IN THE DISTRICT COURT
AT NORTH SHORE

CRI-2012-092-1647

UNDER	Extradition Act 1999
IN THE MATTER	Proceedings to extradite Kim Dotcom, Bram van der Kolk, Finn Habib Batato and Mathias Ortmann
BETWEEN	**THE UNITED STATES OF AMERICA**
	Applicant
AND	**KIM DOTCOM, BRAM VAN DER KOLK, FINN HABIB BATATO AND MATHIAS ORTMANN**
	Respondents

AFFIDAVIT OF LAWRENCE LESSIG
DATED SEPTEMBER 2015

Assigned Judge: *Judge Dawson*
Case Manager: *Jennifer Spence*

SOLICITOR ACTING:
S L Cogan
Anderson Creagh Lai Limited
Level 1, 110 Customs Street West
PO Box 106-3197
Auckland 1143
Tel: (09) 300 3196
Fax: (09) 300 3197
Email: simon@acllaw.co.nz

COUNSEL:
R M Mansfield
22 Lorne Chambers
PO Box 2674
Shortland Street
Auckland 1140
Tel: (09) 304 1627
Email: ron@22lorne.co.nz

I, **LAWRENCE LESSIG** of Cambridge, Massachusetts, United States of America, swear as follows:

1. I am a professor of law at Harvard Law School, Harvard University and a practicing lawyer. One of my chief areas of specialty has been intellectual property law in the context of the Internet.

2. I have been retained by the respondents' (alternatively referred to as "defendants") United States attorneys, Quinn Emanuel Urquhart & Sullivan LLP and Rothken Law Firm as liaison counsel to Anderson Creagh Lai Limited, to evaluate the Superseding Indictment and Record of the Case, to presume the truth of factual allegations therein, and to give my opinion as to whether a prima facie case has been made out that that would be recognized by United States federal law and subject to the *Treaty on Extradition Between the United States of America and New Zealand*, Art. VI, § 3, 1970 U.S.T. LEXIS 470; 22 U.S.T. 1s (**US – NZ Extradition Treaty)**.

3. I have also been asked to give my opinion as to whether the Superseding Indictment and Record of the Case are reliable, viewed in light of obligations of the United States to act as a model litigant in its extradition request for alleged criminal misconduct.

SUMMARY OF OPINIONS

4. It is my opinion that the Superseding Indictment and Record of the Case filed by the United States Department of Justice (**DOJ**) do not meet the requirements necessary to support a prima facie case that would be recognized by United States federal law and subject to the US – NZ Extradition Treaty. On the whole, the filings are not reliable.

5. Charges in the Superseding Indictment fall into three classes:

   (a) Counts Four through Eight allege that respondents themselves committed crimes of copyright infringement. General allegations in such Counts do not find support in specific facts set forth in the Record of the Case. A showing of willful criminal copyright infringement requires compact factual proof identifying a specific copyrighted work, a right of the owner that has been

violated, the geographical location of the infringement and other specific facts needed to establish a violation of United States criminal law. Such compact facts are absent here. The generalized accusations, defective and irrelevant allegations, scattered facts of alleged multiple infringements and statistics set forth in the Superseding Indictment and Record of the Case do not satisfy requirements of proof but rather manifest unreliability of the overall approach. Charges in Counts Four, Seven and Eight are outside the three-year statute of limitations provided by the US-NZ Extradition Treaty that I understand is applicable in this proceeding as well as lacking proof of other necessary elements.

(b) Counts One through Three allege conspiracy. Count Two (Conspiracy to Commit Copyright Infringement) is the chief matter discussed herein. In brief, it is alleged that respondents agreed with users of the Megaupload system that users would commit copyright infringement by means of Megaupload. Again, general allegations do not find support in actual facts. There is no showing of specific criminal "willful" infringements committed by specific individual users. There is an even more serious lack of evidence of communications between respondents and such alleged users needed to prove an agreement that is subject to laws of conspiracy. The United States Constitution (**U.S. Const.**) prohibits the United States DOJ from prosecuting, as they apparently want to here, a new kind of criminal conspiracy based on defendants providing an "environment of infringement" or their failing to disable all links to an allegedly infringing copy. Under the approach of the DOJ, many online operations and even individual persons would, without notice, suddenly become subject to criminal prosecution. Count One (Conspiracy to Commit Racketeering) and Count Three (Conspiracy to Commit Money Laundering) require showings of independent predicate offenses, which are lacking here.

(c) Counts Nine through Thirteen allege Fraud by Wire and Aiding & Abetting Fraud by Wire. Charges involve an online "Abuse

Tool" provided to copyright owners by Megaupload so that owners could report to Megaupload the appearance of unauthorized links to their works and automatically disable access to such links. It is alleged that owners were misled by Megaupload's messages provided with the tool and that links, outside those included in such copyright takedown requests, were not removed although copyright owners believed that they should have been. The facts set forth in the Record of the Case fail to show a Wire Fraud offense or any offense. A novel interpretation of the Digital Millennium Copyright Act (**DMCA**) needed to support such charges would be contrary to the nature of Internet operations and to the DMCA itself. Essential elements of causation and damages are not supported by proof.

QUALIFICATIONS AND EXPERIENCE

6. In 1983, I received a B.S. in management from the Wharton School, and a B.A. in economics from the University of Pennsylvania. I received an M.A. in philosophy from Cambridge University, graduating in 1986. I received a J.D. from Yale Law School in 1989. After completing law school, I clerked for Judge Richard Posner of the Seventh Circuit Court of Appeals, and for Justice Antonin Scalia of the United States Supreme Court. I was a professor of law at the University of Chicago Law School from 1991 to 1997, and from 1997 to 2000 I was the Jack N. and Lillian R. Berkman Professor for Entrepreneurial Legal Studies at the Harvard Law School, where I was affiliated with the Berkman Center for Internet and Society. From 2000 to 2009, I was a professor at Stanford Law School, where I established the Center for Internet and Society. In 2009, I returned to Harvard Law School.

7. I have been a close observer of the Internet and its culture since the 1990s. I taught one of the first "Law of Cyberspace" classes at an academic law school in 1995 (Yale). Since then, I have taught numerous Internet and copyright related classes. I have attended over three hundred conferences about law and technology, and I have

consulted extensively with policy makers about the regulation of cyberspace.

8. In 2001, I co-founded Creative Commons, an alternative copyright licensing regime and online platform that allows authors to license works freely for certain uses, or dedicate them to the public domain.

9. I have written extensively in the field of Internet regulation. I have published six books and over fifty articles exploring the relationship between regulation and cyberspace, and have given scores of lectures on the same topic. The focus of most of this work has been the interplay between technology and law, and on the use of law to effect changes in technology and, in particular, internet architectures. In addition to my scholarly work, I have been a regular columnist for The Industry Standard and Wired. I have also contributed essays to the New York Times, the Wall Street Journal, the Washington Post, the Los Angeles Times, and the Boston Globe.

10. I have been active in a number of Internet-related law suits and policy determinations. I have testified before Congress on a number of issues, including net neutrality, telecommunications regulation, and the Child Online Protection Act. I have met with the DOJ and the Federal Communications Committee on matters related to the merger of AT&T and MediaOne. In 1997, I was asked by Judge Thomas Penfield Jackson to serve as Special Master in the DOJ's consent decree case against Microsoft Corporation. I also represented a group of plaintiffs challenging Congress' Sonny Bono Copyright Term Extension Act before the United States Supreme Court. *Eldred v. Ashcroft*, 537 U.S. 186 (2003).

SCOPE OF INSTRUCTIONS AND EVIDENCE

11. I understand that the United States seeks an order from New Zealand to extradite Kim Dotcom.

12. I have read, and agree to comply with, the Code of Conduct for Expert Witnesses at Schedule 4 of the High Court Rules, New Zealand.

13. I have read the Superseding Indictment and the original Record of the Case, along with the First through Eighth Supplemental Affidavits (collectively called the **Record of the Case** or **ROC**). In my analysis below I refer to Megaupload as shorthand for the cloud storage sites at issue in the superceding indictment and ROC, including for example, Megavideo. If I failed to address anything in my analysis from the superceding indictment or the Record of the Case it is because I found it inconsequential to my ultimate opinions reached herein. I have also read the Ortmann FBI Interview of 20 January 2012 to familiarize myself with particular facts concerning technical operations at Megaupload including, for example, automated cloud storage functions, dual use server infrastructure, caching servers, deduplication, and notice and takedown methods. I have reviewed legacy screenshots of the Megaupload website found at www.archive.org, including, but not limited to, reading the Megaupload Terms of Use as they existed on or about 14 May 2011 (Megaupload TOU).

