Seal and proposed Order be sealed until further Order of the Court. Notwithstanding this request, the United States asks to provide copies as necessary to execute the seizure warrant.

Respectfully submitted,

Neil H. MacBride
United States Attorney

By: 
Lindsay A. Kelly
Assistant United States Attorney

AO 109 (Rev. 12/09) Warrant to Seize Property Subject to Forfeiture

FILED

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

2012 JAN 13 P 2:19

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

In the Matter of the Seizure of)
(Briefly describe the property to be seized))

The Domain Names Megaupload.org, Megaclicks.org,)
and Megastuff.org)

Case No. 1:12-sw-300

UNDER SEAL

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the Eastern District of Virginia be seized as being subject to forfeiture to the United States of America. The property is described as follows:

The Domain Names Megaupload.org, Megaclicks.org, and Megastuff.org

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property on or before Jan 27, 2012
(not to exceed 14 days)

in the daytime - 6:00 a.m. to 10:00 p.m.

at any time in the day or night, as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.


An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to
Honorable Liam O'Grady, U.S. District Judge

(name)

I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) for _____ days (not to exceed 30).

until, the facts justifying, the later specific date of _____

Date and time issued: 1/13/2012


Judge's signature

City and state: Alexandria, Virginia

The Honorable Liam O'Grady, U.S. District Judge

Printed name and title

AO 108 (Rev. 06/09) Application for a Warrant to Seize Property Subject to Forfeiture

FILED

UNITED STATES DISTRICT COURT

for the Eastern District of Virginia

2012 JAN 13 P 2: 19

CLERK US DISTRICT COURT ALEXANDRIA, VIRGINIA

In the Matter of the Seizure of (Briefly describe the property to be seized) The Domain Names Megaupload.org, Megaclicks.org, and Megastuff.org Case No. 1:12-sw-36 UNDER SEAL

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Eastern District of Virginia is subject to forfeiture to the United States of America under 18 U.S.C. § 981(a)(1)(C)* (describe the property):

The Domain Names Megaupload.org, Megaclicks.org, and Megastuff.org

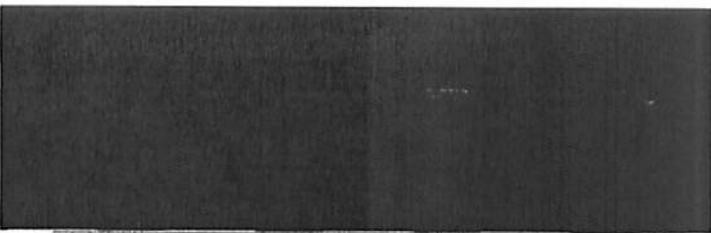
* Such property is also subject to forfeiture to the United States of America under 18 U.S.C. §§ 982(a)(1), 1963(a), and 2323.

The application is based on these facts:

SEE ATTACHED AFFIDAVIT OF [REDACTED]

[X] Continued on the attached sheet.

Reviewed by AUSA Lindsay Kelly



Printed name and title

Sworn to before me and signed in my presence.

Date: 1/13/2012

[Handwritten signature]

Judge's signature

City and state: Alexandria, Virginia

Honorable Liam O'Grady, U.S. District Judge

Printed name and title

violations of fraud, intrusion, and intellectual property laws, and has received training in these areas. Your affiant has also received training and gained experience in, among other things, interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, intellectual property crimes, and computer-based crimes, computer evidence identification, seizure and processing.

3. Your affiant makes this affidavit in support of the government's application, pursuant to Title 21, United States Code, Section 853(f), Title 18, United States Code, Section 2323, Title 18, United States Code, Section 1963, Title 18, United States Code, Section 982(b)(1), and Title 18, United States Code, Section 981(b)(1) for a warrant to seize the domain names Megaclicks.org, Megaupload.org, and Megastuff.org (hereinafter "Subject Domain Names").

4. The procedure by which the government will seize the Subject Domain Names is described in Attachment A hereto and below.

5. As set forth below, there is probable cause to believe that the Subject Domain Names are subject to seizure and forfeiture as property constituting or derived from proceeds obtained directly or indirectly from, or used or intended to be used to facilitate the commission of criminal copyright infringement (17 U.S.C. § 506; 18 U.S.C. §§ 2319 and 2323); constituting or derived from proceeds traceable to conspiracy to commit criminal copyright infringement (18 U.S.C. §§ 371 and 981; 28 U.S.C. § 2461); involved in or traceable to conspiracy to commit money laundering (18 U.S.C. §§ 982 and 1956(h)); or constituting or derived from proceeds obtained directly or indirectly from, or acquired or maintained in violation of, conspiracy to commit racketeering (18 U.S.C. §§ 1962, 1963). This affidavit does not set forth all of your

affiant's knowledge about this matter, and is intended to provide sufficient information to support probable cause.

TECHNICAL BACKGROUND

6. Based on training and experience and information learned from others, your affiant is familiar with the following terms:

a. **Internet Protocol Address:** An Internet Protocol address ("IP address") is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address. The assignment of IP addresses to computers connected to the Internet is controlled by Internet Service Providers ("ISPs").

b. **Domain Name:** A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond to a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

c. **Domain Name System:** The domain name system ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the "top-level" domain.

For example, the domain name “www.example.com” means that the computer assigned that name is in the “.com” top-level domain, and the “example” second-level domain.

d. Domain Name Registry: DNS servers are computers connected to the Internet that convert, or resolve, domain names into IP addresses. For each top-level domain (such as “.com”), there is a single company, called a “registry,” that determines which second-level domain resolves to which IP address. The registry for the “.org” top-level domain is Public Interest Registry.

e. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. For example, the registrar used to register the Megaclicks.org and Megastuff.org domain names was GoDaddy.com. The individual or business that purchases, or registers, a domain name is called a “registrant.” Registrants control the IP address, and thus the computer, to which their domain name resolves. A registrant may easily move a domain name to another computer anywhere in the world. Typically a registrar will provide a registrant with the ability to change the IP address a particular domain name resolves to through an online interface.

PROBABLE CAUSE FOR SEIZURE AND FORFEITURE

7. In March 2010, [REDACTED] initiated an investigation of a worldwide criminal organization known as the “Mega Conspiracy,” which was believed to be hosting and distributing unauthorized copies of copyrighted works over the Internet. The Mega Conspiracy consists of a series of websites and services, including a video hosting and distribution service located at the domain Megavideo.com; an adult video hosting service located at the domain Megaporn.com; a file hosting and distribution service located at the domain Megaupload.com; an

advertising service associated with its other websites located at the domain Megaclick.com; and a number of associated websites. DEFENDANTS and others are members of the Mega Conspiracy, which has operated since at least September 2005 and is estimated to have caused harm to copyright holders in excess of \$500,000,000 and generated more than \$175,000,000 in revenue.

8. Once a user uploads a file to Megaupload.com, the system provides the user with a specific and unique Uniform Resource Locator (“URL link”) from which the file can be downloaded or viewed. If a video file is uploaded, an individual can use the provided URL link to redirect others to the related website Megavideo.com to view the file via the website’s Flash video player. Users can also embed the Flash video player from Megavideo.com into another website to display the video file there. Megaupload.com supports a vast landscape of websites offering the Megupload.com-provided URL links to view unauthorized copies of copyrighted motion pictures and television programs that are being hosted on servers controlled by the Mega Conspiracy. Once a video has been viewed, a user also has the ability to download and save the video to his computer.

9. Paragraph 18 of the Indictment, which your affiant has reviewed and believes to be accurate and consistent with the investigation, alleges that, before any video can be viewed on Megavideo.com, the user must view an advertisement. Originally, the Mega Conspiracy had contracted with companies such as adBrite, Inc., Google AdSense, and PartyGaming plc for Internet advertising. Currently, the Mega Conspiracy’s own advertising website, Megaclick.com, is used to set up advertising campaigns on all the Mega Conspiracy websites. The high traffic volume on the Mega Conspiracy websites allows the Mega Conspiracy to charge

advertisers up-front and at a higher rate than would be achieved by the percentage-per-click methodology used by other popular Internet advertising companies. The popularity of the infringing content on the Mega Conspiracy websites has generated more than \$25 million in online advertising revenues.

10. Paragraph 9 of the Indictment alleges that, in addition to displaying online advertisements, the download pages on Megaupload.com are designed to increase premium subscriptions. All non-premium users are encouraged to buy a premium subscription to decrease wait and download times, which can be at least an hour for popular content (and, for some periods of time, these non-premium users have been ineligible to download files over a certain size). As a result, non-premium users are repeatedly asked by the Mega Conspiracy to pay for more and faster access to content on Megaupload.com.

11. Using an undercover computer, [REDACTED] observed how a visitor may view content hosted on Megaupload.com. For example, on November 20, 2011, [REDACTED] observed the copyrighted motion picture *Zack and Miri Make a Porno*, which was released in 2008 by The Weinstein Company, on the website Megavideo.com. When the file was selected, the URL link redirected to www.megavideo.com/?v=REYCBLNF and a file entitled “[Película] Zack and Miri Make a Porno VOSE” was streamed. The same day, [REDACTED] located the copyrighted motion picture *The Twilight Saga: Breaking Dawn - Part 1* on the website www.peliculasyonkis.com. When selected, the URL link redirected to www.megavideo.com/?s=seriesyonkis&v=HY01ZGSR, where [REDACTED] viewed a camcorder version of the copyrighted motion picture, which had been released in United States theaters only two days prior, on November 18, 2011.

12. Paragraph 10 of the Indictment alleges that the content available from Megaupload.com is not searchable on the website, which allows the Mega Conspiracy to conceal the scope of its infringement. Instead of hosting a search function on its own site, the Mega Conspiracy business model purposefully relies on thousands of third party “linking” sites, which contain user-generated postings of links created by Megaupload.com (as well as those created by other Mega Conspiracy websites, including Megavideo.com and Megaporn.com). While the Mega Conspiracy may not operate these third party sites, the Mega Conspiracy did provide financial incentives for premium users to post links on linking sites through the “Uploader Rewards” program, which ensured widespread distribution of Megaupload.com links throughout the Internet and an inventory of popular content on servers controlled by the Mega Conspiracy. These linking sites, which are usually well organized, promote and direct users to Mega Conspiracy download pages that allow the reproduction and distribution of infringing copies of copyrighted works.

13. Paragraph 14 of the Indictment alleges that, in contrast to the public who is required to significantly rely on third party indexes, members of the Mega Conspiracy have full access to the listings of actual files that are stored on servers they control (as well as the Megaupload.com- and Megavideo.com- and Megaporn.com-generated links to those files). Conspirators have searched the internal database in order to directly access copyright-infringing content on servers controlled by the Mega Conspiracy.

14. Paragraph 19 of the Indictment alleges that, like Megaupload.com, Megavideo.com conceals many of the infringing copies of popular copyrighted videos that are available on and distributed by the website. Megavideo.com does purport to provide both

browse and search functions, but any user's search on Megavideo.com for a full length copyrighted video (which can be downloaded from a Mega Conspiracy-controlled server somewhere in the world) will not produce any results. Similarly, browsing the front page of Megavideo.com does not show any obviously infringing copies of any copyrighted works; instead, the front page contains videos of news stories, user-generated videos, and general Internet videos in a manner substantially similar to Youtube.com. Browsing the most-viewed videos in the Entertainment category on Megavideo.com, however, has at times revealed a number of infringing copies of copyrighted works that are available from Mega Conspiracy-controlled servers and are amongst the most viewed materials being offered.

15. The Mega Conspiracy uses e-mail addresses with the extension @megaupload.com in the operation of the Megaupload.com website. [REDACTED] e-mail account megaupload.support@gmail.com revealed the e-mail address abuse@megaupload.com has received and continues to receive thousands of DMCA infringement notices from copyright holders, including but not limited to Warner Bros. Entertainment Inc., Sony Music Entertainment Inc., and the Business Software Alliance. The e-mails provided notice of the existence of unauthorized copies of copyrighted motion pictures, television shows, software, literature, and music on servers controlled by the Mega Conspiracy. The notice e-mails contained the URL links to the locations on Megaupload.com where the infringing copies of copyrighted works resided. [REDACTED] review of other e-mails has shown that the Mega Conspiracy operators are willfully violating copyright law by ignoring notices of selected infringing content, and are actually uploading infringing content themselves to Mega Conspiracy websites.

16. Using publicly available software that can detect the IP addresses of data incoming to the undercover computer, [REDACTED] was able to determine that the copyrighted content hosted on Megaupload.com was being downloaded from computers assigned IP addresses held by three commercial Internet hosting service companies: Carpathia Hosting, headquartered in Dulles, Virginia, with datacenters in Ashburn, Virginia, both of which are located in the Eastern District of Virginia; Cogent Communications, headquartered in Washington, D.C., with datacenters in Washington, D.C. and France; and Leaseweb in the Netherlands. Each of these Internet hosting service companies leases high-speed computer server space and Internet connectivity to the public.

17. On or about June 24, 2010, members of the Mega Conspiracy were informed, pursuant to a criminal search warrant from the U.S. District Court for the Eastern District of Virginia, that thirty-nine infringing copies of copyrighted motion pictures were present on their leased servers at Carpathia Hosting, a hosting company headquartered in the Eastern District of Virginia. A member of the Mega Conspiracy informed several of his co-conspirators at that time that he located the named files using internal searches of the Mega Conspiracy's systems. As of November 18, 2011, thirty-six of the thirty-nine infringing copies of copyrighted motion pictures were still being stored on servers controlled by the Mega Conspiracy.

18. In addition to Megaupload.com, Megavideo.com, and Megaclick.com, other websites created and domains owned by the Mega Conspiracy include: Megaworld.com; Megastuff.co; Megaclicks.co; Megastuff.info; Megaclicks.org; Megaworld.mobi; Megastuff.org; Megaclick.us; Megaclck.com; HDmegaporn.com; Megaporn.com; Megavkdeo.com; Megarotic.com; and Megavideoclips.com. At least two of these additional sites have also hosted

infringing copies of copyrighted works. The websites and services, as well as the domains themselves, have been facilitated and promoted by illicit proceeds from the operations of Megaupload.com, Megavideo.com, and Megaclick.com.

THE SUBJECT DOMAIN NAMES

19. [REDACTED] the Megaclicks.org domain and the Megastuff.org domain were registered on or about November 29, 2010. The registrant and account holder was indicated to be "Domain Administrator" at Megamedia Ltd, in Hong Kong.

[REDACTED]
[REDACTED] on or about May 20, 2006, DOTCOM registered the company Megamedia Limited in Hong Kong with company registry number 1046613. The company director is listed as KIM TIM JIM VESTOR (a known alias of DOTCOM), with Finland passport no. [REDACTED], and VESTOR LIMITED is listed as the sole shareholder.

20. [REDACTED] the Megaupload.org domain was registered on or about July 17, 2005, to MEGAUPLOAD LIMITED ("MUL"). MUL is a registered company in Hong Kong with company registry number 0835149. MUL has a number of bank accounts in Hong Kong that have been used to facilitate the operations of the Mega Conspiracy. Until August 2011, DOTCOM held the title of Chief Executive Officer of MUL and owned, through VESTOR LIMITED, approximately 68% of the shares of MUL. The remaining shares of MUL are owned by ORTMANN, BENCKO, VAN DER KOLK, ECHTERNACH, and a 1% investor in Hong Kong. Since August 2011, DOTCOM has held the title of Chief Innovation Officer of MUL.

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

21. Title 18, United States Code, Section 2323(a)(1)(A) and (B) and 2323(b) provide, in relevant part, that any property used, or intended to be used to commit or facilitate criminal copyright infringement, or constituting or derived from proceeds obtained directly or indirectly from the commission of criminal copyright infringement, are subject to both civil and criminal forfeiture. Title 18, United States Code, Section 2323(b)(2) authorizes the use of procedures set forth in Title 21, United States Code, Section 853 for the seizure of property subject to criminal forfeiture.

22. Title 18, United States Code, Sections 981(a)(1) and 982(a)(1) provide that a defendant who is convicted of money laundering shall forfeit to the United States “any property involved in the offense, or any property traceable to such property. Title 18, United States Code, Section 982(b)(1) authorizes the use of procedures set forth in Title 21, United States Code, Section 853 for the seizure of property subject to criminal forfeiture.

23. Where there is probable cause to believe that the property to be seized is subject to forfeiture and that an order pursuant to Title 21, United States Code, Section 853(e) may not be sufficient to assure its availability for forfeiture, a district court may issue a warrant authorizing the seizure of such property. 21 U.S.C. § 853(f). Section 853(f) provides that:

The Government may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant. If the court determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that an order under subsection (e) may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property.

A seizure warrant issued under Title 21, United States Code, Section 853(f) has nationwide scope. 21 U.S.C. § 853(l).

24. In addition, Title 18, United States Code, Section 1963(a) provides that any defendant who is convicted of racketeering activity shall forfeit to the United States any property constituting, or derived from, any proceeds which the person obtained, directly or indirectly, from the racketeering activity. Title 18, United States Code, Section 1963(d)(1) provides that:

Upon application of the United States, the court may enter a restraining order or injunction, require the execution of a satisfactory performance bond, or take any other action to preserve the availability of property described in subsection (a) for forfeiture under this section—

(A) upon the filing of an indictment or information charging a violation of section 1962 of this chapter and alleging that the property with respect to which the order is sought would, in the event of conviction, be subject to forfeiture under this section

A seizure warrant issued under Title 21, United States Code, Section 1963(d) has nationwide scope. 18 U.S.C. § 1963(j).

25. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the Subject Domain Names for forfeiture. By seizing the Subject Domain Names and redirecting them to another website, the United States will prevent supporters of the Mega Conspiracy or third parties from redirecting the Subject Domain Names to servers elsewhere in the world, and thus using them to commit additional crimes. Furthermore, seizure of the Subject Domain Names will prevent visitors from continuing to access the websites located at the Subject Domain Names.

26. Title 18, United States Code, Section 2319(a)(2) provides that the procedures set forth in Chapter 46 of Title 18 (18 U.S.C. § 981, et seq.) shall extend to civil forfeitures under

Section 2323(a). Title 18, United States Code, Section 981(b)(1) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause. Title 18, United States Code, Section 981(b)(3) permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed and may be executed in any district in which the property is found.

27. As set forth above, there is probable cause to believe that the Subject Domain Names are subject to both civil and criminal forfeiture because they were used in the commission of criminal copyright infringement, conspiracy to commit criminal copyright infringement, conspiracy to commit racketeering, and conspiracy to commit money laundering.

SEIZURE PROCEDURE

28. As detailed in Attachment A, upon execution of the seizure warrant, the registry for the top-level domain shall be directed to restrain and lock the Subject Domain Names pending transfer of all right, title, and interest in the Subject Domain Names to the United States upon completion of forfeiture proceedings, to ensure that changes to the Subject Domain Names cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI.

29. In addition, upon seizure of the Subject Domain Names, the registry for the top-level domain will be directed to point the Subject Domain Names to IP addresses controlled by the United States, which will display a web page providing public notice of the website seizure.

30. The domain name registrars also maintain certain records relating to the owner of each domain name for which it is the top-level registry, including the Subject Domain Names (the "Domain Name Records"). Certain of these records are available to the public through a

“Whois” lookup through a web browser, among other means. At the time the Subject Domain Names are seized, the registrars will be directed to change the “Technical Contact” and “Administrative Contact” fields of the Domain Name Records for the Subject Domain Names to contact information relating to FBI to reflect the fact that the Subject Domain Names have been seized; and to change the name server fields of the Domain Name Records to effect the forgoing changes. All other fields will be changed so that they do not reflect any individual or entity.

31. Upon completion of forfeiture proceedings, all Domain Name Records for the Subject Domain Names maintained by the top-level registry and the domain name registrars will be changed to reflect the transfer of ownership to the United States.

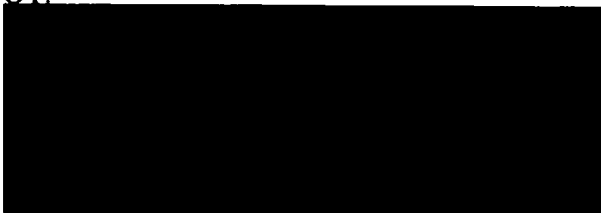
CONCLUSION

32. Based on the information contained in the Indictment and this affidavit there is probable cause to believe that the Subject Domain Names are subject to seizure and forfeiture as property constituting or derived from proceeds obtained directly or indirectly from, or used or intended to be used to facilitate, the commission of criminal copyright infringement (17 U.S.C. § 506; 18 U.S.C. §§ 2319 and 2323); constituting or derived from proceeds traceable to conspiracy to commit criminal copyright infringement (18 U.S.C. §§ 371 and 981; 28 U.S.C. § 2461); involved in or traceable to the conspiracy to commit money laundering (18 U.S.C. §§ 982 and 1956(h)); or constituting or derived from proceeds obtained directly or indirectly from, or acquired in maintained in violation of, a conspiracy to commit racketeering (18 U.S.C. §§ 1962 and 1963).

Accordingly, it is requested that a seizure warrant be issued for the Subject Domain

Names.

FURTHER THIS AFFIANT SAYETH NOT.



Subscribed to and sworn before me on this 13th day of January, 2012.



Honorable Liam O'Grady
United States District Judge

Submitted by Lindsay A. Kelly and Jay V. Prabhu
Assistant United States Attorneys

ATTACHMENT A

I. Seizure Procedure

A. The seizure warrant will be presented in person or transmitted via facsimile or email to personnel of the domain name registry listed in Section II ("Subject Registry") and the domain name registrars listed in Section III ("Subject Registrars") who will be directed, for the domain name listed in Section IV ("Subject Domain Names") for which it serves as the top-level domain registry, to make any changes necessary to restrain and lock the Subject Domain Names pending transfer of all rights, title, and interest in the Subject Domain Names to the United States upon completion of forfeiture proceedings.

B. Upon seizure of the Subject Domain Names, the Subject Registry shall take all steps necessary to restrain and lock the domain at the registry level to ensure that changes to the Subject Domain Names cannot be made absent a court order or, if forfeited to the United States government, without prior consultation with FBI.

C. The Subject Registry shall point the Subject Domain Names to [REDACTED] and [REDACTED] at which the Government will display a web page with the following notice:

This domain name associated with the website Megaupload.com has been seized pursuant to an order issued by the U.S. District Court for the Eastern District of Virginia.

*An indictment has been returned by a grand jury in Alexandria, Virginia, charging several individuals and entities allegedly involved in the operation of Megaupload.com and related websites with the following federal crimes:
Conspiracy to Commit Racketeering (18 U.S.C. § 1962(d)),
Conspiracy to Commit Copyright Infringement (18 U.S.C. § 371),
Conspiracy to Commit Money Laundering (18 U.S.C. § 1956(h)), and
Criminal Copyright Infringement (18 U.S.C. §§ 2, 2319; 17 U.S.C. § 506).*

The case is being prosecuted by the U.S. Attorney's Office for the Eastern District of Virginia and the U.S. Department of Justice's Computer Crime and Intellectual Property Section.

D. Upon seizure of the Subject Domain Names, the Subject Registrars shall modify any records, databases, tables, or documents that are used by the Subject Registrars to identify the owner of the Subject Domain Names to reflect the seizure of the Subject Domain Names. These changes relate to the following records, if they exist:

1. The "Technical Contact" and "Administrative Contact" fields will reflect the following information:
 - a) Name: Federal Bureau of Investigation
 - b) Address: 935 Pennsylvania Ave
Washington, DC 20535
 - c) Country: USA
 - d) Telephone: 202-324-3000
 - e) Email: IPR@ic.fbi.gov
2. Any remaining fields will be changed so they do not reflect any individual or entity.

II. Subject Registry

.ORG, THE PUBLIC INTEREST REGISTRY
1775 Wiehle Avenue, Suite 200
Reston, VA 20190

III. Subject Registrars

GoDaddy.com
14455 N. Hayden Rd., Ste. 226
Scottsdale, AZ 85260

Dotster, Inc.
8100 NE Parkway Drive, Suite 300
Vancouver, WA 98662

IV. Subject Domain Names

MEGACLICKS.ORG

MEGASTUFF.ORG

MEGAUPLOAD.ORG

FILED

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

2012 JAN 13 P 2:19
CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

In the Matter of the Seizure of:) Case No. 1:12-sw-36
)
The Domain Names Megaupload.org,) UNDER SEAL
Megaclicks.org, and Megastuff.org)

**GOVERNMENT'S MOTION TO SEAL SEIZURE WARRANT
PURSUANT TO LOCAL RULE 49(B)**

The United States, through undersigned counsel, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, now asks for an Order to Seal the seizure warrant, the application for seizure warrant, and the affidavit in support of the seizure warrant, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal these documents.


I. REASONS FOR SEALING (See Local Rule 49(B)(1))

1. The Indictment, and arrest warrants, charging nine defendants with various crimes stemming from their involvement in a worldwide criminal enterprise related to Megaupload.com is under seal. [REDACTED]

[REDACTED]

2. While it is anticipated that the Indictment will be unsealed shortly after this seizure warrant is served, premature disclosure of the specific details of this criminal case [REDACTED]

[REDACTED]



3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. THE GOVERNING LAW (See Local Rule 49(B)(2))

4. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. Media General Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4th Cir. 2005); In re Washington Post Company v. Hughes, 923 F.2d 324, 326 (4th Cir. 1991). “But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is ‘essential to preserve higher values’ and ‘narrowly tailored to serve that interest.’” Media General Operations, 417 F.3d at 429 (citations omitted); see also In re Knight Pub. Co., 743 F.2d 231, 235 (4th Cir. 1984) (“[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public’s right of access is outweighed by competing interests”). Sealing search and seizure warrants and their accompanying affidavits and application is within the discretionary powers of a judicial officer where, among other things, an “‘affidavit contain[s] sensitive details of an ongoing investigation’ and it is ‘clear and apparent from the affidavits that any disclosure of the information there would hamper’ th[e] ongoing investigation.” Media General Operations 417 F.3d at 430 (citations omitted); see also In re Search Warrant for Matter of Eye Care Physicians of America, 100 F.3d 514, 518 (7th Cir. 1996).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. Ashcraft v. Conoco, Inc., 218 F.3d 288, 302 (4th Cir. 2000).

6. However, in the specific context of a search and seizure warrant, the Fourth Circuit has cautioned that “the opportunity to object” cannot “arise prior to the entry of a sealing order when a search warrant has not been executed.” Media General Operations, 417 F.3d at 429. “A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant.” Id.; see also Franks v. Delaware, 438 U.S. 154, 169 (1978). Accordingly, “the notice requirement is fulfilled by docketing ‘the order sealing the documents,’ which gives interested parties the opportunity to object after the execution of the search warrants.” Media General Operations, 417 F.3d at 430 (quoting Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989)); see also Local Rule 49(B) (“Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.”).

7. As to the requirement of a court’s consideration of alternatives, the Fourth Circuit counsels that, “[i]f a judicial officer determines that full public access is not appropriate, she ‘must consider alternatives to sealing the documents,’ which may include giving the public access to some of the documents or releasing a redacted version of the documents that are the subject to the government’s motion to seal.” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 66).

8. Finally, regarding the requirement of specific findings, the Fourth Circuit's precedents state that, "in entering a sealing order, a 'judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears credible,'" Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 65), so long as the ultimate "decision to seal the papers" is "made by the judicial officer," Goetz, 886 F.2d at 65. "Moreover, if appropriate, the government's submission and the [judicial] officer's reason for sealing the documents can be filed under seal." Goetz, 886 F.2d at 65; see also In re Washington Post Co., 807 F.2d 383, 391 (4th Cir. 1986) ("if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal").

III. PERIOD OF TIME GOVERNMENT SEEKS TO HAVE MATTER REMAIN UNDER SEAL (See Local Rule 49(B)(3))

9. Pursuant to Local Rule 49(B)(3), the seizure warrant, the application for a seizure warrant, and the affidavit will remain sealed until the need to maintain the confidentiality of the these documents expires and the United States moves to unseal these documents.

WHEREFORE, the United States respectfully requests that the seizure warrant, application for seizure warrant, affidavit in support of the seizure warrant, and this Motion to Seal and proposed Order be sealed until further Order of the Court. Notwithstanding this request, the United States asks to provide copies as necessary to execute the seizure warrant.

Respectfully submitted,

Neil H. MacBride
United States Attorney

By: Lindsay Kelly
Lindsay A. Kelly
Assistant United States Attorney

AO 109 (Rev. 12/09) Warrant to Seize Property Subject to Forfeiture

FILED

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

2012 JAN 13 P 2:18

In the Matter of the Seizure of)
(Briefly describe the property to be seized))
The Domain Names Megastuff.info and)
Megaworld.mobi)

Case No. 1:12-sw-37

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

UNDER SEAL

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests that certain property located in the Eastern District of Pennsylvania be seized as being subject to forfeiture to the United States of America. The property is described as follows:

The Domain Names Megastuff.info and Megaworld.mobi

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property on or before Jan 21, 2012
(not to exceed 14 days)

- in the daytime – 6:00 a.m. to 10:00 p.m.
- at any time in the day or night, as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to

Honorable Liam O'Grady, U.S. District Judge

(name)

I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) for _____ days (not to exceed 30).

until, the facts justifying, the later specific date of _____

Date and time issued: 1/13/2012


Judge's signature

City and state: Alexandria, Virginia

The Honorable Liam O'Grady, U.S. District Judge

Printed name and title

AO 108 (Rev. 06/09) Application for a Warrant to Seize Property Subject to Forfeiture

FILED

UNITED STATES DISTRICT COURT
for the
Eastern District of Virginia

2012 JAN 13 P 2:17

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

In the Matter of the Seizure of)
(Briefly describe the property to be seized))
The Domain Names Megastuff.info)
and Megaworld.mobi)

Case No. 1:12-sw-37

UNDER SEAL

APPLICATION FOR A WARRANT
TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Eastern District of Pennsylvania is subject to forfeiture to the United States of America under 18 U.S.C. § 981(a)(1)(C)* (describe the property):

The Domain Names Megastuff.info and Megaworld.mobi

* Such property is also subject to forfeiture to the United States of America under 18 U.S.C. §§ 982(a)(1), 1963(a), and 2323.

The application is based on these facts:

SEE ATTACHED AFFIDAVIT OF [REDACTED]

Continued on the attached sheet.

Reviewed by AUSA
Lindsay Kelly



Printed name and title

Sworn to before me and signed in my presence.

Date: 1/13/2012

[Signature]
Judge's signature

City and state: Alexandria, Virginia

Honorable Liam O'Grady, U.S. District Judge

Printed name and title

FILED

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

2012 JAN 13 P 2:17

In the Matter of the Seizure of:)
)
The Domain Names Megastuff.info and)
Megaworld.mobi)

1:12SW37
CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

UNDER SEAL

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, [REDACTED], being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. Your affiant is a [REDACTED]

[REDACTED]. This affidavit is in connection with an investigation into the activities of KIM DOTCOM (also known as KIM SCHMITZ and KIM TIM JIM VESTOR) ("DOTCOM"), MEGAUPLOAD LIMITED, VESTOR LIMITED, FINN BATATO, JULIUS BENCKO ("BENCKO"), SVEN ECHTERNACH ("ECHTERNACH"), MATHIAS ORTMANN ("ORTMANN"), ANDRUS NOMM, and BRAM VAN DER KOLK ("VAN DER KOLK") (collectively, "DEFENDANTS"), who are believed to be involved in the operation and administration of several websites that reproduce and distribute infringing copies of copyrighted television programs, software, music, and motion pictures.

2. Your affiant is currently assigned to [REDACTED]

[REDACTED], where your affiant's duties include the investigation of crimes involving the infringement of intellectual property rights, including violations of Title 18, United States Code, Section 2319 and Title 17, United States Code, Section 506. Your affiant has been employed as a [REDACTED]. Your affiant has directed and participated in investigations involving the use of computers and the Internet to commit

violations of fraud, intrusion, and intellectual property laws, and has received training in these areas. Your affiant has also received training and gained experience in, among other things, interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, intellectual property crimes, and computer-based crimes, computer evidence identification, seizure and processing.

3. Your affiant makes this affidavit in support of the government's application, pursuant to Title 21, United States Code, Section 853(f), Title 18, United States Code, Section 2323, Title 18, United States Code, Section 1963, Title 18, United States Code, Section 982(b)(1), and Title 18, United States Code, Section 981(b)(1) for a warrant to seize the domain name Megaclick.us (hereinafter "Subject Domain Name").

4. The procedure by which the government will seize the Subject Domain Names is described in Attachment A hereto and below.

5. As set forth below, there is probable cause to believe that the Subject Domain Names are subject to seizure and forfeiture as property constituting or derived from proceeds obtained directly or indirectly from, or used or intended to be used to facilitate the commission of criminal copyright infringement (17 U.S.C. § 506; 18 U.S.C. §§ 2319 and 2323); constituting or derived from proceeds traceable to conspiracy to commit criminal copyright infringement (18 U.S.C. §§ 371 and 981; 28 U.S.C. § 2461); involved in or traceable to conspiracy to commit money laundering (18 U.S.C. §§ 982 and 1956(h)); or constituting or derived from proceeds obtained directly or indirectly from, or acquired or maintained in violation of, conspiracy to commit racketeering (18 U.S.C. §§ 1962, 1963). This affidavit does not set forth all of your

affiant's knowledge about this matter, and is intended to provide sufficient information to support probable cause.

TECHNICAL BACKGROUND

6. Based on training and experience and information learned from others, your affiant is familiar with the following terms:

a. **Internet Protocol Address**: An Internet Protocol address ("IP address") is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address. The assignment of IP addresses to computers connected to the Internet is controlled by Internet Service Providers ("ISPs").

b. **Domain Name**: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond to a particular IP address. For example, "usdoj.gov" and "cnn.com" are domain names.

c. **Domain Name System**: The domain name system ("DNS") is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or "labels," that are delimited by periods, such as "www.example.com." The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the "top-level" domain.

For example, the domain name “www.example.com” means that the computer assigned that name is in the “.com” top-level domain, and the “example” second-level domain.

d. Domain Name Registry: DNS servers are computers connected to the Internet that convert, or resolve, domain names into IP addresses. For each top-level domain (such as “.com”), there is a single company, called a “registry,” that determines which second-level domain resolves to which IP address. The registry for the “.info” and “.mobi” top-level domains is Afilias.

c. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The registrar used to register the Subject Domain Names was GoDaddy.com. The individual or business that purchases, or registers, a domain name is called a “registrant.” Registrants control the IP address, and thus the computer, to which their domain name resolves. A registrant may easily move a domain name to another computer anywhere in the world. Typically a registrar will provide a registrant with the ability to change the domain name a particular IP address resolves to through an online interface.