14. For the purposes of this analysis, I presume the truth of specific factual allegations in the ROC. I also rely on public court documents and statements of Mathias Ortmann and others regarding cloud storage technology. I presume the truth of statements of Mathias Ortmann on matters of technical functionality, as I find them largely uncontradicted by facts in the Superceding Indictment and Record of the Case, for example, that Megaupload's cloud storage technology was copyright neutral and unable to discern whether user content was infringing, authorized, or fair use.

15. For purposes of this analysis, I do not rely on statements in the Superseding Indictment and Record of the Case that lack a consequential connection to specific charges. Thus, I often disregard general accusations, legal conclusions and allegations that do not support the prima facie case that is the focus of this proceeding and are thus irrelevant.

16. I confirm that opinions stated herein and related issues are within my area of expertise.

17. I am not an expert in New Zealand law. For the purposes of this analysis, I have been instructed that the US-NZ Extradition Treaty requires application of New Zealand's shorter statute of limitations for criminal copyright infringement. *US – NZ Extradition Treaty*, Art. VI, § 3, 1970 U.S.T. LEXIS 470; 22 U.S.T. 1.When the US indictment was filed on January 5, 2012, the statute of limitations for criminal copyright infringement in New Zealand was three years from the date the offence was committed. See New Zealand *Copyright Act 1994* § 131A (repealed July 1, 2013).

FACTUAL CONTEXT AND ALLEGATIONS

18. The following facts appear to be established for purposes of this opinion:

    (a) That Kim Dotcom was a founder and shareholder of Megaupload, and that the charges listed against him relate solely to the functioning of Megaupload, its affiliates, and its employees. (Sup. Indictment ¶ 30.)

    (b) That Megaupload and related sites were members of a class of "cloud storage websites" that provide storage of and access to digital files under the direction of individual "users," "customers" or "visitors." Cloud storage users can access their files from anywhere in the world and can enable other persons to access such files. (Ortmann FBI Interview of 20 January 2012 at 9-12).

    (c) That Megaupload's software code and interface design provided automated processes for users to upload files for storage on Megaupload; that users received unique links or "URLs" to such files; that users decided what persons, if any, could access their files; and that Megaupload had no control over such decisions. (Ortmann FBI Interview of 20 January 2012 at 9).

    (d) That Megaupload and related sites, e.g., MegaVideo, were Online Service Providers ("OSP"), also known as Internet Service Providers ("ISP"), that operated from 2005 to January 2012, when they were shut down.

(e) That Megaupload used standard software methods for data management called "deduplication" that reduce storage requirements for duplicate files. That when a file was uploaded to storage, such methods generated an identifier, called an "MD5 hash," from the contents of the file. (Sup. Indictment ¶ 23). This deduplication approach appears the same as the technology used by Dropbox, a cloud storage industry leader. https://blogs.dropbox.com/dropbox/2011/07/changes-to-our-policies/ ("**De-duplication** – We're always working to make Dropbox more efficient. For example, we may de-duplicate files, which means we store only one copy of files or pieces of files that are the same…")

(f) That when identical files uploaded by different users generated the same MD5 hash, Megaupload would retain only one copy of the file, but would generate a unique link or "URL" for each individual user. (Sup. Indictment ¶ 23).

(g) That Megaupload developed automated "caching" software and hardware combinations that facilitated speedy transfer of the most popular files through geographically efficient storage locations. (Ortmann FBI Interview of 20 January 2012 at 31-33, 56-58). This method is referred to as a Content Delivery Network (CDN). (see, Pathan and Buyya, *A Taxonomy and Survey of Content Delivery Networks* at *www.cloudbus.org/reports/CDN-Taxonomy.pdf*; Wikipedia, "Content delivery network" at https://en.m.wikipedia.org/wiki/Content_delivery_network).

(h) That users of Megaupload's family of online services users agreed to Terms of Use that prohibited copyright infringement. (Megaupload TOU, paragraph 8(c) and 8.4).

(i) That Megaupload had a policy to terminate repeat infringers (Megaupload TOU, para. 8(c), 8.4 and 13.1) and did terminate repeat infringers. (Ortmann FBI Interview of 20 January 2012 at 67).

(j) That Megaupload was a popular cloud storage ISP with many users:

(i) That as of January 2012, Megaupload accounted for four percent of all Internet traffic, had more than one billion visitors in its history, and had an average of 50 million daily visits. (Summary ¶ 22(g).)

(ii) That according to the United States DOJ, Megaupload leased over 25 petabytes of data from Carpathia Hosting Inc. (**Carpathia**) in the United States. (Summary ¶ 22(q).)

(iii) That according to the United States DOJ, Megaupload leased 19 petabytes of data from Leaseweb in the Netherlands. (Summary ¶ 22(s).)

(k) That the United States DOJ further reports that Megaupload users had uploaded "up to approximately 206 million total unique files" as of January 19, 2012. (Summary ¶ 32(h).)

(l) That Megaupload maintained a "rewards program" that applied formulaically to user-controlled files that led to user-controlled file downloads. If the volume of downloads met pre-determined amounts certain payments would be triggered. The program prohibited file sizes over 100MB to deter videos that tend to have larger file sizes. Terms of Use that prohibited infringing materials governed the program. (Megaupload TOU, para. 8(c) and 8.4).

(m) That Megaupload onlines services were capable of and had substantial non-infringing uses including for example:

(i) File backups. Of the 14.9 million unique video files stored on servers located within the United States, roughly 42% had never been viewed. ROC ¶ 32(c).

(ii) Content Owners. One user, Kyle Goodwin, sought relief for the release of his non-infringing files through litigation in the United States. I refer in particular to the

Emergency Motion for Protective Order by Non-Party Carpathia Hosting, Inc. and for Additional Relief, Declaration of Interested Party Kyle Goodwin in Support thereof 12-cr-00003-LO, ¶ 5 (Dkt. 51).

(iii) Fair Use and Authorized Uses. Additional non-infringing uses were reported: Jon Brodkin, "Megaupload Wasn't Just for Pirates: Angry Users Out of Luck for Now," ArsTechnica, Jan. 20, 2012 (available at http://arstechnica.com/gadgets/2012/01/megaupload-wasnt04763.00001/6106406.1) Nick Galvin, "Megaupload Closure Hits Legitimate Users," Sydney Morning Herald, Jan. 23, 2012 (available at http://www.smh.com.au/technology/technology-news/megaupload-closure-itslegitimate-users-20120122-1qc7d.html).

(n) That, from its inception, Megaupload accepted and processed notices from copyright owners of links to infringing materials pursuant to "notice and takedown" provisions of the DMCA. That Megaupload responded to such notices by disabling access to such links. (Ortmann FBI Interview of 20 January 2012 at 29-30.)

(o) That, commencing on October 15, 2009, Megaupload registered an agent to receive DMCA notices from copyright owners. (Sup. Indictment 21 n.1)

(p) That Megaupload also negotiated with copyright holders, or their agents— e.g., the Recording Industry Association of America, Disney, Warner Brothers, NBC, and Microsoft—to facilitate quick removal of infringing files. (Sup. Indictment 23).

(q) That Megaupload reportedly received revenues of at least $175 million during its operation. (Sup. Indictment ¶ 114). This revenue was stored in a variety of accounts located in New Zealand and Hong Kong. (Sup. Indictment ¶ 115.).

LEGAL CONSIDERATIONS BEARING ON EXTRADITION

19. The DOJ has asserted the following claims in the United States against Kim Dotcom: Conspiracy to Commit Racketeering, Conspiracy to Commit Copyright Infringement, Conspiracy to Commit Money Laundering, Criminal Copyright Infringement, Aiding and Abetting Criminal Copyright Infringement, Wire Fraud, and Aiding and Abetting Wire Fraud. (Sup. Indictment at 1.). It is my understanding that the basis of charges against Kim Dotcom are based on his role in founding and operating Megaupload.