PROBABLE CAUSE FOR SEIZURE AND FORFEITURE

7. In March 2010, [REDACTED] initiated an investigation of a worldwide criminal organization known as the “Mega Conspiracy,” which was believed to be hosting and distributing unauthorized copies of copyrighted works over the Internet. The Mega Conspiracy consists of a series of websites and services, including a video hosting and distribution service located at the domain Megavideo.com; an adult video hosting service located at the domain Megaporn.com; a file hosting and distribution service located at the domain Megaupload.com; an

advertising service associated with its other websites located at the domain Megaclick.com; and a number of associated websites. DEFENDANTS and others are members of the Mega Conspiracy, which has operated since at least September 2005 and is estimated to have caused harm to copyright holders in excess of \$500,000,000 and generated more than \$175,000,000 in revenue.

8. Once a user uploads a file to Megaupload.com, the system provides the user with a specific and unique Uniform Resource Locator (“URL link”) from which the file can be downloaded or viewed. If a video file is uploaded, an individual can use the provided URL link to redirect others to the related website Megavideo.com to view the file via the website’s Flash video player. Users can also embed the Flash video player from Megavideo.com into another website to display the video file there. Megaupload.com supports a vast landscape of websites offering the Megupload.com-provided URL links to view unauthorized copies of copyrighted motion pictures and television programs that are being hosted on servers controlled by the Mega Conspiracy. Once a video has been viewed, a user also has the ability to download and save the video to his computer.

9. Paragraph 18 of the Indictment, which your affiant has reviewed and believes to be accurate and consistent with the investigation, alleges that, before any video can be viewed on Megavideo.com, the user must view an advertisement. Originally, the Mega Conspiracy had contracted with companies such as adBrite, Inc., Google AdSense, and PartyGaming plc for Internet advertising. Currently, the Mega Conspiracy’s own advertising website, Megaclick.com, is used to set up advertising campaigns on all the Mega Conspiracy websites. The high traffic volume on the Mega Conspiracy websites allows the Mega Conspiracy to charge

advertisers up-front and at a higher rate than would be achieved by the percentage-per-click methodology used by other popular Internet advertising companies. The popularity of the infringing content on the Mega Conspiracy websites has generated more than \$25 million in online advertising revenues.

10. Paragraph 9 of the Indictment alleges that, in addition to displaying online advertisements, the download pages on Megaupload.com are designed to increase premium subscriptions. All non-premium users are encouraged to buy a premium subscription to decrease wait and download times, which can be at least an hour for popular content (and, for some periods of time, these non-premium users have been ineligible to download files over a certain size). As a result, non-premium users are repeatedly asked by the Mega Conspiracy to pay for more and faster access to content on Megaupload.com.

11. Using an undercover computer, [REDACTED] observed how a visitor may view content hosted on Megaupload.com. For example, on November 20, 2011, [REDACTED] observed the copyrighted motion picture *Zack and Miri Make a Porno*, which was released in 2008 by The Weinstein Company, on the website Megavideo.com. When the file was selected, the URL link redirected to www.megavideo.com/?v=REYCBLNF and a file entitled “[Película] Zack and Miri Make a Porno VOSE” was streamed. The same day, [REDACTED] located the copyrighted motion picture *The Twilight Saga: Breaking Dawn - Part 1* on the website www.peliculasyonkis.com. When selected, the URL link redirected to www.megavideo.com/?s=seriesyonkis&v=HY01ZGSR, where [REDACTED] viewed a camcorded version of the copyrighted motion picture, which had been released in United States theaters only two days prior, on November 18, 2011.

12. Paragraph 10 of the Indictment alleges that the content available from Megaupload.com is not searchable on the website, which allows the Mega Conspiracy to conceal the scope of its infringement. Instead of hosting a search function on its own site, the Mega Conspiracy business model purposefully relies on thousands of third party “linking” sites, which contain user-generated postings of links created by Megaupload.com (as well as those created by other Mega Conspiracy websites, including Megavideo.com and Megaporn.com). While the Mega Conspiracy may not operate these third party sites, the Mega Conspiracy did provide financial incentives for premium users to post links on linking sites through the “Uploader Rewards” program, which ensured widespread distribution of Megaupload.com links throughout the Internet and an inventory of popular content on servers controlled by the Mega Conspiracy. These linking sites, which are usually well organized, promote and direct users to Mega Conspiracy download pages that allow the reproduction and distribution of infringing copies of copyrighted works.

13. Paragraph 14 of the Indictment alleges that, in contrast to the public who is required to significantly rely on third party indexes, members of the Mega Conspiracy have full access to the listings of actual files that are stored on servers they control (as well as the Megaupload.com- and Megavideo.com- and Megaporn.com-generated links to those files). Conspirators have searched the internal database in order to directly access copyright-infringing content on servers controlled by the Mega Conspiracy.

14. Paragraph 19 of the Indictment alleges that, like Megaupload.com, Megavideo.com conceals many of the infringing copies of popular copyrighted videos that are available on and distributed by the website. Megavideo.com does purport to provide both

browse and search functions, but any user's search on Megavideo.com for a full length copyrighted video (which can be downloaded from a Mega Conspiracy-controlled server somewhere in the world) will not produce any results. Similarly, browsing the front page of Megavideo.com does not show any obviously infringing copies of any copyrighted works; instead, the front page contains videos of news stories, user-generated videos, and general Internet videos in a manner substantially similar to Youtube.com. Browsing the most-viewed videos in the Entertainment category on Megavideo.com, however, has at times revealed a number of infringing copies of copyrighted works that are available from Mega Conspiracy-controlled servers and are amongst the most viewed materials being offered.

15. The Mega Conspiracy uses e-mail addresses with the extension @megaupload.com in the operation of the Megaupload.com website. [REDACTED] the e-mail account megaupload.support@gmail.com revealed the e-mail address abuse@megaupload.com has received and continues to receive thousands of DMCA infringement notices from copyright holders, including but not limited to Warner Bros. Entertainment Inc., Sony Music Entertainment Inc., and the Business Software Alliance. The e-mails provided notice of the existence of unauthorized copies of copyrighted motion pictures, television shows, software, literature, and music on servers controlled by the Mega Conspiracy. The notice e-mails contained the URL links to the locations on Megaupload.com where the infringing copies of copyrighted works resided. [REDACTED] review of other e-mails has shown that the Mega Conspiracy operators are willfully violating copyright law by ignoring notices of selected infringing content, and are actually uploading infringing content themselves to Mega Conspiracy websites.

16. Using publicly available software that can detect the IP addresses of data incoming to the undercover computer, [REDACTED] was able to determine that the copyrighted content hosted on Megaupload.com was being downloaded from computers assigned IP addresses held by three commercial Internet hosting service companies: Carpathia Hosting, headquartered in Dulles, Virginia, with datacenters in Ashburn, Virginia, both of which are located in the Eastern District of Virginia; Cogent Communications, headquartered in Washington, D.C., with datacenters in Washington, D.C. and France; and Leaseweb in the Netherlands. Each of these Internet hosting service companies leases high-speed computer server space and Internet connectivity to the public.

17. On or about June 24, 2010, members of the Mega Conspiracy were informed, pursuant to a criminal search warrant from the U.S. District Court for the Eastern District of Virginia, that thirty-nine infringing copies of copyrighted motion pictures were present on their leased servers at Carpathia Hosting, a hosting company headquartered in the Eastern District of Virginia. A member of the Mega Conspiracy informed several of his co-conspirators at that time that he located the named files using internal searches of the Mega Conspiracy's systems. As of November 18, 2011, thirty-six of the thirty-nine infringing copies of copyrighted motion pictures were still being stored on servers controlled by the Mega Conspiracy.

18. In addition to Megaupload.com, Megavideo.com, and Megaclick.com, other websites created and domains owned by the Mega Conspiracy include: Megaworld.com; Megastuff.co; Megaclicks.co; Megastuff.info; Megaclicks.org; Megaworld.mobi; Megastuff.org; Megaclick.us; Megaclick.com; HDmegaporn.com; Megaporn.com; Megavkdeo.com; Megarotic.com; and Megavideoclips.com. At least two of these additional sites have also hosted

infringing copies of copyrighted works. The websites and services, as well as the domains themselves, have been facilitated and promoted by illicit proceeds from the operations of Megaupload.com, Megavideo.com, and Megaclick.com.

THE SUBJECT DOMAIN NAMES

19. [REDACTED] the Subject Domain Names were registered on or about November 29, 2010. The registrant and account holder was indicated to be "Domain Administrator" at Megamedia Ltd, in Hong Kong. [REDACTED] [REDACTED] on or about May 20, 2006, DOTCOM registered the company Megamedia Limited in Hong Kong with company registry number 1046613. The company director is listed as KIM TIM JIM VESTOR (a known alias of DOTCOM), with Finland passport no. [REDACTED], and VESTOR LIMITED is listed as the sole shareholder.

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

20. Title 18, United States Code, Section 2323(a)(1)(A) and (B) and 2323(b) provide, in relevant part, that any property used, or intended to be used to commit or facilitate criminal copyright infringement, or constituting or derived from proceeds obtained directly or indirectly from the commission of criminal copyright infringement, are subject to both civil and criminal forfeiture. Title 18, United States Code, Section 2323(b)(2) authorizes the use of procedures set forth in Title 21, United States Code, Section 853 for the seizure of property subject to criminal forfeiture.

21. Title 18, United States Code, Sections 981(a)(1) and 982(a)(1) provide that a defendant who is convicted of money laundering shall forfeit to the United States "any property

involved in the offense, or any property traceable to such property. Title 18, United States Code, Section 982(b)(1) authorizes the use of procedures set forth in Title 21, United States Code, Section 853 for the seizure of property subject to criminal forfeiture.

22. Where there is probable cause to believe that the property to be seized is subject to forfeiture and that an order pursuant to Title 21, United States Code, Section 853(e) may not be sufficient to assure its availability for forfeiture, a district court may issue a warrant authorizing the seizure of such property. 21 U.S.C. § 853(f). Section 853(f) provides that:

The Government may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant. If the court determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that an order under subsection (e) may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property.

A seizure warrant issued under Title 21, United States Code, Section 853(f) has nationwide scope. 21 U.S.C. § 853(l).

23. In addition, Title 18, United States Code, Section 1963(a) provides that any defendant who is convicted of racketeering activity shall forfeit to the United States any property constituting, or derived from, any proceeds which the person obtained, directly or indirectly, from the racketeering activity. Title 18, United States Code, Section 1963(d)(1) provides that:

Upon application of the United States, the court may enter a restraining order or injunction, require the execution of a satisfactory performance bond, or take any other action to preserve the availability of property described in subsection (a) for forfeiture under this section—

(A) upon the filing of an indictment or information charging a violation of section 1962 of this chapter and alleging that the property with

respect to which the order is sought would, in the event of conviction, be subject to forfeiture under this section

A seizure warrant issued under Title 21, United States Code, Section 1963(d) has nationwide scope. 18 U.S.C. § 1963(j).

24. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the Subject Domain Names for forfeiture. By seizing the Subject Domain Names and redirecting them to another website, the United States will prevent supporters of the Mega Conspiracy or third parties from redirecting the Subject Domain Names to servers elsewhere in the world, and thus using them to commit additional crimes. Furthermore, seizure of the Subject Domain Names will prevent visitors from continuing to access the websites located at the Subject Domain Names.

25. Title 18, United States Code, Section 2319(a)(2) provides that the procedures set forth in Chapter 46 of Title 18 (18 U.S.C. § 981, et seq.) shall extend to civil forfeitures under Section 2323(a). Title 18, United States Code, Section 981(b)(1) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause. Title 18, United States Code, Section 981(b)(3) permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed and may be executed in any district in which the property is found.

26. As set forth above, there is probable cause to believe that the Subject Domain Names are subject to both civil and criminal forfeiture because they were used in the commission of criminal copyright infringement, conspiracy to commit criminal copyright infringement, conspiracy to commit racketeering, and conspiracy to commit money laundering.

SEIZURE PROCEDURE

27. As detailed in Attachment A, upon execution of the seizure warrant, the registry for the top-level domain shall be directed to restrain and lock the Subject Domain Names pending transfer of all right, title, and interest in the Subject Domain Names to the United States upon completion of forfeiture proceedings, to ensure that changes to the Subject Domain Names cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI.

28. In addition, upon seizure of the Subject Domain Names, the registry for the top-level domain will be directed to point the Subject Domain Names to IP addresses controlled by the United States, which will display a web page providing public notice of the website seizure.

29. The domain name registrars also maintain certain records relating to the owner of each domain name for which it is the top-level registry, including the Subject Domain Names (the "Domain Name Records"). Certain of these records are available to the public through a "Whois" lookup through a web browser, among other means. At the time the Subject Domain Names are seized, the registrars will be directed to change the "Technical Contact" and "Administrative Contact" fields of the Domain Name Records for the Subject Domain Names to contact information relating to FBI to reflect the fact that the Subject Domain Names have been seized; and to change the name server fields of the Domain Name Records to effect the forgoing changes. All other fields will be changed so that they do not reflect any individual or entity.

30. Upon completion of forfeiture proceedings, all Domain Name Records for the Subject Domain Names maintained by the top-level registry and the domain name registrars will be changed to reflect the transfer of ownership to the United States.

CONCLUSION

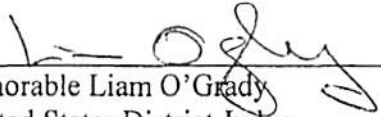
31. Based on the information contained in the Indictment and this affidavit there is probable cause to believe that the Subject Domain Names are subject to seizure and forfeiture as property constituting or derived from proceeds obtained directly or indirectly from, or used or intended to be used to facilitate, the commission of criminal copyright infringement (17 U.S.C. § 506; 18 U.S.C. §§ 2319 and 2323); constituting or derived from proceeds traceable to conspiracy to commit criminal copyright infringement (18 U.S.C. §§ 371 and 981; 28 U.S.C. § 2461); involved in or traceable to the conspiracy to commit money laundering (18 U.S.C. §§ 982 and 1956(h)); or constituting or derived from proceeds obtained directly or indirectly from, or acquired in maintained in violation of, a conspiracy to commit racketeering (18 U.S.C. §§ 1962 and 1963).

Accordingly, it is requested that a seizure warrant be issued for the Subject Domain Names.

FURTHER THIS AFFIANT SAYETH NOT



Subscribed to and sworn before me on this 13th day of January, 2012.



Honorable Liam O'Grady
United States District Judge

Submitted by Lindsay A. Kelly and Jay V. Prabhu
Assistant United States Attorneys

ATTACHMENT A

I. Seizure Procedure

A. The seizure warrant will be presented in person or transmitted via facsimile or email to personnel of the domain name registry listed in Section II ("Subject Registry") and the domain name registrars listed in Section III ("Subject Registrars") who will be directed, for the domain name listed in Section IV ("Subject Domain Names") for which it serves as the top-level domain registry, to make any changes necessary to restrain and lock the Subject Domain Names pending transfer of all rights, title, and interest in the Subject Domain Names to the United States upon completion of forfeiture proceedings.

B. Upon seizure of the Subject Domain Names, the Subject Registry shall take all steps necessary to restrain and lock the domain at the registry level to ensure that changes to the Subject Domain Names cannot be made absent a court order or, if forfeited to the United States government, without prior consultation with FBI.

C. The Subject Registry shall point the Subject Domain Names to [REDACTED] and [REDACTED] at which the Government will display a web page with the following notice:

This domain name associated with the website Megaupload.com has been seized pursuant to an order issued by the U.S. District Court for the Eastern District of Virginia.

*An indictment has been returned by a grand jury in Alexandria, Virginia, charging several individuals and entities allegedly involved in the operation of Megaupload.com and related websites with the following federal crimes:
Conspiracy to Commit Racketeering (18 U.S.C. § 1962(d)),
Conspiracy to Commit Copyright Infringement (18 U.S.C. § 371),
Conspiracy to Commit Money Laundering (18 U.S.C. § 1956(h)), and
Criminal Copyright Infringement (18 U.S.C. §§ 2, 2319; 17 U.S.C. § 506).*

The case is being prosecuted by the U.S. Attorney's Office for the Eastern District of Virginia and the U.S. Department of Justice's Computer Crime and Intellectual Property Section.

D. Upon seizure of the Subject Domain Names, the Subject Registrars shall modify any records, databases, tables, or documents that are used by the Subject Registrars to identify the owner of the Subject Domain Names to reflect the seizure of the Subject Domain Names. These changes relate to the following records, if they exist:

1. The "Technical Contact" and "Administrative Contact" fields will reflect the following information:
 - a) Name: Federal Bureau of Investigation
 - b) Address: 935 Pennsylvania Ave
Washington, DC 20535
 - c) Country: USA
 - d) Telephone: 202-324-3000
 - e) Email: IPR@ic.fbi.gov
2. Any remaining fields will be changed so they do not reflect any individual or entity.

II. Subject Registry

Afilias USA, Inc.
Building 3, Suite 105
300 Welsh Road
Horsham, PA 19044

III. Subject Registrar

GoDaddy.com
14455 N. Hayden Rd., Ste. 226
Scottsdale, AZ 85260

IV. Subject Domain Name

MEGASTUFF.INFO

MEGAWORLD.MOBI

FILED

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

2012 JAN 13 P 2: 18

CLERK US DISTRICT COURT
ALEXANDRIA, VIRGINIA

In the Matter of the Seizure of:) Case No. 1:12-sw- 37
)
The Domain Names Megastuff.info and) UNDER SEAL
Megaworld.mobi)

**GOVERNMENT'S MOTION TO SEAL SEIZURE WARRANT
PURSUANT TO LOCAL RULE 49(B)**

The United States, through undersigned counsel, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, now asks for an Order to Seal the seizure warrant, the application for seizure warrant, and the affidavit in support of the seizure warrant, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal these documents.

I. REASONS FOR SEALING (See Local Rule 49(B)(1))

1. The Indictment, and arrest warrants, charging nine defendants with various crimes stemming from their involvement in a worldwide criminal enterprise related to Megaupload.com is under seal. [REDACTED]

2. While it is anticipated that the Indictment will be unsealed shortly after this seizure warrant is served, premature disclosure of the specific details of this criminal case [REDACTED]

[REDACTED]



3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. THE GOVERNING LAW (See Local Rule 49(B)(2))

4. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. Media General Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4th Cir. 2005); In re Washington Post Company v. Hughes, 923 F.2d 324, 326 (4th Cir. 1991). “But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is ‘essential to preserve higher values’ and ‘narrowly tailored to serve that interest.’” Media General Operations, 417 F.3d at 429 (citations omitted); see also In re Knight Pub. Co., 743 F.2d 231, 235 (4th Cir. 1984) (“[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public’s right of access is outweighed by competing interests”). Sealing search and seizure warrants and their accompanying affidavits and application is within the discretionary powers of a judicial officer where, among other things, an “‘affidavit contain[s] sensitive details of an ongoing investigation’ and it is ‘clear and apparent from the affidavits that any disclosure of the information there would hamper’ th[e] ongoing investigation.” Media General Operations 417 F.3d at 430 (citations omitted); see also In re Search Warrant for Matter of Eye Care Physicians of America, 100 F.3d 514, 518 (7th Cir. 1996).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. Ashcraft v. Conoco, Inc., 218 F.3d 288, 302 (4th Cir. 2000).

6. However, in the specific context of a search and seizure warrant, the Fourth Circuit has cautioned that “the opportunity to object” cannot “arise prior to the entry of a sealing order when a search warrant has not been executed.” Media General Operations, 417 F.3d at 429. “A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant.” Id.; see also Franks v. Delaware, 438 U.S. 154, 169 (1978). Accordingly, “the notice requirement is fulfilled by docketing ‘the order sealing the documents,’ which gives interested parties the opportunity to object after the execution of the search warrants.” Media General Operations, 417 F.3d at 430 (quoting Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989)); see also Local Rule 49(B) (“Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.”).

7. As to the requirement of a court’s consideration of alternatives, the Fourth Circuit counsels that, “[i]f a judicial officer determines that full public access is not appropriate, she ‘must consider alternatives to sealing the documents,’ which may include giving the public access to some of the documents or releasing a redacted version of the documents that are the subject to the government’s motion to seal.” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 66).

8. Finally, regarding the requirement of specific findings, the Fourth Circuit's precedents state that, "in entering a sealing order, a 'judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears credible,'" Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 65), so long as the ultimate "decision to seal the papers " is "made by the judicial officer," Goetz, 886 F.2d at 65. "Moreover, if appropriate, the government's submission and the [judicial] officer's reason for sealing the documents can be filed under seal." Goetz, 886 F.2d at 65; see also In re Washington Post Co., 807 F.2d 383, 391 (4th Cir. 1986) ("if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal").

III. PERIOD OF TIME GOVERNMENT SEEKS TO HAVE MATTER REMAIN UNDER SEAL (See Local Rule 49(B)(3))

9. Pursuant to Local Rule 49(B)(3), the seizure warrant, the application for a seizure warrant, and the affidavit will remain sealed until the need to maintain the confidentiality of the these documents expires and the United States moves to unseal these documents.

WHEREFORE, the United States respectfully requests that the seizure warrant, application for seizure warrant, affidavit in support of the seizure warrant, and this Motion to Seal and proposed Order be sealed until further Order of the Court. Notwithstanding this request, the United States asks to provide copies as necessary to execute the seizure warrant.

Respectfully submitted,

Neil H. MacBride
United States Attorney

By: Lindsay Kelly
Lindsay A. Kelly
Assistant United States Attorney

UNITED STATES DISTRICT COURT
for the
Eastern District of Virginia

In the Matter of the Seizure of
(Briefly describe the property to be seized)
The Domain Names Megastuff.co
and Megaclicks.co
Case No. 1:12-sw- 40
UNDER SEAL

APPLICATION FOR A WARRANT
TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, a federal law enforcement officer or attorney for the government, request a seizure warrant and state under penalty of perjury that I have reason to believe that the following property in the Eastern District of Virginia is subject to forfeiture to the United States of America under 18 U.S.C. § 981(a)(1)(C)* (describe the property):

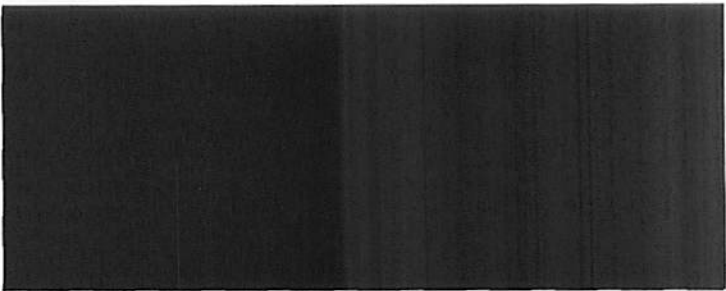
The Domain Names Megastuff.co and Megaclicks.co

* Such property is also subject to forfeiture to the United States of America under 18 U.S.C. §§ 982(a)(1), 1963(a), and 2323.

The application is based on these facts:

SEE ATTACHED AFFIDAVIT OF [REDACTED]

[X] Continued on the attached sheet.



Reviewed by AUSA
Lindsay Kelly

Printed name and title

Sworn to before me and signed in my presence.

Date: 01/18/2012

[Handwritten signature of Liam O'Grady]

Judge's signature

City and state: Alexandria, Virginia

Honorable Liam O'Grady, U.S. District Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

In the Matter of the Seizure of:) 1:12SW 40
)
The Domain Names Megastuff.co and) UNDER SEAL
Megaclicks.co

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, [REDACTED], being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. Your affiant is a [REDACTED]

[REDACTED]. I am currently assigned to [REDACTED]

[REDACTED] My duties include the investigation of crimes involving the infringement of intellectual property rights, including violations of Title 17, United States Code, Section 506 and Title 18, United States Code, Section 2319 (Criminal Infringement of a Copyright). Your affiant has directed and been involved in numerous investigations involving the use of computers and the Internet to commit violations of criminal fraud and intellectual property laws.

2. Your affiant makes this affidavit in support of the government's application, pursuant to Title 21, United States Code, Section 853(f), Title 18, United States Code, Section 2323, Title 18, United States Code, Section 1963, Title 18, United States Code, Section 982(b)(1), and Title 18, United States Code, Section 981(b)(1) for a warrant to seize the domain names Megastuff.co and Megaclicks.co (hereinafter "Subject Domain Names").

3. The procedure by which the government will seize the Subject Domain Names is described in Attachment A hereto and below.

4. As set forth below, there is probable cause to believe that the Subject Domain Names are subject to seizure and forfeiture as property constituting or derived from proceeds obtained directly or indirectly from, or used or intended to be used to facilitate the commission of criminal copyright infringement (17 U.S.C. § 506; 18 U.S.C. §§ 2319 and 2323); constituting or derived from proceeds traceable to conspiracy to commit criminal copyright infringement (18 U.S.C. §§ 371 and 981; 28 U.S.C. § 2461); involved in or traceable to conspiracy to commit money laundering (18 U.S.C. §§ 982 and 1956(h)); or constituting or derived from proceeds obtained directly or indirectly from, or acquired or maintained in violation of, conspiracy to commit racketeering (18 U.S.C. §§ 1962, 1963). This affidavit does not set forth all of your affiant's knowledge about this matter, and is intended to provide sufficient information to support probable cause.

TECHNICAL BACKGROUND

5. Based on training and experience and information learned from others, your affiant is familiar with the following terms:

a. **Internet Protocol Address:** An Internet Protocol address ("IP address") is a unique numeric address used by computers on the Internet. An IP Address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address. The assignment of IP addresses to computers connected to the Internet is controlled by Internet Service Providers ("ISPs").

b. **Domain Name:** A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g., letters, numbers, or other characters) that correspond to a particular IP address. For example, “usdoj.gov” and “cnn.com” are domain names.

c. **Domain Name System:** The domain name system (“DNS”) is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or “labels,” that are delimited by periods, such as “www.example.com.” The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the “top-level” domain. For example, the domain name “www.example.com” means that the computer assigned that name is in the “.com” top-level domain, and the “example” second-level domain.

d. **Domain Name Registry:** DNS servers are computers connected to the Internet that convert, or resolve, domain names into IP addresses. For each top-level domain (such as “.com”), there is a single company, called a “registry,” that determines which second-level domain resolves to which IP address. The registry for the “.co” top-level domain is .co Internet SAS.

e. **Registrar & Registrant:** Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The registrar used to register the Megastuff.co and Megaclicks.co domain names was GoDaddy.com. The individual or business that purchases, or registers, a domain name is called a “registrant.” Registrants control the IP address, and thus the computer, to which their domain name resolves. A registrant may easily move a domain name to another computer anywhere in

the world. Typically a registrar will provide a registrant with the ability to change the IP address a particular domain name resolves to through an online interface.

PROBABLE CAUSE FOR SEIZURE AND FORFEITURE

6. In March 2010, [REDACTED] initiated an investigation of a worldwide criminal organization known as the “Mega Conspiracy,” which was believed to be hosting and distributing unauthorized copies of copyrighted works over the Internet. The Mega Conspiracy consists of a series of websites and services, including a video hosting and distribution service located at the domain Megavideo.com; an adult video hosting and distribution service located at the domain Megaporn.com; a file hosting and distribution service located at the domain Megaupload.com; an advertising service associated with its other websites located at the domain Megaclick.com; and a number of associated websites. DEFENDANTS and others are members of the Mega Conspiracy, which has operated since at least September 2005 and is estimated to have caused harm to copyright holders in excess of \$500,000,000 and generated more than \$175,000,000 in revenue.

7. Once a user uploads a file to Megaupload.com, the system provides the user with a specific and unique Uniform Resource Locator (“URL link”) from which the file can be downloaded or viewed. If a video file is uploaded, an individual can use the provided URL link to redirect others to the related website Megavideo.com to view the file via the website’s Flash video player. Users can also embed the Flash video player from Megavideo.com into another website to display the video file there. Megaupload.com supports a vast landscape of websites offering the Megupload.com-provided URL links to view unauthorized copies of copyrighted motion pictures and television programs that are being hosted on servers controlled

by the Mega Conspiracy. Once a video has been viewed, a user also has the ability to download and save the video to his computer.

8. Your affiant has reviewed the Indictment in this case and believes it to be accurate and consistent with the investigation. Paragraph 18 of the Indictment alleges that, before any video can be viewed on Megavideo.com, the user must view an advertisement. Originally, the Mega Conspiracy had contracted with companies such as adBrite, Inc., Google AdSense, and PartyGaming plc for Internet advertising. Currently, the Mega Conspiracy's own advertising website, Megaclick.com, is used to set up advertising campaigns on all the Mega Conspiracy websites. The high traffic volume on the Mega Conspiracy websites allows the Mega Conspiracy to charge advertisers up-front and at a higher rate than would be achieved by the percentage-per-click methodology used by other popular Internet advertising companies. The popularity of the infringing content on the Mega Conspiracy websites has generated more than \$25 million in online advertising revenues.

9. Paragraph 9 of the Indictment alleges that, in addition to displaying online advertisements, the download pages on Megaupload.com are designed to increase premium subscriptions. All non-premium users are encouraged to buy a premium subscription to decrease wait and download times, which can be at least an hour for popular content (and, for some periods of time, these non-premium users have been ineligible to download files over a certain size). As a result, non-premium users are repeatedly asked by the Mega Conspiracy to pay for more and faster access to content on Megaupload.com.

10. Using an undercover computer, [REDACTED] observed how a visitor may view content hosted on Megaupload.com. For example, on November 20, 2011, [REDACTED] observed

the copyrighted motion picture *Zack and Miri Make a Porno*, which was released in 2008 by The Weinstein Company, on the website Megavideo.com. When the file was selected, the URL link redirected to www.megavideo.com/?v=REYCBLNF and a file entitled “[Película] Zack and Miri Make a Porno VOSE” was streamed. The same day, [REDACTED] located the copyrighted motion picture *The Twilight Saga: Breaking Dawn - Part 1* on the website www.peliculasyonkis.com. When selected, the URL link redirected to www.megavideo.com/?s=seriesyonkis&v=HY01ZGSR, where [REDACTED] viewed a camcorder version of the copyrighted motion picture, which had been released in United States theaters only two days prior, on November 18, 2011.

11. Paragraph 10 of the Indictment alleges that the content available from Megaupload.com is not searchable on the website, which allows the Mega Conspiracy to conceal the scope of its infringement. Instead of hosting a search function on its own site, the Mega Conspiracy business model purposefully relies on thousands of third party “linking” sites, which contain user-generated postings of links created by Megaupload.com (as well as those created by other Mega Conspiracy websites, including Megavideo.com and Megaporn.com). While the Mega Conspiracy may not operate these third party sites, the Mega Conspiracy did provide financial incentives for premium users to post links on linking sites through the “Uploader Rewards” program, which ensured widespread distribution of Megaupload.com links throughout the Internet and an inventory of popular content on servers controlled by the Mega Conspiracy. These linking sites, which are usually well organized, promote and direct users to Mega Conspiracy download pages that allow the reproduction and distribution of infringing copies of copyrighted works.

12. Paragraph 14 of the Indictment alleges that, in contrast to the public, which is required to significantly rely on third party indexes, members of the Mega Conspiracy have full access to the listings of actual files that are stored on servers they control (as well as the Megaupload.com- and Megavideo.com- and Megaporn.com-generated links to those files). Conspirators have searched the internal database in order to directly access copyright-infringing content on servers controlled by the Mega Conspiracy.

13. Paragraph 19 of the Indictment alleges that, like Megaupload.com, Megavideo.com conceals many of the infringing copies of popular copyrighted videos that are available on and distributed by the website. Megavideo.com does purport to provide both browse and search functions, but any user's search on Megavideo.com for a full length copyrighted video (which can be downloaded from a Mega Conspiracy-controlled server somewhere in the world) will not produce any results. Similarly, browsing the front page of Megavideo.com does not show any obviously infringing copies of any copyrighted works; instead, the front page contains videos of news stories, user-generated videos, and general Internet videos in a manner substantially similar to Youtube.com. Browsing the most-viewed videos in the Entertainment category on Megavideo.com, however, has at times revealed a number of infringing copies of copyrighted works that are available from Mega Conspiracy-controlled servers and are amongst the most viewed materials being offered.

14. The Mega Conspiracy uses e-mail addresses with the extension @megaupload.com in the operation of the Megaupload.com website. [REDACTED] the e-mail account megaupload.support@gmail.com revealed the e-mail address abuse@megaupload.com has received and continues to receive thousands of DMCA

infringement notices from copyright holders, including but not limited to Warner Bros. Entertainment Inc., Sony Music Entertainment Inc., and the Business Software Alliance. The e-mails provided notice of the existence of unauthorized copies of copyrighted motion pictures, television shows, software, literature, and music on servers controlled by the Mega Conspiracy. The notice e-mails contained the URL links to the locations on Megaupload.com where the infringing copies of copyrighted works resided. ██████████ review of other e-mails has shown that the Mega Conspiracy operators are willfully violating copyright law by ignoring notices of selected infringing content, and are actually uploading infringing content themselves to Mega Conspiracy websites.

15. Using publicly available software that can detect the IP addresses of data incoming to the undercover computer, ██████████ was able to determine that the copyrighted content hosted on Megaupload.com was being downloaded from computers assigned IP addresses held by three commercial Internet hosting service companies: Carpathia Hosting, headquartered in Dulles, Virginia, with datacenters in Ashburn, Virginia, both of which are located in the Eastern District of Virginia; Cogent Communications, headquartered in Washington, D.C., with datacenters in Washington, D.C. and France; and Leaseweb in the Netherlands. Each of these Internet hosting service companies leases high-speed computer server space and Internet connectivity to the public.

16. On or about June 24, 2010, members of the Mega Conspiracy were informed, pursuant to a criminal search warrant from the U.S. District Court for the Eastern District of Virginia, that thirty-nine infringing copies of copyrighted motion pictures were present on their leased servers at Carpathia Hosting, a hosting company headquartered in the Eastern District of

Virginia. A member of the Mega Conspiracy informed several of his co-conspirators at that time that he located the named files using internal searches of the Mega Conspiracy's systems. As of November 18, 2011, thirty-six of the thirty-nine infringing copies of copyrighted motion pictures were still being stored on servers controlled by the Mega Conspiracy.

17. In addition to Megaupload.com, Megavideo.com, and Megaclick.com, other websites created and domains owned by the Mega Conspiracy include: Megaworld.com; Megastuff.co; Megaclicks.co; Megastuff.info; Megaclicks.org; Megaworld.mobi; Megastuff.org; Megaclick.us; Mageclick.com; HDmegaporn.com; Megaporn.com; Megavkdeo.com; Megarotic.com; and Megavideoclips.com. At least two of these additional sites have also hosted infringing copies of copyrighted works. The websites and services, as well as the domains themselves, have been facilitated and promoted by illicit proceeds from the operations of Megaupload.com, Megavideo.com, and Megaclick.com.