20. It is my understanding that the charges of conspiracy to commit copyright infringement and wire fraud are of chief importance. I am instructed that the US-NZ Extradition Treaty limits the scope of the DOJ's extradition request. Extradition is not available for direct or primary criminal copyright offenses. Rather, the DOJ must prove a prima facie case of a conspiracy of or between three or more of an underlying offense. Here, it appears that the DOJ has identified felony copyright infringement as the chief underlying crime. However, to better inform the court, the discussion below also touches upon the possibility of either wire fraud or money laundering serving as the underlying crime.

PRINCIPLES OF UNITED STATES CRIMINAL LAW

21. The United States has filed a criminal indictment against Kim Dotcom and others in a United States federal court. In federal courts, the governing law comes from the Constitution of the United States—which is the supreme law of the United States—as well as from subordinate federal statutes, and decisions of other United States federal courts which interpret and apply those statutes and the constitution. All United States federal courts are bound by decisions of the Supreme Court of the United States.

22. In addition to decisions of the Supreme Court, federal trial courts are also bound by the decisions of their local United States Court of Appeals. The United States Court of Appeals is divided into 12 different Circuit Courts, which govern different geographical regions.

(There is also a 13th Circuit dedicated to patent cases and other distinct areas of law, referred to as the Federal Circuit). While many issues are treated uniformly across the 12 regional circuits of the United States, some issues of common law have developed distinct doctrines in different parts of the country.

23. This case is within the jurisdiction of the Fourth Circuit Court of Appeals. The Eastern District of Virginia, where the DOJ filed the indictment, is bound by the precedential decisions handed down by the United States Court of Appeals for the Fourth Circuit, as well as the precedential decisions of the Supreme Court of the United States. The Eastern District of Virginia will also look to other US Appellate Circuits and Federal District Courts for case law guidance.

24. Additionally, the indictment itself must meet minimum standards under United States criminal law. Indictments are required for felony prosecutions by the Fifth Amendment to the United States Constitution. See U.S. Const. amend. V ("No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury"). As indictments are prerequisites for federal felony prosecutions, defects in the indictment are cause for the DOJ's case to be dismissed and the defendant to be set free, even after a trial has been held. See *United States v. Daniels*, 973 F.2d 272, 276 (4th Cir. 1992) (holding that where an indictment was defective the conviction must be overturned).

25. An "indictment must include every essential element of an offense, or else the indictment is invalid[.]" *United States v. Kingrea*, 573 F.3d 186, 191 (4th Cir. 2009). An indictment must specifically allege facts that demonstrate the elements of the crime; an indictment that simply recites the statutory requirements and conclusions is not sufficient. See, *Id*. ("mere reference to the applicable statute does not cure the defect").

26. For nearly 200 years, the United States Supreme Court has held that federal crimes cannot be expanded by decisions of prosecutors or courts. Federal crimes are “solely creatures of statute.” *Liparota v. United States*, 471 U.S. 419, 424 (1985). Charges against a defendant

must be based on a statute. An indictment must allege facts that satisfy every statutory element. Likewise, a prima facie showing requires proof of all elements. If the crime is not defined by statute or if there is a defect in the indictment or proof, the case will be dismissed. (See *In re Int'l Sys. & Controls Corp. Sec. Litig.*, 693 F.2d 1235 (4th Cir. 1982); *U.S.. v. Under Seal (In re Grand Jury Proceedings #5),* 401 F.3d 247, 251 (4th Cir. 2005).)

ENFORCEMENT OF CRIMINAL LAWS IN THE UNITED STATES IS TIGHTLY CONSTRAINED AND CANNOT BE EXPANDED BY PROSECUTORS

27. In the Superseding Indictment, the DOJ appears to attempt expansive definitions of crimes by borrowing concepts of secondary liability from civil copyright case law. Such attempts are improper because, in the United States, crimes must be clearly defined by the legislature and prosecutions are confined within express criminal statutes.

28. In copyright law in particular, “the deliberation with which Congress . . . has addressed the problem of copyright infringement for profit, as well as the precision with which it has chosen to apply criminal penalties in this area, demonstrates anew the wisdom of leaving it to the legislature to define crime and prescribe penalties.” *Dowling v. United States*, 473 U.S. 207, 228 (1985). The court also stated: “It is the legislature, not the Court, which is to define a crime”) (quoting *United States v. Wilberger*, 5 Wheat. 76 (1820)). “When assessing the reach of a federal criminal statute, the courts are to “pay close heed to language, legislative history, and purpose in order strictly to determine the scope of the conduct the enactment forbids.” *Id*. at 213.

29. As Justice Blackmun observed in *Dowling*, copyright is an area in which Congress has chosen to tread cautiously, relying "chiefly . . . on an array of civil remedies to provide copyright holders protection against infringement," while mandating "studiously graded penalties" in those instances where Congress has concluded that the deterrent effect of criminal sanctions are required. *Dowling, supra* at 221, 225. "This step-by-step, carefully considered approach is consistent with

Congress' traditional sensitivity to the special concerns implicated by the copyright laws." *Id* at 225.

30. In my opinion, expansive allegations in the Superseding Indictment cannot support a criminal conviction. As discussed below, the DMCA is part of the package of civil copyright liability safe harbors provided to online service providers, not a basis for ciminal copyright liability either by direct application or indirectly by means of “Wire Fraud” charges.

31. The DOJ appears to be asserting that an ISP like Megaupload, which receives copyright take down notices identifying one URL, must search for and delete all duplicate files used by different users in the cloud system or be subject to a copyright or fraud claim. In my opinion the DOJ’s novel theory of copyright or fraud liability is erroneous.

32. Megaupload reduced operating loads by “deduplication” namely maintaining only a single copy of a file in its database and generating multiple links to such file. Each link identified an uploader of the common file. It is possible for one uploader to have a right to fair use of a copy of a file, e.g., a purchaser uploading a backup or an educational organization offering critical commentary, while other uploaders might have no such fair use right. It is contrary to the purpose of the DMCA that a fair use right would be violated through a take-down notice directed at another person’s wrongful use. If such a violation were to occur, the provider of the take-notice would be subject to liability under the DMCA (17 U.S.C. § 512(f)).

33. Similarly, criminal copyright liability cannot be broadened by invoking civil concepts of secondary copyright infringement directly or under the guise of the general aiding and abetting statute, 18 U.S.C. § 2. *See* Sup. Ind. Counts Four, Five, Six, Seven, and Eight. The United States legislature previously removed “aiding and abetting” from the copyright act, evincing an intent to eliminate that form of liability. *See* Irina D. Manta, *The Puzzle of Criminal Sanctions for Intellectual Property Infringement*, 24 Harv. J.L. & Tech. 469, 481 (2011) (“Several years later, countering what had been a trend of expansion in the area of criminal sanctions, the Copyright Act of 1976 eliminated the provisions for aiding and abetting . . .”).

34. In doubtful cases of criminal charges, the Supreme Court applies "the rule of lenity," which requires a court to interpret ambiguous statutory schemes in favor of defendants. *See Skilling v. United States*, 561 U.S. 358, 410 (2010) ("ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity").

35. It is also worth noting that, at present, there is no law which explicitly gives rise to felony criminal copyright infringement for the act of video streaming. Indeed the issue and "gap" has been debated before Congress but the copyright statute has not been updated to provide for such criminal liability. See, e.g. S. HRG. 112-922, "Oversight of Intellectual Property Law Enforcement Efforts" (committee debate over the need for a law to criminalize streaming copyrighted works on the internet).

36. The Superseding Indictment and Record of the Case include a great number of references to the "DMCA" or *Digital Millennum Copyright Act of 1998*, 17 U.S.C. § 512. See, e.g, Superseding Indictment, ¶¶ 21-24, 30, 32, 35, 36 and 38.

37. Among other provisions, the DMCA establishes a "safe harbor" for online service providers ("OSP"), namely, a statutory defense against civil infringement claims. *See UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1036 (9th Cir. 2013).

38. The DMCA is only a defense in the civil context because only civil indirect or secondary liability is possible under the common law. Common law liability principles cannot be extended to *criminal* liability, which must be specifically proscribed by statute. *See Dowling v. United States*, 473 U.S. 207, 213-214 (1985). Because there cannot be common law crimes under United States law, the DMCA further emphasizes that criminal indirect liability for copyright infringement does not exist by statute.

39. In *CoStar Group, Inc. v. LoopNet, Inc*., 373 F.3d 544, 552 (4th Cir. 2004) ("*Loopnet*"), the court held that lack of a DMCA defense did not mean that the defendant was civilly liable for infringements that occurred through its system. The court relied on § 512(l), which states:

"Other defenses not affected. — The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense."

40. The *Loopnet* court held (373 F.3d at 555): "It is clear that Congress intended the DMCA's safe harbor for ISPs to be a floor, not a ceiling, of protection. Congress said nothing about whether passive ISPs should ever be held strictly liable as direct infringers or whether plaintiffs suing ISPs should instead proceed under contributory theories. The DMCA has merely added a second step to assessing infringement liability for Internet service providers, after it is determined whether they are infringers in the first place under the preexisting Copyright Act. Thus, the DMCA is irrelevant to determining what constitutes a prima facie case of copyright infringement."

41. In my opinion, allegations of defendant's failure to maintain a DMCA policy or defects in a defendant's DMCA procedures cannot be the basis of criminal copyright charges. As discussed below, facts involving the DMCA do not support Copyright or Wire Fraud charges that are alleged in the Superseding Indictment.

42. Criminal prosecutions are also implicitly confined by express permissions in the civil area. An established protection against civil liability must perforce provide protection from a novel criminal prosecution. A leading case is *Religious Technology Center v. Netcom On-Line Communications Services, Inc*., 907 F. Supp. 1361 (N.D. Cal. 1995), relied on in *Loopnet*. (373 F.3d at 546.)

43. In *Loopnet*, a web hosting provider for real estate related content including photographs, was sued for copyright infringement arising out of end-user uploaded and distributed photographs. As stated in *Loopnet* (373 F.3d at 550): "something more must be shown than mere ownership of a machine used by others to make illegal copies. There must be actual infringing conduct with a nexus sufficiently close and causal to the illegal copying that one could conclude that the machine owner himself trespassed on the exclusive domain of the

copyright owner. The *Netcom* court described this nexus as requiring some aspect of volition or causation. 907 F. Supp. at 1370. Indeed, counsel for both parties agreed at oral argument that a copy machine owner who makes the machine available to the public to use for copying is not, without more, strictly liable under §106 for illegal copying by a customer. The ISP in this case is an analogue to the owner of a traditional copying machine whose customers pay a fixed amount per copy and operate the machine themselves to make copies. When a customer duplicates an infringing work, the owner of the copy machine is not considered a direct infringer. Similarly, an ISP who owns an electronic facility that responds automatically to users' input is not a direct infringer."

44. Criminal infringement is necessarily "direct infringement," in contrast to liabilities for "indirect" or "secondary" infringement in the civil context. Many allegations in the Superseding Indictment appear to attempt to allege secondary copyright infringement. (E.g., allegations as to "linking sites" at ¶¶ 11-14.) Such allegations may be relevant in a civil case alleging secondary infringement but they cannot be a basis for criminal charges of direct copyright infringement. Congress has never defined a crime of "secondary copyright infringement."

45. The Megaupload cloud service is a dual use technology capable of substantial non-infringing uses and thus protected by the "Sony Doctrine." In *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984) (***Sony***), the Court held that, because the video tape recorders at issue were "capable of substantial noninfringing uses," manufacturers could not be held liable for indirect infringement. 464 U.S. at 442 ("[T]he sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses."). *Id*. at 439.

46. In a later civil case, *MGM Studios, Inc. v. Grokster, Ltd*., 545 U.S. 913 (2005), the Court explained that, because many technologies have both infringing and non-infringing uses, otherwise known as "dual use" technologies, "mere knowledge of infringing potential or of actual

infringing uses would not be enough [] to subject a distributor to liability," and neither would "ordinary acts incident to product distribution, such as offering customers technical support or product updates, support liability in themselves." *Id.* at 937 (citation omitted).

47. Under civil copyright law, internet service providers, such as Megaupload, do not have a duty to investigate potential infringement. *See, e.g. Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627, 644 (S.D.N.Y. 2011).

THE IMPORTANCE OF GEOGRAPHICAL LOCATION

48. An important limitation on enforcement powers of the DOJ is the principle that the United State Copyright Act has no application outside of the territorial bounds of the US, and therefore there is neither civil nor criminal liability under United States law for acts of infringement taking place outside of US borders.

49. It is an "'undisputed axiom that United States copyright law has no extraterritorial application[.]'" *Subafilms, Ltd. v. MGM-Pathe Commc'ns Co.*, 24 F.3d 1088, 1093 (9th Cir. 1994) (*en banc*), *cert. denied*, 513 U.S. 1001 (1994) (quoting 3 David Nimmer & Melville B., *Nimmer on Copyrights* § 12.04[A][3][b], at 12-86 (1991)); *see Nintendo of Am., Inc. v. Aeropower Co. Ltd.*, 34 F.3d 246, 249 n.5 (4th Cir. 1994) (noting that the Copyright Act is "generally considered to have no extraterritorial application"); *In re Outsidewall Tire Litig.*, 2010 WL 2929626, at *8 (E.D. Va. July 21, 2010) (citing with approval the Ninth Circuit's extraterritoriality analysis in *Subafilms*).

50. "For the Copyright Act to apply, 'at least one alleged infringement must be completed entirely within the United States.'" *Elmo Shropshire v. Canning*, No. 10-CV-01941-LHK, 2011 WL 90136, at *3 (N.D. Cal. Jan. 11, 2011) (quoting *Los Angeles News Serv. v. Reuters Television Int'l, Ltd.*, 149 F.3d 987, 990-91 (9th Cir. 1998)); *accord Rundquist v. Vapiano SE*, 798 F. Supp. 2d 102, 126 (D.D.C. 2011).

51. The Superseding Indictment does discuss the existence of Megaupload servers in the United States, Sup. Ind. ¶¶ 26, 39, 40. But the mere presence of data servers in Virginia does not establish that

direct infringement took place there. *See, e.g., CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 549-50 (4th Cir. 2004) (holding that direct infringement under the civil standard requires more than "mere ownership of a machine used by others to make illegal copies" and that there "must be actual infringing conduct[.]"); *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121, 131-32 (2d Cir. 2008) (direct civil infringement requires "volitional conduct," not mere ownership of device used by others to infringe).

52. The Superseding Indictment never states that any specific user, much less any of the criminal defendants, chose to upload or download any specific infringing work from within the United States. *See, e.g.* Sup. Ind. ¶¶ 30, 33-38, 55, 73(k), 73(v), 73(y), 73(ee), 73(uu), 73(fff), 73(qqq), 73(www), 73(xxx), 73(yyy), 73(aaaa), 73(gggg), 73(aaaaa), 73(bbbbb), 73(jjjjj), 73(kkkkk), 73(rrrrr). Although facts in the Record of the Case identify unindicted co-conspirators as residing in the Eastern District of Virginia, specific allegations of criminal conduct are lacking. (See e.g., ¶¶ 50, 51, 57, 61, 64, 66, 67, 69 and 70 of the Record of the Case.

THE UNITED STATES HAS FAILED TO PROVE A PRIMA FACIE CASE OF DIRECT INFRINGEMENT UNDER CIVIL COPYRIGHT LAW

53. In order to establish a prima facie case of civil copyright infringement, a plaintiff must prove: (1) that he owns a valid copyright, and (2) that the defendant engaged in unauthorized copying. *Nelson-Salabes, Inc. v. Morningside Dev., Inc.*, 284 F.3d 505, 513 (4th Cir. 2002).

54. Requirements of specificity in the civil context were set forth in *Energy Intelligence Group, Inc. v. Jefferies, LLC*, 2015 U.S. Dist. LEXIS 43230 (S.D.N.Y. 2015), where the court stated, in a claim for copyright infringement:

> "Rule 8 requires that the particular infringing acts be set out with some specificity." *Kelly v. L.L. Cool J.*, 145 F.R.D. 32, 36, n.3 (S.D.N.Y.1992), aff'd 23 F.3d 398 (2d Cir. 1994), cert. denied, 513 U.S. 950, 115 S. Ct. 365, 130 L. Ed. 2d 318 (1994)" (internal citations omitted).

55. Under the *Kelly* court's four-prong test, a claim of copyright infringement must allege (*Jacobs v. Carnival Corp*., 2009 U.S. Dist. LEXIS 31374, 2009 WL 856637 (S.D.N.Y. Mar. 25, 2009):

> "(1) which specific original works are the subject of the copyright claim, (2) that plaintiff owns the copyrights in those works, (3) that the copyrights have been registered in accordance with the statute, and (4) by what acts and during what time the defendant infringed the copyright."