THE SUBJECT DOMAIN

18. [REDACTED] the Megastuff.co domain was registered on or about November 13, 2010, and that the Megaclicks.co domain was registered on or about November 24, 2010. The registrant and account holder for both domains was indicated to be "Domain Administrator" at Megamedia Ltd, in Hong Kong. [REDACTED] on [REDACTED] or about May 20, 2006, DOTCOM registered the company Megamedia Limited in Hong Kong with company registry number 1046613. The company director is listed as KIM TIM JIM VESTOR (a known alias of DOTCOM), with Finland passport no. [REDACTED], and VESTOR LIMITED is listed as the sole shareholder

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

19. Title 18, United States Code, Section 2323(a)(1)(A) and (B) and 2323(b) provide, in relevant part, that any property used, or intended to be used to commit or facilitate criminal copyright infringement, or constituting or derived from proceeds obtained directly or indirectly from the commission of criminal copyright infringement, are subject to both civil and criminal forfeiture. Title 18, United States Code, Section 2323(b)(2) authorizes the use of procedures set forth in Title 21, United States Code, Section 853 for the seizure of property subject to criminal forfeiture.

20. Title 18, United States Code, Sections 981(a)(1) and 982(a)(1) provide that a defendant who is convicted of money laundering shall forfeit to the United States “any property involved in the offense, or any property traceable to such property. Title 18, United States Code, Section 982(b)(1) authorizes the use of procedures set forth in Title 21, United States Code, Section 853 for the seizure of property subject to criminal forfeiture.

21. Where there is probable cause to believe that the property to be seized is subject to forfeiture and that an order pursuant to Title 21, United States Code, Section 853(e) may not be sufficient to assure its availability for forfeiture, a district court may issue a warrant authorizing the seizure of such property. 21 U.S.C. § 853(f). Section 853(f) provides that:

The Government may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant. If the court determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that an order under subsection (e) may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property.

A seizure warrant issued under Title 21, United States Code, Section 853(f) has nationwide scope. 21 U.S.C. § 853(l).

22. In addition, Title 18, United States Code, Section 1963(a) provides that any defendant who is convicted of racketeering activity shall forfeit to the United States any property constituting, or derived from, any proceeds which the person obtained, directly or indirectly, from the racketeering activity. Title 18, United States Code, Section 1963(d)(1) provides that:

Upon application of the United States, the court may enter a restraining order or injunction, require the execution of a satisfactory performance bond, or take any other action to preserve the availability of property described in subsection (a) for forfeiture under this section—

(A) upon the filing of an indictment or information charging a violation of section 1962 of this chapter and alleging that the property with respect to which the order is sought would, in the event of conviction, be subject to forfeiture under this section

A seizure warrant issued under Title 21, United States Code, Section 1963(d) has nationwide scope. 18 U.S.C. § 1963(j).

23. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the Subject Domain Names for forfeiture. By seizing the Subject Domain Names and redirecting them to another website, the United States will prevent supporters of the Mega Conspiracy or third parties from redirecting the Subject Domain Names to servers elsewhere in the world, and thus using them to commit additional crimes. Furthermore, seizure of the Subject Domain Names will prevent visitors from continuing to access the websites located at the Subject Domain Names.

24. Title 18, United States Code, Section 2319(a)(2) provides that the procedures set forth in Chapter 46 of Title 18 (18 U.S.C. § 981, et seq.) shall extend to civil forfeitures under

Section 2323(a). Title 18, United States Code, Section 981(b)(1) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause. Title 18, United States Code, Section 981(b)(3) permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed and may be executed in any district in which the property is found.

25. As set forth above, there is probable cause to believe that the Subject Domain Names are subject to both civil and criminal forfeiture because they were used in the commission of criminal copyright infringement, conspiracy to commit criminal copyright infringement, conspiracy to commit racketeering, and conspiracy to commit money laundering.

SEIZURE PROCEDURE

26. As detailed in Attachment A, upon execution of the seizure warrant, the registry for the top-level domain shall be directed to restrain and lock the Subject Domain Names pending transfer of all right, title, and interest in the Subject Domain Names to the United States upon completion of forfeiture proceedings, to ensure that changes to the Subject Domain Names cannot be made absent court order or, if forfeited to the United States, without prior consultation with FBI.

27. In addition, upon seizure of the Subject Domain Names, the registry for the top-level domain will be directed to point the Subject Domain Names to IP addresses controlled by the United States, which will display a web page providing public notice of the website seizure.

28. The domain name registrars also maintain certain records relating to the owner of each domain name for which it is the top-level registry, including the Subject Domain Names (the "Domain Name Records"). Certain of these records are available to the public through a

“Whois” lookup through a web browser, among other means. At the time the Subject Domain Names are seized, the registrars will be directed to change the “Technical Contact” and “Administrative Contact” fields of the Domain Name Records for the Subject Domain Names to contact information relating to FBI to reflect the fact that the Subject Domain Names have been seized; and to change the name server fields of the Domain Name Records to effect the forgoing changes. All other fields will be changed so that they do not reflect any individual or entity.

29. Upon completion of forfeiture proceedings, all Domain Name Records for the Subject Domain Names maintained by the top-level registry and the domain name registrars will be changed to reflect the transfer of ownership to the United States.

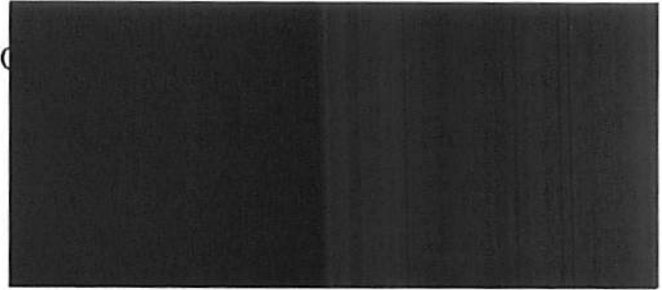
CONCLUSION

30. Based on the information contained in the Indictment and this affidavit there is probable cause to believe that the Subject Domain Names are subject to seizure and forfeiture as property constituting or derived from proceeds obtained directly or indirectly from, or used or intended to be used to facilitate, the commission of criminal copyright infringement (17 U.S.C. § 506; 18 U.S.C. §§ 2319 and 2323); constituting or derived from proceeds traceable to conspiracy to commit criminal copyright infringement (18 U.S.C. §§ 371 and 981; 28 U.S.C. § 2461); involved in or traceable to the conspiracy to commit money laundering (18 U.S.C. §§ 982 and 1956(h)); or constituting or derived from proceeds obtained directly or indirectly from, or acquired in maintained in violation of, a conspiracy to commit racketeering (18 U.S.C. §§ 1962 and 1963).

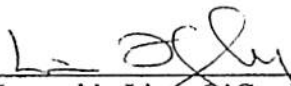
Accordingly, it is requested that a seizure warrant be issued for the Subject Domain

Names.

FURTHER THIS AFFIANT SAYETH NO



Subscribed to and sworn before me on this 18th day of January, 2012.



Honorable Liam O'Grady
United States District Judge

Submitted by Lindsay A. Kelly
Assistant United States Attorney

ATTACHMENT A

I. Seizure Procedure

A. The seizure warrant will be presented in person or transmitted via facsimile or email to personnel of the domain name registry listed in Section II (“Subject Registry”) and the domain name registrars listed in Section III (“Subject Registrars”) who will be directed, for the domain name listed in Section IV (“Subject Domain Names”) for which it serves as the top-level domain registry, to make any changes necessary to restrain and lock the Subject Domain Names pending transfer of all rights, title, and interest in the Subject Domain Names to the United States upon completion of forfeiture proceedings.

B. Upon seizure of the Subject Domain Names, the Subject Registry shall take all steps necessary to restrain and lock the domain at the registry level to ensure that changes to the Subject Domain Names cannot be made absent a court order or, if forfeited to the United States government, without prior consultation with FBI.

C. The Subject Registry shall point the Subject Domain Names to [REDACTED] and [REDACTED] at which the Government will display a web page with the following notice:

This domain name associated with the website Megaupload.com has been seized pursuant to an order issued by the U.S. District Court for the Eastern District of Virginia.

*An indictment has been returned by a grand jury in Alexandria, Virginia, charging several individuals and entities allegedly involved in the operation of Megaupload.com and related websites with the following federal crimes:
Conspiracy to Commit Racketeering (18 U.S.C. § 1962(d)),
Conspiracy to Commit Copyright Infringement (18 U.S.C. § 371),
Conspiracy to Commit Money Laundering (18 U.S.C. § 1956(h)), and
Criminal Copyright Infringement (18 U.S.C. §§ 2, 2319; 17 U.S.C. § 506).*

The case is being prosecuted by the U.S. Attorney’s Office for the Eastern District of Virginia and the U.S. Department of Justice’s Computer Crime and Intellectual Property Section.

D. Upon seizure of the Subject Domain Names, the Subject Registrars shall modify any records, databases, tables, or documents that are used by the Subject Registrars to identify the owner of the Subject Domain Names to reflect the seizure of the Subject Domain Names. These changes relate to the following records, if they exist:

1. The "Technical Contact" and "Administrative Contact" fields will reflect the following information:
 - a) Name: Federal Bureau of Investigation
 - b) Address: 935 Pennsylvania Ave
Washington, DC 20535
 - c) Country: USA
 - d) Telephone: 202-324-3000
 - e) Email: IPR@ic.fbi.gov
2. Any remaining fields will be changed so they do not reflect any individual or entity.

II. Subject Registry

.co Internet SAS
World Trade Center
Calle 100 No. 8 A - 49
Torre B ofc. 507
Bogotá, Columbia

III. Subject Registrar

GoDaddy.com
14455 N. Hayden Rd., Ste. 226
Scottsdale, AZ 85260

IV. Subject Domain Name

Megaclicks.co
Megastuff.co

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

In the Matter of the Seizure of:) Case No. 1:12-sw-40
)
The Domain Names Megastuff.co and) UNDER SEAL
Megaclicks.co)

**GOVERNMENT'S MOTION TO SEAL SEIZURE WARRANT
PURSUANT TO LOCAL RULE 49(B)**

The United States, through undersigned counsel, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, now asks for an Order to Seal the seizure warrant, the application for seizure warrant, and the affidavit in support of the seizure warrant, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal these documents.

I. REASONS FOR SEALING (See Local Rule 49(B)(1))

1. The Indictment, and arrest warrants, charging nine defendants with various crimes stemming from their involvement in a worldwide criminal enterprise related to Megaupload.com is under seal. [REDACTED]

2. While it is anticipated that the Indictment will be unsealed shortly after this seizure warrant is served, premature disclosure of the specific details of this criminal case [REDACTED]

[REDACTED]



3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. THE GOVERNING LAW (See Local Rule 49(B)(2))

4. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. Media General Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4th Cir. 2005); In re Washington Post Company v. Hughes, 923 F.2d 324, 326 (4th Cir. 1991). “But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is ‘essential to preserve higher values’ and ‘narrowly tailored to serve that interest.’” Media General Operations, 417 F.3d at 429 (citations omitted); see also In re Knight Pub. Co., 743 F.2d 231, 235 (4th Cir. 1984) (“[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public’s right of access is outweighed by competing interests”). Sealing search and seizure warrants and their accompanying affidavits and application is within the discretionary powers of a judicial officer where, among other things, an “‘affidavit contain[s] sensitive details of an ongoing investigation’ and it is ‘clear and apparent from the affidavits that any disclosure of the information there would hamper’ th[e] ongoing investigation.” Media General Operations 417 F.3d at 430 (citations omitted); see also In re Search Warrant for Matter of Eye Care Physicians of America, 100 F.3d 514, 518 (7th Cir. 1996).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. Ashcraft v. Conoco, Inc., 218 F.3d 288, 302 (4th Cir. 2000).

6. However, in the specific context of a search and seizure warrant, the Fourth Circuit has cautioned that “the opportunity to object” cannot “arise prior to the entry of a sealing order when a search warrant has not been executed.” Media General Operations, 417 F.3d at 429. “A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant.” Id.; see also Franks v. Delaware, 438 U.S. 154, 169 (1978). Accordingly, “the notice requirement is fulfilled by docketing ‘the order sealing the documents,’ which gives interested parties the opportunity to object after the execution of the search warrants.” Media General Operations, 417 F.3d at 430 (quoting Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989)); see also Local Rule 49(B) (“Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.”).

7. As to the requirement of a court’s consideration of alternatives, the Fourth Circuit counsels that, “[i]f a judicial officer determines that full public access is not appropriate, she ‘must consider alternatives to sealing the documents,’ which may include giving the public access to some of the documents or releasing a redacted version of the documents that are the subject to the government’s motion to seal.” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 66).

8. Finally, regarding the requirement of specific findings, the Fourth Circuit's precedents state that, "'in entering a sealing order, a 'judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears creditable,'" Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 65), so long as the ultimate "decision to seal the papers " is "made by the judicial officer," Goetz, 886 F.2d at 65. "Moreover, if appropriate, the government's submission and the [judicial] officer's reason for sealing the documents can be filed under seal." Goetz, 886 F.2d at 65; see also In re Washington Post Co., 807 F.2d 383, 391 (4th Cir. 1986) ("if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal").

III. PERIOD OF TIME GOVERNMENT SEEKS TO HAVE MATTER REMAIN UNDER SEAL (See Local Rule 49(B)(3))

9. Pursuant to Local Rule 49(B)(3), the seizure warrant, the application for a seizure warrant, and the affidavit will remain sealed until the need to maintain the confidentiality of the these documents expires and the United States moves to unseal these documents.

WHEREFORE, the United States respectfully requests that the seizure warrant, application for seizure warrant, affidavit in support of the seizure warrant, and this Motion to Seal and proposed Order be sealed until further Order of the Court. Notwithstanding this request, the United States asks to provide copies as necessary to execute the seizure warrant.

Respectfully submitted,

Neil H. MacBride
United States Attorney

By: 
Lindsay A. Kelly
Assistant United States Attorney

AO 93 (Rev. 12/09) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the Eastern District of Virginia

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address)
THE PREMISES LOCATED AT 21691 Fillgree Court,)
21701 Fillgree Court, and 21715 Fillgree Court., Bldg. D.)
Ashburn, VA 20147)

Case No. 1:12SW41

UNDER SEAL

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Virginia (identify the person or describe the property to be searched and give its location): Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before February 1, 2012 (not to exceed 14 days)

- in the daytime 6:00 a.m. to 10 p.m. at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Liam O'Grady, U.S. District Judge (name)

- I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) for days (not to exceed 30). until, the facts justifying, the later specific date of

Date and time issued: 1/18/12 4:27 PM

[Handwritten Signature] Judge's signature

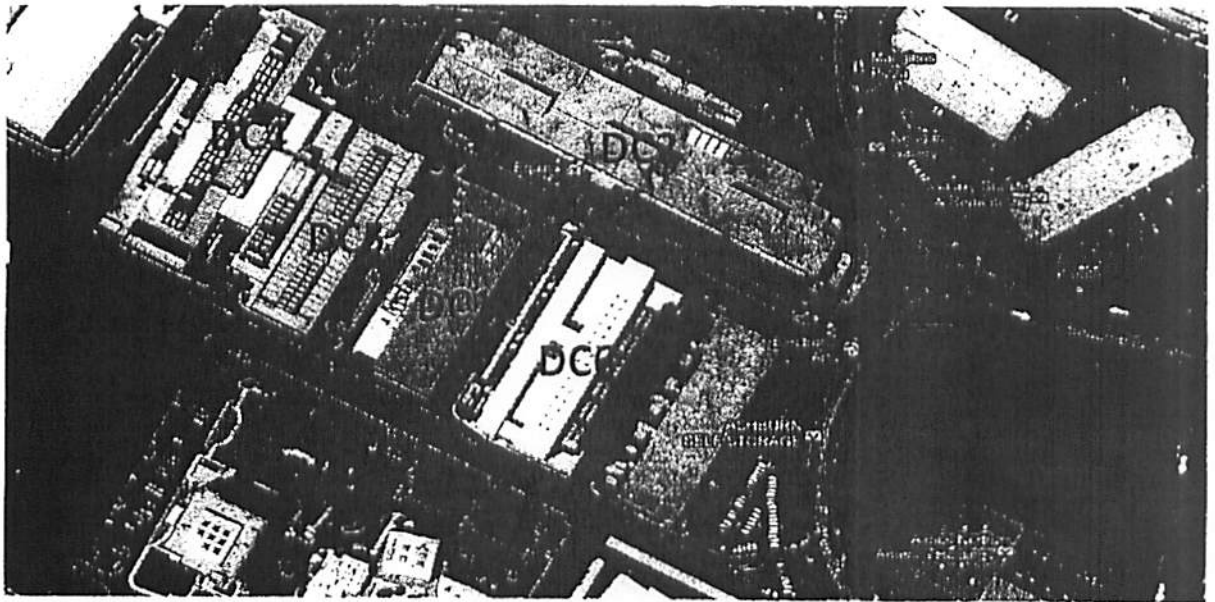
City and state: Alexandria, VA

Honorable Liam O'Grady, U.S. District Judge Printed name and title

Attachment A

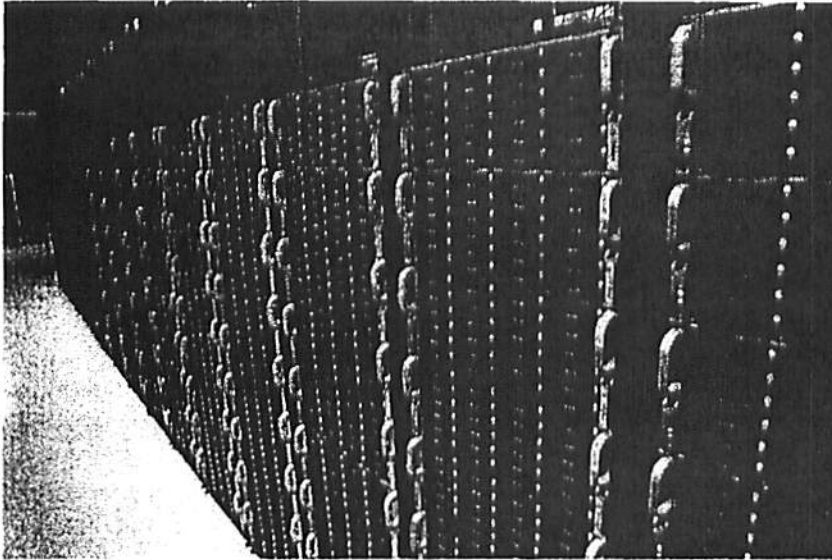
PREMISES TO BE SEARCHED

The SUBJECT PREMISES consists of several buildings that are part of a data center campus owned by Equinix. Carpathia leases warehouse space on this campus from Equinix and, in turn, leases servers housed on this campus to the Mega Conspiracy. The Equinix data center campus consists of a complex of six warehouse-type one-story office buildings, identified by Equinix as buildings DC1 through DC6. The SUBJECT PREMISES includes buildings housing servers leased by Carpathia to the Mega Conspiracy, and includes at least those buildings identified as DC2, DC4, and DC5. The photograph below shows the relative layout of buildings DC2, DC4, and DC5 on the Equinix campus.