56. In my opinion, there is a failure of proof of claims of direct infringement against respondents, in the light of constraints on civil claims discussed above. Relevant allegations fail to prove a case under the civil standards set forth in *Loopnet*, supra. There is no connection between “specific original works” and allegations of wrongdoing that would show “by what acts and during what time the defendant infringed the copyright.” What is alleged is “mere ownership of a machine used by others to make illegal copies.” Absent are allegations of “actual infringing conduct with a nexus sufficiently close and causal to the illegal copying that one could conclude that the machine owner himself trespassed on the exclusive domain of the copyright owner.” (Para. 40, above.) Liability cannot be “based on a failure to take affirmative steps to prevent infringement, if the device otherwise was capable of substantial noninfringing uses.” (Para. 42.) Respondents do not have a duty to investigate potential infringement.” (Para. 44.) The failure to allege a prima facie case under the civil case law is fatal to the Government’s claims. See *Kelly*, *supra*, 145 F.R.D. at 39 (“conduct that does not support a civil action for infringement cannot constitute criminal conduct under 17 U.S.C. § 506(a).”

57. Megaupload cloud users, like those in *Loopnet*, used automated cloud storage processes, agreed to Terms of Use, and uploaded and shared digital materials with other users on a dual use technology platform. If there were no user-uploaded content then the Megaupload cloud storage systems would be devoid of content. If no user made use of a given URL to share such uploaded content then no online distribution would ever occur. Strip away the user-controlled conduct and content and the voluminous Government allegations disappear.

58. Megaupload cloud storage services, handling at one point 4% of all Internet traffic in which automated server data transactions occur with breathtaking volume and speed, are a prototypical example of an ISP's lack of volitional control over user infringements. This type of passive hosting scenario led the Fourth Circuit Court of Appeals in *Loopnet* to conclude that, "[a]t bottom, we hold that ISPs, when passively storing materials available to other users upon their request, do not 'copy' the material in direct violation of section 106 of the Copyright Act." *Loopnet*, *supra*, at 555.

59. But, as discussed below, the criminal allegations give the Megaupload defendants even broader protections than the civil *Loopnet* defendant. The crime of felony copyright infringement requires the DOJ to demonstrate that the defendants "willfully" undertook the infringing acts on a work by work basis under the required elements of the statute. The criminal copyright statute itself emphasizes the high threshold of evidence needed to make out a *prima facie* criminal copyright claim, namely, that "[e]vidence of reproducing and distributing copyrighted works does not, by itself, establish willfulness." *See* 17 U.S.C. § 506(a)(2).

THE UNITED STATES HAS FAILED TO PROVE A PRIMA FACIE CASE UNDER CRIMINAL COPYRIGHT LAW

60. I am aware that Judge Harvey in New Zealand has stated that all of the extradition charges "hang upon the establishment of criminal copyright infringement." *Dotcom et al v. US*, DC NSD (May 29, 2012) at ¶ 68.

61. As a summary of my opinion: the DOJ fails to show direct criminal copyright infringement on the part of Megaupload personnel or on the part of Megaupload cloud storage users. The allegations in the Superseding Indictment and the Record of the Case do not match up to all of the elements of offenses. Importantly, there is no showing that *any* specific Megaupload representative or third-party user had the requisite *mens rea* to willfully violate copyright law. There is an even more fatal failure to show that Megaupload personnel agreed with a third party user to commit such violations. An agreement requires

communications between defendants and the user, not just discussions among Megaupload personnel and a general "environment of infringement." Attempts to juxtapose pieces of allegations do not succeed in making even a single whole, unified criminal charge.

62. Criminal copyright infringement is codified at 17 U.S.C.§ 506(a) and has the following requirements:

> "(1) In general.--Any person who willfully infringes a copyright shall be punished as provided under section 2319 of title 18, if the infringement was committed--
>
> (A) for purposes of commercial advantage or private financial gain;
>
> (B) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000; or
>
> (C) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if such person knew or should have known that the work was intended for commercial distribution."

63. The *mens rea* standard — "willfully infringes a copyright" — requires a stronger showing in a criminal copyright claim than in a civil claim. See *Kelly*, *supra*, 145 F.R.D. at 39 ("conduct that does not support a civil action for infringement cannot constitute criminal conduct under 17 U.S.C. § 506(a). *Nimmer on Copyright*, § 15.01.") aff'd sub nom. *Kelly v. L.L. Cool J*, 23 F.3d 398 (2d Cir. 1994); see also *Berry v. Hawaii Exp. Serv., Inc*., 2006 WL 505319, at *7 (D. Haw. Feb. 27, 2006).

64. The copyright statute itself indicates the higher level of knowledge and intent in a "willfulness" mental state. "Evidence of reproducing and

distributing copyrighted works does not, by itself, establish willfulness." *See* 17 U.S.C. § 506(a)(2).

65. Thus, under a willfulness standard, proof of indifference, recklessness, or negligence is insufficient to constitute criminal copyright infringement. Attacking an ISP for generally bad or negligent policies or alleging how the ISP could be better, faster, or more precise in its takedown or repeat infringer policies is not enough. "Willfully" as used in 17 U.S.C. § 506(a) connotes a "voluntary, intentional violation of a known legal duty." *United States v. Liu*, 731 F.3d 982, 990 (9th Cir. 2013). Proof of the "defendant's specific intent to violate someone's copyright is required." *Id.* at 989-90.

66. *Liu* further holds that a general intent to copy is insufficient for criminal copyright liability. *Id.* at 991. If 17 U.S.C. § 506(a)'s willfulness requirement were read "to mean only an intent to copy, there would be no meaningful distinction between civil and criminal liability in the vast majority of cases." *Id.* "[W]illful infringement requires a showing of specific intent to violate copyright law." *BC Tech., Inc. v. Ensil Int'l Corp*., 464 Fed. Appx. 689, 696 (10th Cir. 2012). For example, vague allegations borrowed from civil copyright case law regarding Megaupload's "rewards program" does not arise to "willfulness" under the criminal standard even if it can be shown that such a policy generally increased infringing use of the site.

67. Indeed, a defendant's erroneous belief that copying was lawful is sufficient to avoid criminal liability. In 1997, the Registrar of Copyrights testified before Congress and stated (http://www.copyright.gov/docs/2265_stat.html):

> "The courts have held that it is not enough for the defendant in a criminal case to have had an intent to copy the work; he must have acted with knowledge that his conduct constituted copyright infringement. See, e.g., *United States v. Cross*, 816 F.2d 297, 300 (7th Cir. 1987) and United *States v. Moran,* 757 F. Supp. 1046 (D. Neb. 1991). In *Cross*, the Seventh Circuit upheld the

> following jury instruction for determining willfulness under the criminal provision of the Copyright Act:
>
> '[W]illfully' as used in the statute means the act was committed by a defendant voluntarily, with knowledge that it was prohibited by law, and with the purpose of violating the law, and not by mistake, accident or in good faith. 816 F.2d at 300.
>
> In *Moran*, the defendant was charged with criminal infringement for his practice of making backup copies of the videotapes he purchased for his video rental store. The court held that the "willful" element of criminal copyright infringement was similar to that in federal criminal tax statutes, and thus requires a "voluntary, intentional violation of a known legal duty." *Id*. at 1049 (citing *U.S. v. Cheek*, 111 S.Ct. 604, 610 (1991)). The court therefore held that because the defendant believed, albeit incorrectly, that he had a right to make such copies, he could not be convicted of criminal infringement. *Id*. at 1051-52."

68. In my opinion, proof of charges of both Criminal Copyright Infringement and also Conspiracy to commit such crimes must identify specific copyrighted works on a work by work, link by link basis, and describe the who, what, when, where, why, and how to meet all the elements for each such instance and to examine fair use, amongst other things. The "willfulness" requirement means that a person must have had the specific intent to commit copyright infringement as to each individual work.

69. See also *Viacom Int'l, Inc. v. YouTube, Inc*., 676 F.3d 19, 34 (2d Cir. 2012) (requiring in the civil context assessment of knowledge level of defendant as regarded each and every file alleged to be part of defendant's mass infringement); *Viacom Int'l Inc. v. YouTube, Inc*., 940 F. Supp. 2d 110, 115-123 (S.D.N.Y. 2013) (ruling that plaintiffs had no "clip-by-clip" evidence to prove knowledge of infringement for any of the 63,060 video clips-in-suit)

70. In my opinion, during the applicable period of time, no individual Megaupload defendant is shown to have so "willfully" or criminally copied or distributed a copyrighted work.

71. Counts Five through Eight charge "Criminal Copyright Infringement By Electronic Means & Aiding and Abetting Criminal Copyright Infringement." It appears that criminal infringements were alleged committed by unnamed Megaupload cloud storage users and that respondents are charged with "Aiding and Abetting." Under United States law, aiding and abetting is a theory of accomplice liability for those who participate in crimes. Thus a defendant who is charged with "aiding and abetting criminal copyright infringement," has only been charged with the crime of copyright infringement, and not with any other crime or with extraditable conspiracy.

72. As noted above (para. 33), charges of aiding and abetting are facially improper under the reasoning in *Dowling* and its progeny as Congress removed "aiding and abetting" from the copyright statute.

73. Under 18 U.S.C. § 2 (a), whoever aids, abets, counsels, commands, induces, or procures the commission of an offense against the United States is punishable as a principal. Under 18 U.S.C. § 2 (b), Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal. In order to make out a prima facie case against a defendant for aiding and abetting crime, the Government must produce sufficient evidence to show that the defendant knowingly associated himself with and participated in the criminal venture. See United States v. Winstead, 708 F.2d 925, 927 (4th Cir. 1983) (citing Nye & Nissen v. United States, 336 U.S. 613, 619-20, 69 S. Ct. 766, 93 L. Ed. 919 (1949); United States v. Beck, 615 F.2d 441, 448 (7th Cir. 1980); United States v. Pearlstein, 576 F.2d 531, 546 (3d Cir. 1978); United States v. Di Stefano, 555 F.2d 1094, 1103 (2d Cir. 1977)). In order to prove the element of association, the Government must show that the defendant shared in the principal's criminal intent. See id. (citing Beck, 615 F.2d at 449). As the Fourth Circuit stated in Winstead, this requires evidence that the defendant be aware of the principal's criminal intent and the unlawful nature of his acts. See id.

(citing Pearlstein, 576 F.2d at 546). Evidence that the defendant merely brought about the arrangement that made the criminal acts of the principal possible does not alone support a conclusion that the defendant was aware of the criminal nature of defendant's acts. See id. (citing United States v. Belt, 574 F.2d 1234, 1240 (5th Cir. 1978)). (United States v. Ecklin, 837 F. Supp. 2d 589, 591-92 (E.D. Va. 2011)

74. Aiding and abetting requires a showing of "double wilfulness," which is lacking in the Superceding Indictment and ROC. A vague charge of "making available" a copyrighted work under a theory of "Aiding and Abetting Criminal Copyright Infringement," is insufficient. In my opinion the government has failed to allege sufficient facts that the Megaupload defendants shared in any alleged infringer's criminal willful intent. Gestalt allegations that the Megaupload cloud storage system brought about the arrangment that made the vague criminal acts of the alleged infringers possible is insufficient "willfulness" as a matter of law. As discussed above, Megaupload did not exercise volitional control over user uploads, link sharing, and downloads.

75. The Supreme Court of the United States has stated that the aiding and abetting statute converts an accomplice into a principal, but that aiding and abetting is neither a separate crime nor is it relevant to the distinct crime of conspiracy. See *Pereira v. United States*, 347 U.S. 1, 11 (1954) ("Aiding, abetting, and counseling are not terms which presuppose the existence of an agreement. Those terms . . . mak[e] the defendant a principal when he consciously shares in a criminal act, regardless of the existence of a conspiracy.") (emphasis added). Therefore, allegations that defendants aided or abetted a crime of copyright infringement do not amount to an extraditable offense. The crime, if it exists, must be specifically shown.

THE UNITED STATES HAS FAILED TO PROVE A PRIMA FACIE CASE UNDER THE LAW OF CONSPIRACY

76. Charges of Conspiracy to Commit Copyright Infringement are alleged in Count Two of the Superseding Indictment. Defects in charges of Criminal Copyright Infringment (Counts Four through Eight) re-appear in doubled form in Count Two.

77. The Fourth Circuit has stated that a conspiracy charge contains three elements: (1) "an agreement between two or more persons to act together in committing an offense," (2) "an overt act in furtherance of the conspiracy," and (3) "[t]here must be some showing that the defendant knew the conspiracy's purpose and took some action indicating his participation." *United States v. Chorman*, 910 F.2d 102, 109 (4th Cir. 1990). See *United States v. Kingrea*, 573 F.3d 186, 193 (4th Cir. 2009) (dismissing indictment that "failed to state an offense against the United States as the object of the conspiracy.").

78. The DOJ must show a union of criminally willful conduct on the part of an actual infringer and criminally willful conduct on the part of a conspirator. Evidence that Megaupload acted willfully is insufficient if it does not unite with underlying *direct* infringements that are also willful. *See* 17 U.S.C. § 506(a); *United States v. Mekjian*, 505 F.2d 1320, 1324 (5th Cir. 1975) (dismissing indictment that failed to allege willfulness); *Med. Supply Chain, Inc. v. Neoforma, Inc*., 419 F. Supp. 2d 1316, 1328 (D. Kan. 2006) (civil complaint). “Even if civil liability has been established, without the requisite *mens rea* it does not matter how many unauthorized copies or phonorecords have been made or distributed: No criminal violation has occurred.” House Report, *Copyright Felony Act*, H.R. Rep. No. 997, 102nd Cong., 2nd Sess. 1992, 1992 U.S.C.C.A.N. 3569, P.L. 102-561. See *Kelly*, *supra*, 145 F.R.D. at 39 (“conduct that does not support a civil action for infringement cannot constitute criminal conduct under 17 U.S.C. § 506(a).”)

79. The required agreement between conspirators need not take a particular form, however, there must be some genuine meeting of the minds as to commission of a crime: merely engaging in a business transaction is not sufficient to charge the crime of conspiracy. As one court explained, ordinary retail businesses are not engaged in a conspiracy with their customers merely because they engage in repeat or standardized transactions. See *United States v. Colon*, 549 F.3d 565, 567-68 (7th Cir. 2008) (finding no conspiracy because “[i]f you buy from Wal-Mart your transactions will be highly regular and utterly

standardized, but there will be no mutual trust suggestive of a relationship other than that of buyer and seller.").

80. *United States v. Hickman*, 626 F.3d 756 (4th Cir. 2010), a decision by the Fourth Circuit Court of Appeals is particularly instructive. In that case, the court was asked to decide if a store that sold thousands of glass vials was engaged in a conspiracy to distribute heroin, since it was well known that such glass vials were used primarily to package heroin for sale. *Id*. at 767-73. The Fourth Circuit explained that merely selling the vials was not sufficient to demonstrate the crime of conspiracy without something more. *Id*. The court would have required that the defendant possess explicit knowledge of specific plans to distribute heroin in order to be convicted of conspiracy. *Id*. This is consistent with other Fourth Circuit decisions which generally require a "showing that the defendant knew the conspiracy's purpose and took some action indicating his participation." *Chorman*, 910 F.2d at 109.

81. As mentioned above, a member of the conspiracy must undertake some "overt act" which furthers the underlying offense of the conspiracy. *Chorman*, 910 F.2d at 109. Thus, in order to properly state a claim for conspiracy to commit felony copyright infringement, there must be an agreement between two individuals to commit that crime, and then one of the individuals, who is a party to the agreement, must commit an act in furtherance of that crime.

82. As discussed above, infringing acts are alleged to have been committed by unnamed Megaupload users. A crime of conspiracy requires an agreement with criminal infringers. No such agreement is shown.

83. Megaupload had no reliable means of detecting which uploads were authorized uses, which were fair uses and which were infringing uses in the United States or in some other country. No criminal statute or legal decision imposes a duty on an online services provider to employ such means of detection. In my opinion, the criminal law may not be used to impose a duty to employ such means of detection.

84. Evidence in the Record of the Case fails to overcome the defects. For example, in paragraph 73y of the Superseding Indictment, the DOJ describes a conversation between two Megaupload employees regarding a Megaupload user who allegedly stored infringing content on Megaupload. However, there is no allegation of direct communication with the user, and no reason to believe that the Megaupload employees entered into a relationship with the user beyond a series of retail transactions regarding cloud storage space on the Megaupload leased servers.