Building DC2 is a warehouse building approximately 147,600 square feet in size, constructed of tan concrete on a concrete slab foundation. The address for building DC2 is 21715 Filigree Court, Ashburn, VA 20147. The numbers "21715" are displayed at the top corner of the building exterior. The building interior consists of a series of metal-enclosed cages storing computer servers. The cages have key locks or biometric locks, and are generally numbered.

Building DC4 is a warehouse building approximately 100,000 square feet in size, constructed of tan concrete on a concrete slab foundation. The address for building DC5 is 21691 Filigree Court, Ashburn, VA 20147. The numbers "21691" are displayed at the top corner of the building exterior. The photograph copied below is believed to depict some of the Mega Conspiracy servers housed at the DC4 building.



Building DC5 is a warehouse building approximately 148,000 square feet in size, constructed of tan concrete on a concrete slab foundation. The address for building DC5 is 21701 Filigree Court, Building D, Ashburn, VA 20147. The numbers "21701" are displayed at the top corner of the building exterior. The entrance to DC5 is a single door of tinted glass, directly behind to three narrow cylindrical concrete barriers separating the entrance door from a parking space. Adjacent to the entrance door there are tinted windows to the right. There are also more tinted windows to the left, separated by a narrow portion of the stone building wall. The letter "D" is displayed above, and slightly to the left of, the entry door.

The premises to be searched includes all cages containing servers leased by Carpathia to the Mega Conspiracy, including but not limited to those in buildings DC2, DC4, and DC5.

Attachment B

ITEMS TO BE SEIZED

Evidence or instrumentalities of violations of Title 18, United States Code, Sections 2 (Aiding and Abetting), 371 (Conspiracy), 1956(h) (Money Laundering), 1962(d) (Racketeering), 2319 (Copyright Infringement); or Title 17, United States Code, Section 506 (Copyright Infringement), including the following:

A. All servers leased or used by MEGAUPLOAD LIMITED, Megaupload.com, Megavideo.com, or associated websites or entities, including but not limited to:

a. Servers identified as:

mega076
mega-ash-3006
mega-ash-3007
mega-ash-3008
mega-ash-3009
mega-ash-3012
mega-ash-3013
mega-ash-3014
mega-ash-3015
mega-ash-3016
mega-ash-3017
mega-ash-3018
mega-ash-3019
mega-ashdc4-3024
mega-ashdc4-3025
mega-ashdc4-3026
mega-ashdc4-3102
mega-ashdc4-3104
mega-ashdc4-3106
mega-ashdc4-3108
mega-ashdc4-3110
mega-ashdc4-3112
mega-ashdc5-1071

b. Servers with the following assigned IP addresses:

174.140.154.12
174.140.154.13
174.140.154.14
174.140.154.15
174.140.154.18
174.140.154.19
174.140.154.20

174.140.154.21
174.140.154.22
174.140.154.23
174.140.154.24
174.140.154.25
174.140.154.28
174.140.154.29
174.140.154.30
174.140.154.31
174.140.154.32
174.140.154.43
174.140.154.45
174.140.154.47
174.140.154.49
174.140.154.51
174.140.154.58
174.140.154.60

c. Servers accessible at the following URLs:

www44.megaupload.com through www49.megaupload.com,
www146.megaupload.com through www164.megaupload.com,
www400.megaupload.com through www599.megaupload.com,
www700.megaupload.com through www798.megaupload.com,
www900.megaupload.com through www952.megaupload.com,
www997.megaupload.com through www999.megaupload.com,
www44.megavideo.com through www49.megavideo.com,
www146.megavideo.com through www164.megavideo.com,
www400.megavideo.com through www599.megavideo.com,
www700.megavideo.com through www798.megavideo.com,
www900.megavideo.com through www952.megavideo.com, and
www997.megavideo.com through www999.megavideo.com.

- B. Records located on the hard drives, RAM, or other storage media incorporated into or attached to the computers described in paragraph A of this Attachment;
- C. Records relating to the unauthorized distribution of copyrighted motion pictures, television programs, musical recordings, electronic books, images, video games, or other computer software, in violation of 18 U.S.C. §§ 2, 2319 & 18 U.S.C. § 506;
- D. Passwords, encryption keys, and other access devices that may be necessary to access the above-listed servers;
- E. Documentation and manuals that may be necessary to access or to conduct a forensic examination of the above-listed servers;

- F. **Contextual information necessary to understand the evidence described in this attachment.**

AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the Eastern District of Virginia

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address)

THE PREMISES LOCATED AT 21691 Filigree Court, 21701 Filigree Court, and 21715 Filigree Court., Bldg. D, Ashburn, VA 20147

Case No. 1:12SW 41

UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- [x] evidence of a crime;
[x] contraband, fruits of crime, or other items illegally possessed;
[x] property designed for use, intended for use, or used in committing a crime;
[] a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Table with 2 columns: Code Section (18 §§ 2, 371, 1956(h), 1962(d), and 2319; 17 § 506) and Offense Description (Aiding and Abetting, Conspiracy, Money Laundering, Racketeering, and Copyright Infringement).

The application is based on these facts:

See Attached Affidavit

- [x] Continued on the attached sheet.
[] Delayed notice of ___ days (give exact ending date if more than 30 days: ___) is requested under 18 U.S.C. § 3103a, the basis of which is set forth in the attached affidavit.

Reviewed by AUSA/SAUSA:

Lindsay Kelly, AUSA

[Redacted signature area]

Applicant's signature

[Redacted name area]

Printed name and title

Sworn to before me and signed in my presence.

Date: 01/18/2012

[Handwritten signature of Liam O'Grady]

Judge's signature

City and state: Alexandria, Virginia

Honorable Liam O'Grady, U.S. District Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE SEARCH OF)
)
THE PREMISES LOCATED AT) Crim. No.: 1:12-sw-41
21691 Filigree Court, 21701 Filigree Court,) UNDER SEAL
and 21715 Filigree Court, Bldg. D,)
Ashburn, VA 20147)

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, [REDACTED], being duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a [REDACTED]

[REDACTED]. I am currently assigned to [REDACTED]

[REDACTED]

[REDACTED]. My duties include the investigation of crimes involving the infringement of intellectual property rights, including violations of Title 17, United States Code, Section 506 and Title 18, United States Code, Section 2319 (Criminal Infringement of a Copyright). I have directed and been involved in numerous investigations involving the use of computers and the Internet to commit violations of criminal fraud and intellectual property laws.

2. This affidavit is made in support of an application for a warrant to:

- a. Search the premises located at 21691 Filigree Court, 21701 Filigree Court, and 21715 Filigree Court., Bldg. D, Ashburn, VA 20147 (the "SUBJECT PREMISES"), which are more particularly described in Attachment A; and
- a. Seize the items specified in Attachment B, which constitutes instrumentalities or evidence of violations of Title 18, United States Code, Sections 2, 371, 1956(h), 1962(d), 2319; or Title 17, United States Code, Section 506.

3. The facts in this affidavit come from my personal observations, training, and experience, as well as information obtained from other agents and witnesses.

4. This affidavit is intended only to show there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

THE GOVERNMENT'S INVESTIGATION

5. In March 2010, the FBI initiated an investigation of a worldwide criminal organization known as the "Mega Conspiracy," which was believed to be hosting and distributing unauthorized copies of copyrighted works over the Internet. The Mega Conspiracy consists of a series of websites and services, including a video hosting and distribution service located at the domain Megavideo.com; an adult video hosting and distribution service located at the domain Megaporn.com; a file hosting and distribution service located at the domain Megaupload.com; an advertising service associated with its other websites located at the domain Megaclick.com; and a number of related websites.

6. The information set forth in this affidavit was derived primarily from three categories of sources. First, the general operation of Megaupload.com, Megavideo.com, and related websites was established through multiple undercover visits to the websites by FBI agents, including visits in which infringing copies of copyrighted works were both uploaded and downloaded. Second, financial records [REDACTED] documented transactions between the Mega Conspiracy, subscribers, advertisers and service providers. Third, the FBI obtained e-mails between and among DEFENDANTS and third parties.

7. The FBI investigation has revealed that, once a user uploads a file to Megaupload.com, the website's system provides the user with a specific and unique Uniform Resource Locator ("URL link"), which is an Internet address that points to the location on a

server from which the file uploaded by that user can be downloaded or viewed. Uploaders frequently attempt to upload files, including infringing copies of copyrighted works, that are already present on servers controlled by the Mega Conspiracy. When that happens, the subsequent copies of the file are not in fact re-uploaded and stored. Instead, the Megaupload.com system simply generates another unique URL link, which points to the previously-uploaded file. Therefore, at any given time, numerous unique Megaupload.com-generated URL links point to the same file on Mega Conspiracy-controlled servers.

8. A user who has uploaded a file to Megaupload.com can distribute the file to others in several ways: by distributing the URL link to others; by posting the URL link on a public website; or, in the case of video files, by embedding the Flash video player available from the related website Megavideo.com on yet another website, which would allow visitors to view the uploaded file from servers controlled by the Mega Conspiracy without ever having to visit one of the Mega Conspiracy websites. Instead, as discussed in paragraph 11, users can view infringing content stored on servers controlled by the Mega Conspiracy through one or more of the thousands of “linking” sites that organize and provide links to Megaupload.com files.

9. If a video file is uploaded, an individual can use the URL link generated by the Megaupload.com system to redirect others to either the Megaupload.com website or the Megavideo.com website. With a Megaupload.com URL link, a visitor can download the video for viewing on his personal computer. With the Megavideo.com URL link, a visitor can either download the file or view the file in a streaming format through the Megavideo.com website’s Flash video player.

10. The FBI investigation has revealed that, before any video can be viewed on Megavideo.com, the user must view an advertisement. Originally, the Mega Conspiracy had

contracted with companies such as adBrite, Inc., Google AdSense, and PartyGaming plc for Internet advertising. Currently, the Mega Conspiracy's own advertising website, Megaclick.com, is used to set up advertising campaigns on all the Mega Conspiracy websites. The high traffic volume on the Mega Conspiracy websites allows the Mega Conspiracy to charge advertisers up-front and at a higher rate than would be achieved by the percentage-per-click methodology used by other popular Internet advertising companies. The popularity of the infringing content on the Mega Conspiracy websites has generated more than \$25 million in online advertising revenues for the Mega Conspiracy.

11. The FBI investigation has revealed that, in addition to displaying online advertisements, the download pages on Megaupload.com are designed to increase revenue to the Mega Conspiracy from premium subscriptions. Whereas non-premium users are subject to delays in uploading and downloading, are ineligible to download files over a certain size, are limited to viewing a certain length of video (which is shorter than most motion picture lengths), and are subject to having uploaded files deleted after a certain period of inactivity, premium users have no such restrictions. Premium memberships may be purchased through Paypal (or Moneybookers, a European counterpart to Paypal) by increments ranging from a day to a lifetime. During visits to Mega Conspiracy websites, non-premium users are repeatedly asked by the Mega Conspiracy to pay for a premium subscription.

12. Using an undercover computer, the FBI has observed how a visitor may view content hosted on Megaupload.com. For example, on November 20, 2011, [REDACTED] observed the copyrighted motion picture *Zack and Miri Make a Porno*, which was released in 2008 by The Weinstein Company, listed on the website Megavideo.com. When the file was selected, the URL link redirected to www.megavideo.com/?v=REYCLBNF and a file entitled "[Película] Zack and

Miri Make a Porno VOSE” was streamed. The same day, [REDACTED] located the copyrighted motion picture *The Twilight Saga: Breaking Dawn - Part 1* on the website www.peliculasyonkis.com. When selected, the URL link redirected to www.megavideo.com/?s=seriesyonkis&v=HY01ZGSR, where [REDACTED] viewed a camcorder version of the copyrighted motion picture, which had been released in United States theaters only two days prior, on November 18, 2011.

13. The FBI investigation has revealed that the content available from Megaupload.com is not searchable on the website, which allows the Mega Conspiracy to conceal the scope of its infringement. Instead of hosting a search function on its own site, the Mega Conspiracy business model purposefully relies on thousands of third party “linking” websites, which contain user-generated postings of links created by Megaupload.com (as well as those created by other Mega Conspiracy websites, including Megavideo.com and Megaporn.com). These linking websites, which are usually well-organized, promote and direct users to Mega Conspiracy download pages that facilitate the reproduction and distribution of infringing copies of copyrighted works. Although the Mega Conspiracy may not operate these third party websites, the Mega Conspiracy generates URL links for these third party websites and encouraged the third party websites to disseminate these URL links widely throughout the Internet by the use of financial incentives known as the “Uploader Rewards” program, which rewarded premium users whose URL links enjoyed the most “hits” with prizes such as cash rewards.

14. The FBI investigation has revealed that, in contrast to the public, which is required to significantly rely on third party indices, members of the Mega Conspiracy have full access to the listings of actual files that are stored on servers they control (as well as the

Megaupload.com- and Megavideo.com- and Megaporn.com-generated URL links to those files).
Conspirators have searched the internal Mega Conspiracy database in order to directly access copyright-infringing content on servers controlled by the Mega Conspiracy.

15. The FBI investigation has revealed that, like Megaupload.com, Megavideo.com conceals many of the infringing copies of copyrighted videos that are available on and distributed by the website. Megavideo.com purports to provide both browse and search functions, but any user's search on Megavideo.com for a video title will not produce search results that include a full-length version of the copyrighted video (even though the full-length video is present on and can be downloaded from a Mega Conspiracy-controlled server). Similarly, browsing the front page of Megavideo.com does not show any obviously infringing copies of any copyrighted works; instead, the front page contains videos of news stories, user-generated videos, and general Internet videos in a manner substantially similar to Youtube.com. The "most-viewed" videos section of the Entertainment category on Megavideo.com, however, has at times listed a number of infringing copies of copyrighted works that are available from Mega Conspiracy-controlled servers.

16. The Mega Conspiracy uses e-mail addresses with the extension @megaupload.com in the operation of the Megaupload.com website. [REDACTED]
[REDACTED] the e-mail address abuse@megaupload.com has received and continues to receive thousands of infringement notices from copyright holders, including but not limited to Warner Bros. Entertainment Inc., Sony Music Entertainment Inc., and the Business Software Alliance. The e-mails provided notice of the existence of unauthorized copies of copyrighted motion pictures, television shows, software, literature, and music on servers controlled by the Mega Conspiracy. The notice e-mails

contained the URL links to the locations on Megaupload.com where the infringing copies of copyrighted works resided. These infringement notices were submitted to the Mega Conspiracy pursuant to the notice and takedown provisions of the Digital Millennium Copyright Act (“DMCA”), codified at 17 U.S.C. § 512. The FBI’s review of other e-mails has shown that the Mega Conspiracy operators also ignored notices of selected infringing content, and actually uploaded infringing content themselves to servers controlled by the Mega Conspiracy.

17. The Mega Conspiracy also received millions of infringement notices through an automated system that allows copyright holders to identify active URL links to infringing copies of copyrighted works. Copyright holders were led to believe that the Mega Conspiracy’s systems would then remove, or disable access to, the infringing content. In practice, however, only the specific URL links identified in the notices were disabled. The infringing content remained on servers controlled by the Mega Conspiracy, and any other active URL links pointing to that server location continued to provide access to the infringing content.

18. The FBI investigation has revealed that DEFENDANTS and others are members of the Mega Conspiracy, which has operated since at least September 2005 and is estimated to have caused harm to copyright holders in excess of \$500,000,000 and generated more than \$175,000,000 in revenue.