85. The allegations relating to the "Uploader Rewards" program similarly describe a series of retail transactions. Paragraph 73jj describes standardized payments based upon regular uploads, yet the paragraph contains no further details and no allegation as to how the individuals involved were coordinating in a manner beyond ordinary commercial transactions.

86. Paragraphs 73qq, 73uu, 73ppp, 73qqq, 73www, 73xxx, 73yyy, 73aaaa, and 73gggg of the indictment all likewise describe payments going to or from Megaupload but fail to allege any agreement to infringe. The fact that the payments were made repeatedly or at regular intervals does not change this analysis. As the courts have explained, "utterly regular and highly standardized" payments do not create an inference of conspiracy. *United States v. Colon*, 549 F.3d 565, 567-68 (7th Cir. 2008).

THE UNITED STATES HAS FAILED TO PROVE A PRIMA FACIE CASE OF WIRE FRAUD

87. Counts Nine through Thirteen of the Superseding Indictment charge respondents with "Fraud By Wire & Aiding and Abetting of Fraud by Wire." For reasons discussed above, "Aiding & Abetting" adds nothing to the charges.

88. In my opinion, the DOJ is improperly attempting to use a "wire fraud" theory to criminalize new categories of conduct without the required Congressional authorization.

89. In *United States v. LaMacchia*, 871 F.Supp. 535 (D. Mass. 1994), the court relied on Dowling, *supra*, to prohibit prosecution of a "bulletin board operator" (for an online bulletin board intended for students) charged with wire fraud by the DOJ. In that case, the DOJ attempted a similar kind of "end run" around the copyright statute.

90. Allegations here revolve around Megaupload's procedures for implementing a civil copyright safe harbor statute, part of the DMCA (17 U.S.C. § 512). The DMCA specifies procedures for removing access to infringing files by defining a "notice" of infringing materials that is sent by copyright owners to website operators and resulting "takedowns" of access and/or materials. Access to the DMCA civil safe harbor requires a "reasonable" take down policy, not a perfect one. Although Congress provided civil relief for certain injured parties who are presented with take-down notices that contain material misrepresentations, there is no criminal liability. Any potential civil liability for misrepresentations in take down notices under 512(f) would be against the parties providing take down notices. Congress did not codify misrepresentation claims against Online Service Providers who make DMCA errors. A criminal theory that attempts to turn unfulfilled promises of DMCA compliance into a Wire Fraud claim is contrary to the plain intentions and language of the statute. In addition, causation and damages allegedly resulting from the alleged Wire Fraud are shown in only the most general and conclusory way that are clearly insufficient.

91. Alleged frauds revolve around Megaupload's practices under the DMCA and around an "Abuse Tool" Megaupload provided to copyright owners or agents who wanted to deliver to Megaupload DMCA notices of infringing materials on the Megaupload site and automatically disable access to such materials. It is alleged that Megaupload made misrepresentations in connection with the Abuse Tool, promising to delete access to referenced materials while only deleting the referenced URLs and without deleting all other URLs in the database that pointed to such materials. It is further alleged that the Abuse Tool did not operate as represented, that deletions were delayed and that

the site promised to terminate repeat infringers but failed to do so. Sup. Indict. ¶ 102-104.

92. As mentioned above, the DMCA serves to explicitly limit the copyright liability of Internet service providers and to provide a "safe harbor" from copyright claims. *See* 17 U.S.C.A. § 512 ("A service provider shall not be liable . . ."). If an online service provider like Megaupload is non-compliant the result is loss of the civil safe harbor defense not a criminal fraud.

93. In *United States v. Aleynikov*, 676 F.3d 71, 78 (2d Cir. 2012), the appellate court would not allow distribution of copyrighted computer code to be charged as a crime under the *National Stolen Property Act*; once again the proper recourse would have been to charge the defendant under the copyright statute, and an attempt to avoid that statute was barred. Likewise, in *United States v. Brooks*, 945 F. Supp. 830, 834 (E.D. Pa. 1996), the court held that a statute which criminalized making false statements to the United States Government, *did not apply* to false statements made to the copyright office, where that was separately punished under the copyright act.

94. It is, therefore, my opinion that the general criminal statute of wire fraud cannot take the place of the copyright act or alleged broken DMCA compliance policies.

95. The crime of wire fraud has two elements: the DOJ "must show that the defendant (1) devised or intended to devise a scheme to defraud and (2) used the mail or wire communications in furtherance of the scheme." *United States v. Wynn*, 684 F.3d 473, 477 (4th Cir. 2012). The offense is also defined as: "wronging one in his property rights by dishonest methods or schemes and usually signify[ing] the deprivation of something of value by trick, deceit, chicane, or overreaching." *Id*.

96. Under Fourth Circuit precedent, an actionable deprivation requires "convergence" between the person who is deceived and the person whose property is obtained. *See Lifschultz Fast Freight, Inc. v. Consol. Freightways Corp. of Delaware*, 805 F. Supp. 1277, 1294 (D.S.C. 1992) *aff'd*, 998 F.2d 1009 (4th Cir. 1993) ("the better reasoned rule is

to require a convergence of the identity of the injured and the deceived.") This means that "the intent must be to obtain money or property from the one who is deceived." *United States v. Lew*, 875 F.2d 219, 221 (9th Cir. 1989). The instant charges fail the convergence test.

97. It is alleged that Megaupload received "advertising revenue as a result of the continued availability of files," while never stating that the copyright holders themselves made any pay outs. Sup. Indict. ¶ 103. Thus, there is no allegation that *the advertisers* were ever lied to, deceived or misled; in other words, the party deceived and the party that lost property were two completely different individuals.

98. It is also alleged that Megaupload received money from users who purchased premium subscriptions. Sup. Indict. ¶ 103. However, as with the advertisers, there is no indication that the users were deceived or misled in any way. .

99. Moreover, the DOJ must look at the monies actually received when charging the crime of wire fraud, and cannot look to any "intangible right" that may belong to the copyright holder. United States courts have explained that intangible rights cannot form the basis of a wire fraud charge. *See United States v. Hilling*, 891 F.2d 205, 208 (9th Cir. 1988) (reversing a mail fraud conviction based on intangible rights). Nor is a "license" a recognized property right. *See United States v. Schwartz*, 924 F.2d 410, 418 (2d Cir. 1991) (overturning wire fraud conviction because "[t]he [] licenses given appellants were merely the expression of its regulatory imprimatur, and they had no other effect as 'property'").

100. In sum, the DOJ only alleges that one party was deceived: the copyright holders. Sup. Indict. ¶ 102. However, that party cannot lay a claim to a recognized property right that Megaupload is alleged to have taken; at best the rights claimed would be the right to license their works, or similar intangible rights which cannot form the basis of a wire fraud conviction. *See Hilling*, 891 F.2d at 208; *Schwartz*, 924 F.2d at 418.

101. Another defect in the DOJ approach is that it is contrary to the DMCA. The Fourth Circuit has repeatedly upheld the principal of statutory interpretation which holds that courts "must give effect to every provision and word in a statute and avoid any interpretation that may render statutory terms meaningless[.]" *Scott v. United States*, 328 F.3d 132, 139 (4th Cir. 2003). Here, in order to give proper effect to the DMCA, the wire fraud statute cannot be interpreted to criminalize Megaupload's conduct.

102. The DMCA also expressly limits liability when an internet service provider "reasonably implement[s]" a policy to terminate "repeat infringers[.]" 17 U.S.C.A. § 512.

103. While the statute does not define "reasonably implement" courts have found a service provider to act reasonably "if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications." *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1109 (9th Cir. 2007).

104. The DOJ does not allege that Megaupload had no policy at all, nor does the DOJ allege that Megaupload "actively prevent[ed] copyright owners from collecting information[.]" Instead, the DOJ charges a much lower standard: that Megaupload failed to terminate 100% of all repeat infringers, Sup. Indict. ¶ 102, and moreover, that this failure, in the face of Megaupload's stated policy, was a misrepresentation sufficient to sustain a charge of wire fraud. *Id*.