THE DEFENDANTS

19. KIM DOTCOM, who has also been known as KIM SCHMITZ and KIM TIM JIM VESTOR, is a resident of both Hong Kong and New Zealand, and a dual citizen of Finland and Germany. DOTCOM is the founder of MEGAUPLOAD LIMITED and Megamedia Limited. Until on or about August 14, 2011, DOTCOM was the Chief Executive Officer of MEGAUPLOAD LIMITED, and he is currently MEGAUPLOAD LIMITED’s Chief Innovation

Officer. As the head of the Mega Conspiracy, DOTCOM employs more than 30 people residing in approximately nine countries. From the onset of the Mega Conspiracy through to the present, DOTCOM has supervised the development of the websites and companies utilized in the Mega Conspiracy. DOTCOM directed the creation of the network infrastructure behind the Mega Conspiracy websites, negotiated contracts with Internet Service Providers and advertisers, administered the domain names used by the Mega Conspiracy, and exercises ultimate control over all decisions in the Mega Conspiracy. DOTCOM has arranged millions of dollars in payments for the computer servers utilized by the MEGAUPLOAD LIMITED and Megamedia Ltd. properties around the world, and has also distributed proceeds of the Mega Conspiracy to his co-conspirators. DOTCOM is the director and sole shareholder of both VESTOR LIMITED and Kingdom International Ventures Limited, which have been used to hold his ownership interests in MEGAUPLOAD LIMITED - and Megamedia Ltd.- related properties; for example, DOTCOM owns approximately 68% of Megaupload.com, Megaclick.com, and Megapix.com, and 100% of the registered companies behind Megavideo.com, Megaporn.com, and Megapay.com, through VESTOR LIMITED. DOTCOM has personally distributed a link to a copy of a copyrighted work on, and has received at least one infringing copy of a copyrighted work from, the Mega Conspiracy websites. Additionally, on numerous instances, DOTCOM received DMCA copyright infringement takedown notices from third-party companies. In calendar year 2010, DOTCOM received more than \$42 million in Mega Conspiracy proceeds.

20. MEGAUPLOAD LIMITED is the registered owner of Megaupload.com, the primary website operated by the Mega Conspiracy, and Megaclick.com, a site that offers advertising associated with Mega Conspiracy properties. MEGAUPLOAD LIMITED is a registered company in Hong Kong with a registry number of 0835149. MEGAUPLOAD

LIMITED has a number of bank accounts in Hong Kong that have been used to facilitate the operations of the Mega Conspiracy. DOTCOM, in addition to holding the title of Chief Executive Officer of MEGAUPLOAD LIMITED until as recently as August 2011, owns, through VESTOR LIMITED, approximately 68% of the shares of MEGAUPLOAD LIMITED; MATHIAS ORTMANN, through Netplus International Limited LLC, owns an additional 25%; JULIUS BENCKO, through Basemax International Limited, owns 2.5%; BRAM VAN DER KOLK utilizes Mindpoint International Limited LLC to hold 2.5% of the shares of MEGAUPLOAD LIMITED; SVEN ECHTERNACH owns approximately 1%; and the remaining 1% is owned by an investor in Hong Kong.

21. VESTOR LIMITED is a registered company in Hong Kong with a registry number of 0994358. VESTOR LIMITED has a DBS Bank account in Hong Kong that has been used to facilitate the operations of the Mega Conspiracy. DOTCOM (under the alias KIM TIM JIM VESTOR) is the sole director and shareholder of VESTOR LIMITED, and thus is effectively the sole director and 68% owner of MEGAUPLOAD LIMITED, Megaupload.com, Megaclick.com, and Megapix.com. DOTCOM is the sole director of, and VESTOR LIMITED is the sole shareholder of, Megamedia Ltd., which is the parent company and sole shareholder of the following companies: Megavideo Limited (which is the registered owner of Megavideo.com), Megarotic Limited (which is the registered owner of Megaporn.com), and Megapay Limited. VESTOR LIMITED is also the sole owner of Megaworld.com.

22. FINN BATATO is both a citizen and resident of Germany. BATATO is the Chief Marketing and Sales Officer for Megaupload.com and other Mega Conspiracy properties. Specifically, BATATO is in charge of selling advertising space, primarily through Megaclick.com. BATATO supervises a team of approximately ten salespeople around the world.

The objective of the sales team is to increase advertising revenue in localized markets by targeting certain advertisements in certain countries. BATATO handles advertising customers on the Megaclick.com website and approves advertising campaigns for Megaupload.com, Megavideo.com, and Megaporn.com. BATATO has personally distributed a URL link to at least one infringing copy of a copyrighted work stored on Mega Conspiracy-controlled servers. Additionally, on numerous instances, BATATO received DMCA copyright infringement takedown notices from third-party companies. In calendar year 2010, BATATO received more than \$400,000 in Mega Conspiracy proceeds.

23. JULIUS BENCKO is both a citizen and resident of Slovakia. BENCKO is the Graphic Director for MEGAUPLOAD LIMITED and Megamedia Ltd. BENCKO, as the director and sole shareholder of Basemax International Limited, is effectively a 2.5% shareholder of MEGAUPLOAD LIMITED. From the onset of the Mega Conspiracy through to the present, BENCKO has been the lead graphic designer of Megaupload.com and other Mega Conspiracy websites. BENCKO designed the Megaupload.com logos, the layouts of advertisement space, and the integration of the Megavideo.com Flash video player. BENCKO has requested and received at least one infringing copy of a copyrighted work as part of the Mega Conspiracy. In calendar year 2010, BENCKO received more than \$1 million in Mega Conspiracy proceeds.

24. SVEN ECHTERNACH is both a citizen and resident of Germany. ECHTERNACH is the Head of Business Development for MEGAUPLOAD LIMITED and Megamedia Ltd. ECHTERNACH is a 1% shareholder in MEGAUPLOAD LIMITED. ECHTERNACH leads the Mega Team company, registered in the Philippines, which is tasked with removing illegal or abusive content from Mega Conspiracy websites, reviewing advertising campaigns for inappropriate content, and responding to customer support e-mails. Additionally,

ECHTERNACH handles the Mega Conspiracy's relationships with electronic payment processors, accounting firms, and law firms. His activities include traveling and approaching companies for new business ventures and services. On numerous instances, ECHTERNACH received DMCA copyright infringement takedown notices from third-party companies. In calendar year 2010, ECHTERNACH received more than \$500,000 in Mega Conspiracy proceeds.

25. MATHIAS ORTMANN is a citizen of Germany and a resident of both Germany and Hong Kong. ORTMANN is the Chief Technical Officer, co-founder, and a director of MEGAUPLOAD LIMITED. ORTMANN, as the director and sole shareholder of Netplus International Limited LLC, effectively owns 25% of the shares of MEGAUPLOAD LIMITED. From the onset of the Mega Conspiracy through to the present, ORTMANN has overseen software programmers that developed the Mega Conspiracy's websites, and has handled technical issues with Internet Service Providers. His particular areas of responsibility include setting up new servers, sending and responding to equipment service requests, and problem solving connectivity issues with the Mega Conspiracy websites. Additionally, on numerous occasions, ORTMANN received DMCA copyright infringement takedown notices from other conspirators and third-party companies. ORTMANN also had authority to distribute funds from one of the Mega Conspiracy's main financial accounts. ORTMANN has received a URL link to a copy of a copyrighted work associated with the Mega Conspiracy. In calendar year 2010, ORTMANN received more than \$9 million in Mega Conspiracy proceeds.

26. ANDRUS NOMM is a citizen of Estonia and a resident of both Turkey and Estonia. NOMM is a software programmer and Head of the Development Software Division for MEGAUPLOAD LIMITED. NOMM is responsible for the technical aspects of Megaclick.com.

NOMM develops new projects, tests code, and provides routine maintenance for the Megaclick.com website. Additionally, NOMM provides web coding assistance to various projects on other Mega Conspiracy websites. Such projects have included testing high definition video on Megavideo.com, installing the thumbnail screen captures for uploaded videos, and transferring still images across the various Mega Conspiracy website platforms. NOMM has accessed at least one infringing copy of a copyrighted work from a computer associated with the Mega Conspiracy. In calendar year 2010, NOMM received more than \$100,000 in Mega Conspiracy proceeds.

27. BRAM VAN DER KOLK, who has also been known as BRAMOS, is a Dutch citizen and resident of both the Netherlands and New Zealand. VAN DER KOLK is the “Programmer-in-Charge” for MEGAUPLOAD LIMITED and Megamedia Ltd. VAN DER KOLK, as the director and sole shareholder of Mindpoint International Limited LLC, effectively owns 2.5% of the shares of MEGAUPLOAD LIMITED. From the onset of the Mega Conspiracy through to the present, VAN DER KOLK has overseen programming on the Mega Conspiracy websites, as well as the underlying network infrastructure. VAN DER KOLK is also responsible for responding to DMCA copyright infringement takedown notices directed to Mega Conspiracy websites. Lastly, VAN DER KOLK oversaw the selection of featured videos that were listed on Megavideo.com, and he was previously in charge of the “Uploader Rewards” program. VAN DER KOLK has personally uploaded multiple infringing copies of copyrighted works to Mega Conspiracy websites and searched servers controlled by the Mega Conspiracy for infringing copies of copyrighted works at the request of other co-conspirators, including several DEFENDANTS. In calendar year 2010, VAN DER KOLK received more than \$2 million in Mega Conspiracy proceeds.

28. On January 5, 2012, a grand jury in the Eastern District of Virginia issued an Indictment charging DEFENDANTS with conspiracy to commit racketeering (18 U.S.C. § 1962(d)), conspiracy to commit copyright infringement (18 U.S.C. § 371), conspiracy to commit money laundering (18 U.S.C. § 1956(h)), and criminal copyright infringement (18 U.S.C. §§ 2, 2319; 17 U.S.C. § 506). The Indictment is presently under seal.

PROBABLE CAUSE TO SEARCH THE SUBJECT PREMISES

29. Using publicly available software that can detect the Internet Protocol ("IP") addresses of data incoming to the undercover computer, [REDACTED] was able to determine that copyright-infringing content hosted on Megaupload.com was being downloaded from computers assigned IP addresses held by three commercial Internet hosting service companies: Carpathia Hosting, headquartered in Dulles, Virginia, with datacenters at the SUBJECT PREMISES, both of which are located in the Eastern District of Virginia; Cogent, headquartered in Washington, D.C., with datacenters in Washington, D.C. and France; and Leaseweb in the Netherlands. Each of these Internet hosting service companies leases high-speed computer server space and Internet connectivity to the public.

30. The FBI investigation has shown that Carpathia provides approximately 25 petabytes of storage to the Mega Conspiracy in Ashburn, Virginia; Los Angeles, California; and Toronto, Canada. Approximately 1,000 computer servers owned by Carpathia in North America are leased and operated by the Mega Conspiracy; approximately 550 of these servers are currently located in Ashburn, Virginia (the "Ashburn Servers"). The FBI's analysis of the Mega Conspiracy network suggests that the Ashburn Servers consist of approximately 100 web servers associated with testing or hosting Mega Conspiracy websites, approximately 70 database/control or support servers, and approximately 380 content servers.

31. Open source Internet Domain Name System (DNS) records indicate that, as of January 10, 2012, the nine primary web servers hosting www.megaupload.com can be reached via the IP addresses 174.140.154.12 through 174.140.154.15 and 174.140.154.20 through 174.140.154.24. These records similarly indicate that the eleven primary web servers hosting www.megavideo.com can be reached via the IP addresses 174.140.154.18, 174.140.154.19, 174.140.154.25, 174.140.154.30 through 174.140.154.32, 174.140.154.43, 174.140.154.45, 174.140.154.47, 174.140.154.49 and 174.140.154.51. These IP addresses all are owned by Carpathia.

32. [REDACTED] e-mail account of ORTMANN has revealed e-mails from Carpathia [REDACTED] dated November 5, 2009 and from Carpathia [REDACTED] dated November 7, 2010, January 14, 2010 and January 19, 2010, that link these IP addresses to the servers identified as mega-ash-3006 through mega-ash-3009, mega-ash-3012 through mega-ash-3019, mega-ashdc4-3024 through mega-ashdc4-3026, mega-ashdc4-3102, mega-ashdc4-3104, mega-ashdc4-3106, mega-ashdc4-3108, mega-ashdc4-3110 and mega-ashdc4-3112. E-mails from ORTMANN's account also indicate that these servers are located at the SUBJECT PREMISES. An Internet traceroute conducted on January 10, 2011, confirmed that these IPs were still located in the northern Virginia area at that time.

33. The investigation has identified approximately 90 additional supporting web servers located at the SUBJECT PREMISES. These servers support web addresses, such as wwwstatic.megavideo.com, which hosts static content for the Mega Conspiracy websites and can be reached via IP addresses including but not limited to 174.140.154.28, 174.140.154.29, 174.140.154.58 and 174.140.154.60.

34. The investigation has revealed that approximately 380 servers owned by Carpathia and leased by MEGAUPLOAD LIMITED at the SUBJECT PREMISES are dedicated to hosting files uploaded and downloaded by Megaupload.com users, including infringing copies of copyrighted content. These servers are accessible from the Internet via the domains www44.megaupload.com through www49.megaupload.com, www146.megaupload.com through www164.megaupload.com, www400.megaupload.com through www599.megaupload.com, www700.megaupload.com through www798.megaupload.com, www900.megaupload.com through www952.megaupload.com, www997.megaupload.com through www999.megaupload.com, and the corresponding 380 megavideo.com domains.

35. As part of the investigation, [REDACTED] downloaded copyrighted motion pictures, television programs, and software from many of these servers. For example, [REDACTED] downloaded an infringing copy of the copyrighted motion picture *The Green Hornet* from www905.megavideo.com, which is the server identified as mega-ashdc5-1071 located at the SUBJECT PREMISES.

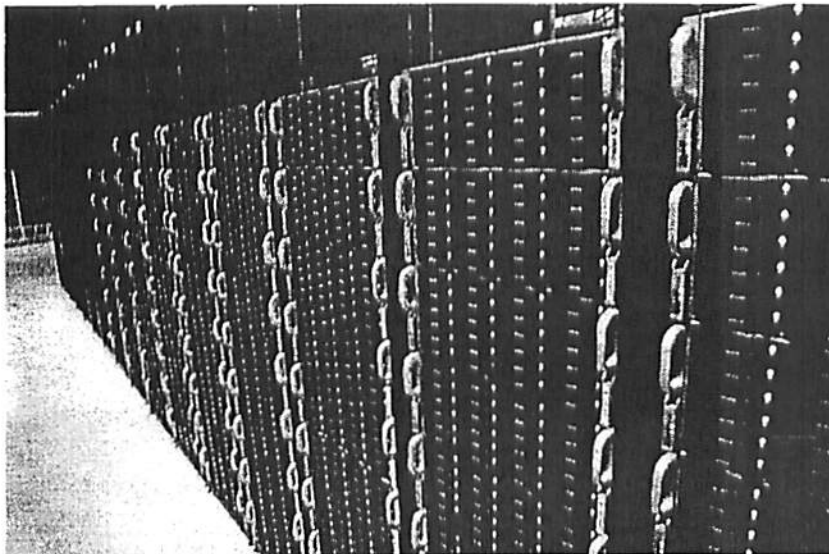
36. On or about October 25, 2008, VAN DER KOLK uploaded an infringing copy of the copyrighted motion picture *Taken* to Megaupload. On October 27, 2011, [REDACTED] downloaded this file from www404.megavideo.com, which is the server identified as mega076, located at the SUBJECT PREMISES.

37. The FBI investigation has further indicated that the central database used to operate Megaupload.com and Megavideo.com is located in the SUBJECT PREMISES. On September 8, 2008, ORTMANN wrote in an email to Carpathia's [REDACTED]: "The servers will be needed to complement our existing two database servers with the same specs and should be located in the 209.222.148.128 subnet." This subnet is at the SUBJECT PREMISES.

In an e-mail dated September 25, 2009, ORTMANN described to an employee of Cogent Communications, which is a company that provides bandwidth for customers including the Mega Conspiracy, the “central traffic control logic located at Ashburn.” On August 23, 2010, ORTMANN sent an e-mail to Carpathia [REDACTED] [REDACTED] entitled “Quote needed – eight DB servers” and stating “for deployment in the 174.140.154 subnet in Ashburn.”

38. [REDACTED] e-mail account known to belong to ORTMANN contained correspondence with Carpathia employees dealing with technical support, which revealed that servers leased by the Mega Conspiracy are present in at least buildings DC2, DC4, and DC5 at the SUBJECT PREMISES.

39. On November 24, 2008, ECHTERNACH sent an e-mail to ORTMANN with the subject line “re: Carpathia.” Although the text of the e-mail was in German, the e-mail mentioned “Equinix DC4” and included a link to several photographs, including the photograph copied below, which is believed to depict some of the Mega Conspiracy servers housed in building DC4 of the SUBJECT PREMISES.



SEARCH AND SEIZURE PROCEDURE

40. Upon execution of the search and seizure warrant, and identification of the servers listed in Attachment B, the servers shall be disconnected from the Internet. This step will maximize the preservation of any evidence for the criminal case and prevent any remote alteration or deletion of computer data.

41. **Website Servers.** The executing agents intend to locate the servers that host the Mega Conspiracy websites, and conduct live forensic analysis on at least the servers identified as mega-ash-3006 and mega-ash-3012. The executing agents intend to perform full live images of several servers, including at least the servers identified as mega-ash-3005, mega-ash-3007, and mega-ash-3013.

42. **Database/Control Servers.** The executing agents intend to locate the servers that store the Mega Conspiracy databases, and extract all databases used to operate the Mega Conspiracy websites. The executing agents intend to access the Mega Conspiracy databases in order to identify the specific servers used to store (1) content associated with Megaupload.com accounts belonging to the DEFENDANTS, and (2) the most popular downloads on Megaupload.com and Megavideo.com. The executing agents intend to perform full images of all non-redundant database servers, which are estimated to be around fifty of the seventy database servers. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files.

43. **Content Servers.** Using the information obtained from the database servers, the executing agents intend to image content servers identified as containing (1) content associated with Megaupload.com accounts belonging to the DEFENDANTS, and (2) the most popular downloads on Megaupload.com and Megavideo.com. The executing agents may also perform

full images of additional servers, including at least those identified as mega-ashdc5-1071 and mega076.

44. In sum, the executing agents currently intend to image roughly fifty-five to seventy-five servers at the SUBJECT PREMISES. It is anticipated that, to complete this imaging, the executing agents will be required to maintain a presence at the SUBJECT PREMISES for an extended period of time. It is intended that, following the imaging process, the executing agents will leave all Ashburn Servers at the SUBJECT PREMISES.

45. Necessity of seizing Ashburn Servers. Though it is not the intention of the executing agents to seize any of the Ashburn Servers, there are a number of scenarios that may require the executing agents to physically remove servers from the SUBJECT PREMISES for imaging and analysis elsewhere, including:

- a. *Inability to gain access to the servers.* To “view” a server, a username and password is generally required, and servers are often encrypted. If passwords are not provided voluntarily, executing agents may nonetheless be able to gain access to the Ashburn Servers through processes such as rebooting a server. If those processes are not successful, however, it may not be possible for executing agents to image servers at the SUBJECT PREMISES.
- b. *Extended imaging process.* Depending on the amount of data stored on the servers, and the complexity of the Mega Conspiracy server system, the time required to image servers may substantially exceed projections. In that case, it may become unreasonable and invasive to remain at the SUBJECT PREMISES until the imaging process is complete. In that case,

it may be necessary for executing agents to seize servers in order to perform imaging elsewhere.

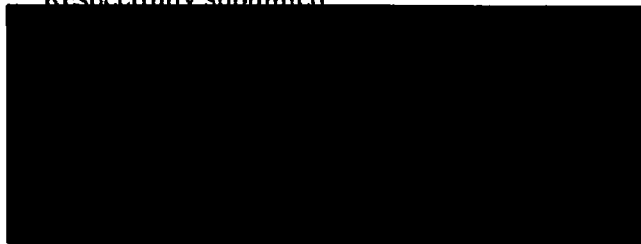
For these reasons, the warrant I am applying for would permit seizure of all servers leased by the Mega Conspiracy that reasonably appear to contain some or all of the evidence described in the warrant, as stated in Attachment B.

CONCLUSION


46. Based upon the above information, there is probable cause to believe that at the SUBJECT PREMISES, there is evidence or instrumentalities of violations of Title 18, United States Code, Sections 2, 371, 1956(h), 1962(d), 2319; or Title 17, United States Code, Section 506.

47. Based upon the foregoing, I respectfully request that the Court issue a search warrant for the SUBJECT PREMISES, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B.

Respectfully submitted



Subscribed and sworn to before me this 18th day of January, 2012.



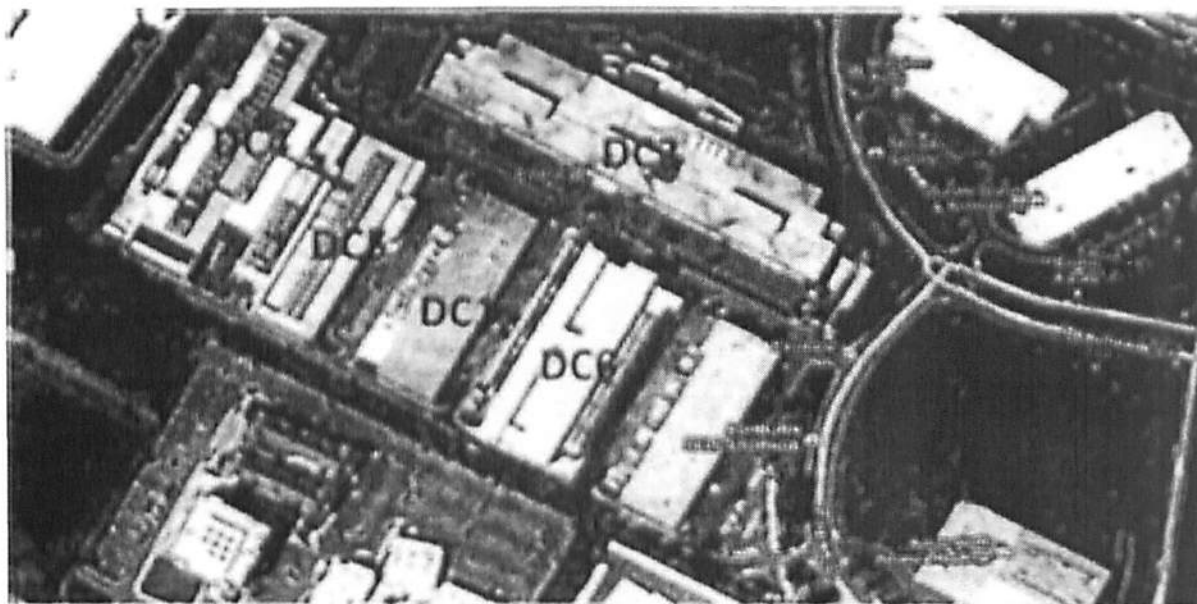
Honorable Liam O'Grady
United States District Judge

Submitted by Lindsay A. Kelly and Jay V. Prabhu
Assistant United States Attorneys

Attachment A

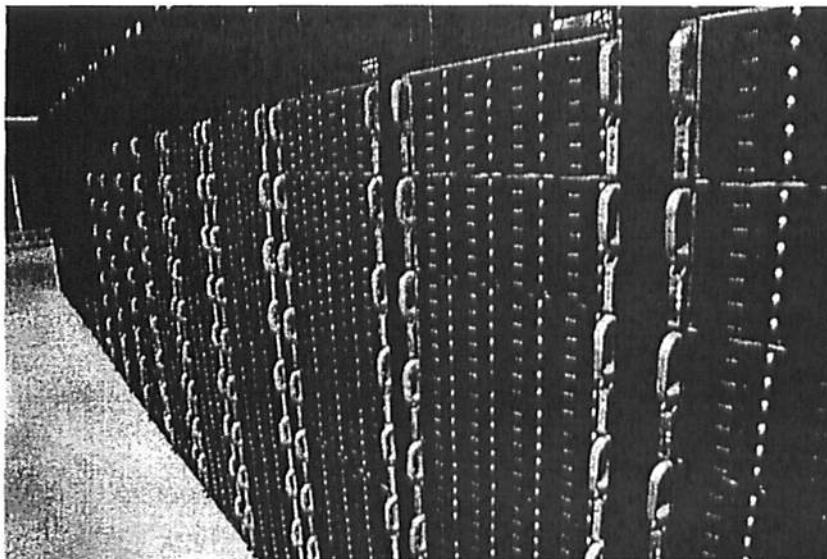
PREMISES TO BE SEARCHED

The SUBJECT PREMISES consists of several buildings that are part of a data center campus owned by Equinix. Carpathia leases warehouse space on this campus from Equinix and, in turn, leases servers housed on this campus to the Mega Conspiracy. The Equinix data center campus consists of a complex of six warehouse-type one-story office buildings, identified by Equinix as buildings DC1 through DC6. The SUBJECT PREMISES includes buildings housing servers leased by Carpathia to the Mega Conspiracy, and includes at least those buildings identified as DC2, DC4, and DC5. The photograph below shows the relative layout of buildings DC2, DC4, and DC5 on the Equinix campus.



Building DC2 is a warehouse building approximately 147,600 square feet in size, constructed of tan concrete on a concrete slab foundation. The address for building DC2 is 21715 Filigree Court, Ashburn, VA 20147. The numbers "21715" are displayed at the top corner of the building exterior. The building interior consists of a series of metal-enclosed cages storing computer servers. The cages have key locks or biometric locks, and are generally numbered.

Building DC4 is a warehouse building approximately 100,000 square feet in size, constructed of tan concrete on a concrete slab foundation. The address for building DC5 is 21691 Filigree Court, Ashburn, VA 20147. The numbers "21691" are displayed at the top corner of the building exterior. The photograph copied below is believed to depict some of the Mega Conspiracy servers housed at the DC4 building.



Building DC5 is a warehouse building approximately 148,000 square feet in size, constructed of tan concrete on a concrete slab foundation. The address for building DC5 is 21701 Filigree Court, Building D, Ashburn, VA 20147. The numbers "21701" are displayed at the top corner of the building exterior. The entrance to DC5 is a single door of tinted glass, directly behind to three narrow cylindrical concrete barriers separating the entrance door from a parking space. Adjacent to the entrance door there are tinted windows to the right. There are also more tinted windows to the left, separated by a narrow portion of the stone building wall. The letter "D" is displayed above, and slightly to the left of, the entry door.

The premises to be searched includes all cages containing servers leased by Carpathia to the Mega Conspiracy, including but not limited to those in buildings DC2, DC4, and DC5.

Attachment B

ITEMS TO BE SEIZED

Evidence or instrumentalities of violations of Title 18, United States Code, Sections 2 (Aiding and Abetting), 371 (Conspiracy), 1956(h) (Money Laundering), 1962(d) (Racketeering), 2319 (Copyright Infringement); or Title 17, United States Code, Section 506 (Copyright Infringement), including the following:

A. All servers leased or used by MEGAUPLOAD LIMITED, Megaupload.com, Megavideo.com, or associated websites or entities, including but not limited to:

a. Servers identified as:

mega076
mega-ash-3006
mega-ash-3007
mega-ash-3008
mega-ash-3009
mega-ash-3012
mega-ash-3013
mega-ash-3014
mega-ash-3015
mega-ash-3016
mega-ash-3017
mega-ash-3018
mega-ash-3019
mega-ashdc4-3024
mega-ashdc4-3025
mega-ashdc4-3026
mega-ashdc4-3102
mega-ashdc4-3104
mega-ashdc4-3106
mega-ashdc4-3108
mega-ashdc4-3110
mega-ashdc4-3112
mega-ashdc5-1071

b. Servers with the following assigned IP addresses:

174.140.154.12
174.140.154.13
174.140.154.14
174.140.154.15
174.140.154.18
174.140.154.19
174.140.154.20

174.140.154.21
174.140.154.22
174.140.154.23
174.140.154.24
174.140.154.25
174.140.154.28
174.140.154.29
174.140.154.30
174.140.154.31
174.140.154.32
174.140.154.43
174.140.154.45
174.140.154.47
174.140.154.49
174.140.154.51
174.140.154.58
174.140.154.60

c. Servers accessible at the following URLs:

www44.megaupload.com through www49.megaupload.com,
www146.megaupload.com through www164.megaupload.com,
www400.megaupload.com through www599.megaupload.com,
www700.megaupload.com through www798.megaupload.com,
www900.megaupload.com through www952.megaupload.com,
www997.megaupload.com through www999.megaupload.com,
www44.megavideo.com through www49.megavideo.com,
www146.megavideo.com through www164.megavideo.com,
www400.megavideo.com through www599.megavideo.com,
www700.megavideo.com through www798.megavideo.com,
www900.megavideo.com through www952.megavideo.com, and
www997.megavideo.com through www999.megavideo.com.

- B. Records located on the hard drives, RAM, or other storage media incorporated into or attached to the computers described in paragraph A of this Attachment;
- C. Records relating to the unauthorized distribution of copyrighted motion pictures, television programs, musical recordings, electronic books, images, video games, or other computer software, in violation of 18 U.S.C. §§ 2, 2319 & 18 U.S.C. § 506;
- D. Passwords, encryption keys, and other access devices that may be necessary to access the above-listed servers;
- E. Documentation and manuals that may be necessary to access or to conduct a forensic examination of the above-listed servers;

- F. Contextual information necessary to understand the evidence described in this attachment.**

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN THE MATTER OF THE SEARCH OF)
) Case No. 1:12-sw- 41
THE PREMISES LOCATED AT)
21691 Filigree Court, 21701 Filigree Court,) UNDER SEAL
and 21715 Filigree Court, Bldg. D, Ashburn,)
Virginia 20147)

**GOVERNMENT'S MOTION TO SEAL SEARCH WARRANT
PURSUANT TO LOCAL RULE 49(B)**

The United States, through undersigned counsel, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, now asks for an Order to Seal the search warrant, the application for search warrant, and the affidavit in support of the search warrant, together with this Motion to Seal and proposed Order, until the United States makes a motion to unseal these documents.


I. REASONS FOR SEALING (See Local Rule 49(B)(1))

1. The Indictment, and arrest warrants, charging nine defendants with various crimes stemming from their involvement in a worldwide criminal enterprise related to Megaupload.com

is under seal. [REDACTED]

2. While it is anticipated that the Indictment will be unsealed shortly after this seizure warrant is served, premature disclosure of the specific details of this criminal case [REDACTED]

[REDACTED]



3. The United States has considered alternatives less drastic than sealing, including, for example, the possibility of redactions, and has determined that none would suffice to protect this investigation.

II. THE GOVERNING LAW (See Local Rule 49(B)(2))

4. It is generally recognized that the public has a common law right of access, but not a First Amendment right of access, to judicial documents, including documents associated with *ex parte* proceedings such as search warrant affidavits. Media General Operations, Inc. v. Buchanan, 417 F.3d 424, 429 (4th Cir. 2005); In re Washington Post Company v. Hughes, 923 F.2d 324, 326 (4th Cir. 1991). “But the right of access is qualified, and a judicial officer may deny access to search warrant documents if sealing is ‘essential to preserve higher values’ and ‘narrowly tailored to serve that interest.’” Media General Operations, 417 F.3d at 429 (citations omitted); see also In re Knight Pub. Co., 743 F.2d 231, 235 (4th Cir. 1984) (“[t]he trial court has supervisory power over its own records and may, in its discretion, seal documents if the public’s right of access is outweighed by competing interests”). Sealing search and seizure warrants and their accompanying affidavits and application is within the discretionary powers of a judicial officer where, among other things, an “‘affidavit contain[s] sensitive details of an ongoing investigation’ and it is ‘clear and apparent from the affidavits that any disclosure of the information there would hamper’ th[e] ongoing investigation.” Media General Operations 417 F.3d at 430 (citations omitted); see also In re Search Warrant for Matter of Eye Care Physicians of America, 100 F.3d 514, 518 (7th Cir. 1996).

5. Before a district court generally may seal judicial records or documents, it must (a) provide public notice of the request to seal and allow interested parties a reasonable opportunity to object, (b) consider less drastic alternatives to sealing the documents, and (c) provide specific reasons and factual findings supporting its decision to seal the documents and for rejecting the alternatives. Ashcraft v. Conoco, Inc., 218 F.3d 288, 302 (4th Cir. 2000).

6. However, in the specific context of a search and seizure warrant, the Fourth Circuit has cautioned that “the opportunity to object” cannot “arise prior to the entry of a sealing order when a search warrant has not been executed.” Media General Operations, 417 F.3d at 429. “A rule to the contrary would endanger the lives of officers and agents and allow the subjects of the investigation to destroy or remove evidence before the execution of the search warrant.” Id.; see also Franks v. Delaware, 438 U.S. 154, 169 (1978). Accordingly, “the notice requirement is fulfilled by docketing ‘the order sealing the documents,’ which gives interested parties the opportunity to object after the execution of the search warrants.” Media General Operations, 417 F.3d at 430 (quoting Baltimore Sun Co. v. Goetz, 886 F.2d 60, 65 (4th Cir. 1989)); see also Local Rule 49(B) (“Until an executed search warrant is returned, search warrants and related papers are not filed with the Clerk.”).

7. As to the requirement of a court’s consideration of alternatives, the Fourth Circuit counsels that, “[i]f a judicial officer determines that full public access is not appropriate, she ‘must consider alternatives to sealing the documents,’ which may include giving the public access to some of the documents or releasing a redacted version of the documents that are the subject to the government’s motion to seal.” Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 66).

8. Finally, regarding the requirement of specific findings, the Fourth Circuit's precedents state that, "in entering a sealing order, a 'judicial officer may explicitly adopt the facts that the government presents to justify sealing when the evidence appears credible,'" Media General Operations, 417 F.3d at 429 (quoting Goetz, 886 F.2d at 65), so long as the ultimate "decision to seal the papers" is "made by the judicial officer," Goetz, 886 F.2d at 65. "Moreover, if appropriate, the government's submission and the [judicial] officer's reason for sealing the documents can be filed under seal." Goetz, 886 F.2d at 65; see also In re Washington Post Co., 807 F.2d 383, 391 (4th Cir. 1986) ("if the court concludes that a denial of public access is warranted, the court may file its statement of the reasons for its decision under seal").

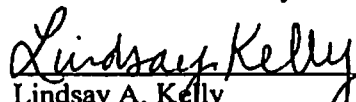
III. PERIOD OF TIME GOVERNMENT SEEKS TO HAVE MATTER REMAIN UNDER SEAL (See Local Rule 49(B)(3))

9. Pursuant to Local Rule 49(B)(3), the search warrant, the application for a search warrant, and the affidavit will remain sealed until the need to maintain the confidentiality of these documents expires and the United States moves to unseal these documents.

WHEREFORE, the United States respectfully requests that the search warrant, application for search warrant, affidavit in support of the search warrant, and this Motion to Seal and proposed Order be sealed until further Order of the Court. Notwithstanding this request, the United States asks to provide copies as necessary to execute the search warrant.

Respectfully submitted,

Neil H. MacBride
United States Attorney

By: 
Lindsay A. Kelly
Assistant United States Attorney