105. The purpose of the DMCA is to prevent liability where a defendant has stated a policy and *reasonably* implemented it—not where a defendant has failed to terminate each and every repeat infringer. Indeed, the statute recognizes that service providers are *not* required to terminate all repeat infringers in order to comply with the DMCA (17 U.S.C. § 512(I)(1)(A)) or to remove their posted content. *See e.g. Perfect 10, Inc. v. Giganews, Inc.*, 2014 WL 8628034, at *9 (C.D. Cal. Nov. 14, 2014) ("Giganews had no obligation to indiscriminately remove every post a repeat infringer ever posted and Perfect 10 may not shift its

burden of policing copyright infringement to Giganews in the guise of a claim for direct infringement.").

106. Were the DOJ able to simply charge defendants with a separate crime (in this case wire fraud) then the liability safe harbor becomes meaningless, and *Scott v. United States* is thus violated. As a result, it is improper to interpret the wire fraud statute as criminalizing Megaupload's actions, and the proper interpretation is to give effect to the DMCA's stated safe harbor provisions.

107. The DOJ appears to be asserting that an online operator who receives copyright take down notices identifying one URL must search for and delete all duplicate files in the system or be subject to a copyright or fraud claim. In my opinion the DOJ's theory of copyright or fraud liability is erroneous.

108. Megaupload reduced operating loads by "deduplication," namely maintaining only a single copy of a file in its database and generating multiple pointers to such file. Each pointer identified an uploader of the common file. It is possible for one uploader to have a right to fair use of a copy of a file, e.g., a purchaser uploading a backup or an educational organization offering critical commentary, while other uploaders might have no such fair use right. It is contrary to the purpose of the DMCA that a fair use right would be violated though a take-down notice directed at another person's wrongful use. If such a violation were to occur, the provider of the take-notice would be subject to liability under the DMCA (17 U.S.C. § 512(f)).

109. Such an approach can lead to mass DMCA 512(f) misrepresentation claims against the DMCA noticing parties.

110. The DOJ's charges would compel Online Service Providers to take down all duplicates of a file for which notice is sent without the benefit of analysis of all the other varying uses, users, and contexts. The sender of the notice would be ignorant of all contexts and would not know of users who had purchased the work and had a right to make and store a copy or users who had fair use rights or authorization. For example news, archive, and educational institutions may have broader

rights to use certain copyrighted works than other organizations. In *Lenz v. Universal Music Corp.*, No. 5:07-cv-03783, slip op. at 5 (N.D. Cal. Aug. 20, 2008) the court squarely rejected the DOJ approach and held as follows:

> "[I]n order for a copyright owner to proceed under the DMCA with "a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law," the owner must evaluate whether the material makes fair use of the copyright. An allegation that a copyright owner acted in bad faith by issuing a takedown notice without proper consideration of the fair use doctrine thus is sufficient to state a misrepresentation claim pursuant to Section 512(f) of the DMCA. *Id*. at 6."

THE UNITED STATES HAS FAILED TO SHOW ANY CONSPIRACY TO COMMIT RACKETEERING OR CONSPIRACY TO COMMIT MONEY LAUNDERING

111. Counts One and Three allege Conspiracy to Commit Racketeering under 18 U.S.C. § 1962(d) and Conspiracy to Commit Money Laundering under 18 U.S. C. 1956(h). Each of these Counts requires a predicate offense that is lacking here.

112. Under 18 U.S.C. § 1962(d), it is unlawful to "conspire to violate" RICO. RICO makes it unlawful "for any person employed by or associated with any enterprise engaged in, or the activities of which affect, interstate or foreign commerce, to conduct or participate, directly or indirectly, in the conduct of such enterprise's affairs through a pattern of racketeering activity." 18 U.S.C. § 1962(c). A "pattern of racketeering activity," consists of "at least two acts of racketeering activity" occurring within a ten-year period, 18 U.S.C. § 1961(5), that are related and "amount to or pose a threat of continued criminal activity." *H.J. Inc. v. Nw. Bell Tel. Co*., 492 U.S. 229, 239, 109 S. Ct. 2893, 106 L. Ed. 2d 195 (1989). "To properly allege the predicate acts, plaintiff must specify the 'who, what, where, and when' of each purported act.' " *Med. Supply Chain, Inc. v. Neoforma, Inc*., 419 F.

Supp. 2d 1316, 1329 (D. Kans. 2006). See also See *United States v. Baker*, 598 Fed. Appx. 165, 172 (4th Cir. 2015).

113. The money laundering statutes criminalize either the concealing or trafficking of funds which represent the proceeds of criminal activity. See 18 U.S.C. §§ 1956, 1957. The government must prove that a separate crime occurred first, and that this separate crime generated proceeds which were later concealed or trafficked. See, e.g. *United States v. Mankarious*, 151 F.3d 694, 702 (7th Cir. 1998) ("The government must prove that the defendant conducted a financial transaction which in fact involves the proceeds of specified unlawful activity").

CONCLUSION

114. The DOJ has failed to prove a case of direct civil copyright infringement. The Megaupload cloud storage system was the type of passive Internet hosting contemplated by the *Loopnet* court. There is an absence of compact facts that show liability of respondents for copyright infringement in the United States of a specific copyrighted work. Just as important, the Fourth Circuit Court of Appeals in *Loopnet* concluded that, "[a]t bottom, we hold that ISPs, when passively storing materials available to other users upon their request, do not 'copy' the material in direct violation of section 106 of the Copyright Act." *Loopnet*, *supra*, at 555.

115. The DOJ has failed to prove a case of criminal copyright infringement. Criminal infringement prohibitions under 17 U.S.C. § 506(a) apply to specific kinds of misconduct or to protect specific kinds of copyrighted works. Necessary specificity as to extraditable offenses is not clearly stated in the ROC. To prove a criminal case, in addition to showing copyright infringement of specific works in the United States, the DOJ must show a very high level of knowledge and intent, namely, a "willfulness" mental state. "Evidence of reproducing and distributing copyrighted works does not, by itself, establish willfulness." *See* 17 U.S.C. § 506(a)(2). Under a willfulness standard, proof of indifference, recklessness, or negligence is insufficient to constitute criminal copyright infringement. Attacking an ISP for generally bad or negligent

policies or alleging how the ISP could be better, faster, or more precise in its takedowns, user terminations, or repeat infringer policies is not enough. “Willfully” as used in 17 U.S.C. § 506(a) connotes a “voluntary, intentional violation of a known legal duty.” (See para. 61 and *United States v. Liu*, 731 F.3d 982, 990 (9th Cir. 2013).) Allegations revolve around, “fostering an environment conducive to infringement,” similar to a civil case of secondary copyright infringement. Principles of United States criminal law prohibit novel and expansive prosecutions on the basis of such evidence.

116. The DOJ has failed to prove a case of criminal conspiracy. In addition to proof of criminal copyright infringement in the United States of specific copyrighted works, the DOJ must show an agreement with respect thereto between the actual infringer and an alleged conspirator. No such agreement is shown here. General allegations of, “fostering an environment” cannot substitute for the requisite agreement or for the necessary “willful” mental state of the alleged conspirator.

117. The DOJ has failed to prove a case of wire fraud. In my opinion, the DOJ is improperly attempting to use an inappropriate “wire fraud” theory to criminalize new categories of conduct without the required Congressional authorization. Criminal charges based on alleged DMCA shortcomings would be contrary to DMCA principles stated by Congress. Wire fraud allegations further suffer from lack of requisite damages suffered by the victim of the fraud.

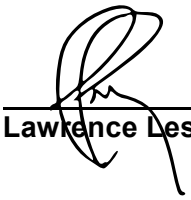
118. The remaining alleged counts of RICO and Money Laundering require a predicate offense that is lacking here.

119. It is my opinion that the Superseding Indictment and Record of the Case filed by the DOJ do not meet the requirements necessary to support a prima facie case that would be recognized by United States federal law and subject to the **US-NZ Extradition Treaty**. An attempt has been made to extract facts from multiple sources and over a wide span of time, to organize a large number of otherwise disconnected facts by using systematic phraseology and to juxtapose phrases in order to create an impression of coherence and substance. However,

the attempt fails to reach its goals and any impression of coherence or substance dissolves under examination. Insofar as they are alleged in the Superceding Indictment and the ROC, respondents' actions were not prohibited by criminal statutes of the United States. Filings of the DOJ attempt to create a false impression of criminal guilt and are not reliable.

I DECLARE under penalty of perjury under the laws of the State of Massachusetts and the United States of America that the foregoing is true and correct.

EXECUTED this 14th day of September 2015, at



Lawrence Lessig